Gruppentheorie

Vorlesung im Wintersemester 2020/21

Benjamin Sambale
Leibniz Universität Hannover

Version: 12. August 2020

Inhaltsverzeichnis

Vorwort

Dieses Skript entstand aus einer Vorlesung im Wintersemester 2016/17 an der Technischen Universität Kaiserslautern. Es dient als Grundlage einer entsprechenden Vorlesung im Wintersemester 2020/21 an der Leibniz Universität Hannover. Diese Vorlesung richtet sich hauptsächlich an Studierende des Studiengangs Bachelor Mathematik. Es werden Kenntnisse der Algebra 1 & 2 vorausgesetzt, wobei die wichtigsten Ergebnisse im ersten Kapitel ohne Beweis wiederholt werden (Beweise findet man zum Beispiel in meinem Algebra-Skript).

Literatur:

- H. Kurzweil, B. Stellmacher, *Theorie der endlichen Gruppen*, Springer, Berlin, 1998[1]
- G. Stroth, *Endliche Gruppen*, De Gruyter, Berlin, 2013[2]
- I. M. Isaacs, *Finite group theory*, Amer. Math. Soc., R.I., 2008[3]
- B. Huppert, *Endliche Gruppen I*, Springer, Berlin, 1967[4]
- D. Gorenstein, *Finite groups*, 2nd edition, Chelsea, New York, 1980

[1] 2004 erschien eine Version auf Englisch.
[2] Ein kurzes Buch mit einigen fortgeschrittenen Themen.
[3] Anfängerfreundlich mit sehr ausführlichen Beweisen. Für meinen Geschmack zu ausführlich – es bleiben keine eigenen Aha-Effekte.
[4] Ein Klassiker mit fast 800 Seiten. Wegen Fraktursymbolen etwas schwer zu lesen.

1 Untergruppen, Normalteiler und Faktorgruppen

Wir wiederholen in diesem Kapitel einige Ergebnisse der Algebra-Vorlesung.

Definition 1.1. Eine *Gruppe* G ist eine Menge zusammen mit einer Abbildung $G \times G \to G$, $(x, y) \mapsto xy$, sodass folgende Eigenschaften gelten:

- $\forall x, y, z \in G : (xy)z = x(yz)$ (*Assoziativität*).
- $\exists e \in G : \forall x \in G : ex = x$ (*neutrales Element*).
- $\forall x \in G : \exists y \in G : yx = e$ (*inverse Elemente*).

Gilt zusätzlich

- $\forall x, y \in G : xy = yx$ (*Kommutativität*),

so nennt man G *abelsch*. Die *Ordnung* von G ist die Mächtigkeit $|G|$.

Bemerkung 1.2.

(i) Im Folgenden sei G stets eine Gruppe.

(ii) Für $x \in G$ existieren $y, z \in G$ mit $yx = e = zy$. Es folgt

$$xy = e(xy) = (zy)(xy) = z(yx)y = z(ey) = zy = e$$

und $xe = x(yx) = (xy)x = ex = x$. Ist auch $e' \in G$ ein neutrales Element, so gilt $e' = e'e = e$. Also ist e eindeutig bestimmt und wir schreiben $e = 1_G = 1$. Sei nun $y' \in G$ mit $y'x = e$. Dann ist $y' = y'e = y'(xy) = (y'x)y = ey = y$. Somit hat x genau ein Inverses und wir schreiben $y = x^{-1}$. Offenbar ist $(x^{-1})^{-1} = y^{-1} = z = x$.

(iii) Für $x, y \in G$ ist $(xy)^{-1} = y^{-1}x^{-1}$.

(iv) Für $x \in G$ und $k \in \mathbb{Z}$ definieren wir

$$x^k := \begin{cases} 1_G & \text{falls } k = 0, \\ x \dots x \text{ (k Faktoren)} & \text{falls } k > 0, \\ (x^{-1})^{-k} & \text{falls } k < 0. \end{cases}$$

Sicher ist dann $x^m x^n = x^{m+n}$ und $(x^m)^n = x^{mn}$ für $n, m \in \mathbb{Z}$. Man nennt $\inf\{n \geq 1 : x^n = 1\}$ die *Ordnung* von x. Dabei sei $\inf \varnothing = \infty$. Besteht G aus Potenzen von x, so heißt G *zyklisch*.

Beispiel 1.3.

(i) Die *triviale* Gruppe $G = \{1\}$. Wir schreiben dann auch $G = 1$.

(ii) Die ganzen Zahlen $\mathbb{Z}$ bilden bzgl. Addition eine abelsche Gruppe. Das neutrale Element ist dabei 0. Dagegen ist $\mathbb{Z}$ bzgl. Multiplikation *keine* Gruppe.

(iii) Die invertierbaren $n \times n$-Matrizen über einen Körper K bilden bzgl. Matrizenmultiplikation die *allgemeine lineare Gruppe* $\mathrm{GL}(n, K)$. Das neutrale Element ist die Einheitsmatrix 1_n. Es gilt $\mathrm{GL}(1, K) = K^\times = K \setminus \{0\}$. Für $n \geq 2$ ist $\mathrm{GL}(n, K)$ nichtabelsch.

(iv) Die Bijektionen einer Menge Ω bilden bzgl. Komposition von Abbildungen die *symmetrische Gruppe* $\mathrm{Sym}(\Omega)$ mit neutralem Element id_Ω. Die Elemente von $\mathrm{Sym}(\Omega)$ heißen *Permutationen*. Für $\Omega = \{1, \ldots, n\}$ schreiben wir $S_n := \mathrm{Sym}(\Omega)$. Es gilt dann $|S_n| = n!$.

(v) Für jede nichtleere Familie von Gruppen $(G_i)_{i \in I}$ ist das *direkte Produkt* $\times_{i \in I} G_i$ eine Gruppe mit $(g_i)_{i \in I}(h_i)_{i \in I} := (g_i h_i)_{i \in I}$ für $(g_i)_{i \in I}, (h_i)_{i \in I} \in \times_{i \in I} G_i$. Für $I = \{1, \ldots, n\}$ schreibt man auch $G_1 \times \ldots \times G_n$ und G^n, falls $G := G_1 = \ldots = G_n$.

Definition 1.4. Eine nichtleere Teilmenge $H \subseteq G$ mit $xy^{-1} \in H$ für $x, y \in H$ heißt *Untergruppe* von G. Wir schreiben dann $H \leq G$ und $H < G$, falls $H \neq G$. Die Mengen der Form $gH := \{gh : h \in H\}$ nennt man *(Links)nebenklassen* von H in G. Die Menge aller Linksnebenklassen ist $G/H := \{gH : g \in G\}$ und $|G : H| := |G/H|$ ist der *Index* von H in G.

Bemerkung 1.5. Man zeigt leicht, dass dann H mit der eingeschränkten Verknüpfung ebenfalls eine Gruppe ist. Ist G abelsch, so auch H. Ist $K \leq H$, so gilt auch $K \leq G$.

Beispiel 1.6.

(i) Jede Gruppe G besitzt die Untergruppen 1 und G. Eine Untergruppe $H < G$ heißt *maximal*, falls keine Untergruppe K mit $H < K < G$ existiert. Analog definiert man *minimale* Untergruppen.

(ii) Für $H_i \leq G$ ist $\bigcap_{i \in I} H_i \leq G$.

(iii) Für $U \subseteq G$ ist

$$\langle U \rangle := \bigcap_{U \subseteq H \leq G} H$$

die von U *erzeugte* Untergruppe. Offenbar besteht $\langle U \rangle$ aus den Elementen der Form $x_1^{\pm 1} \ldots x_n^{\pm 1}$ mit $x_1, \ldots, x_n \in U$. Im Fall $\langle U \rangle = G$ ist U ein *Erzeugendensystem* von G. Ist zusätzlich $U = \{x_1, \ldots, x_n\}$, so schreibt man $G = \langle x_1, \ldots, x_n \rangle$ statt $\langle U \rangle$. In diesem Fall ist G *endlich erzeugt*. Ist $|U| \leq 1$, so ist G zyklisch. Im Allgemeinen ist $|\langle x \rangle|$ die Ordnung von x.

(iv) Für $n \in \mathbb{Z}$ ist $n\mathbb{Z} \leq \mathbb{Z}$.

(v) Nach Algebra ist jede endliche Untergruppe von $\mathbb{C}^\times$ zyklisch. Für $n \in \mathbb{N}$ ist $\{e^{2\pi i k/n} \in \mathbb{C} : k \in \mathbb{Z}\} \leq \mathbb{C}^\times$ die einzige Untergruppe der Ordnung n, da es nur n Einheitswurzeln der Ordnung n gibt.

(vi) Die *spezielle lineare Gruppe* ist $\mathrm{SL}(n, K) := \{A \in \mathrm{GL}(n, K) : \det(A) = 1\} \leq \mathrm{GL}(n, K)$.

(vii) Die *alternierende Gruppe* $\mathrm{Alt}(\Omega) := \{\sigma \in \mathrm{Sym}(\Omega) : \mathrm{sgn}(\sigma) = 1\} \leq \mathrm{Sym}(\Omega)$ für eine nichtleere, endliche Menge Ω. Wir setzen $A_n := \mathrm{Alt}(\{1, \ldots, n\})$ für $n \geq 1$.

Satz 1.7 (Lagrange). *Für eine Gruppe G und $H \leq G$ gilt*

$$\boxed{|G| = |G : H||H|.}$$

Insbesondere sind $|H|$ und $|G : H|$ Teiler von $|G|$, falls $|G| < \infty$.

Beweis. Algebra. □

Definition 1.8. Für $X, Y \subseteq G$ sei $XY := \{xy : x \in X, y \in Y\}$ und $X^{-1} := \{x^{-1} : x \in X\}$.

Lemma 1.9. *Für $U, V, W \leq G$ gilt*

(i) $U \subseteq V \Longrightarrow |G : U| = |G : V||V : U|$.

(ii) $UV \leq G \Longleftrightarrow UV = VU$.

(iii) $|UV| = |U : U \cap V||V| = |V : U \cap V||U|$.

(iv) $U \subseteq W \Longrightarrow UV \cap W = U(V \cap W)$ *(*Dedekind*-Identität).*

(v) Sind $|G : U|$ und $|G : V|$ endlich und teilerfremd, so ist $|G : U \cap V| = |G : U||G : V|$ und $G = UV$.

Beweis. Aufgabe 2. □

Definition 1.10. Eine Untergruppe $H \leq G$ heißt *Normalteiler* von G, falls $ghg^{-1} \in H$ für alle $g \in G$ und $h \in H$ gilt. Man sagt auch: H ist *normal* in G. In diesem Fall schreiben wir $H \trianglelefteq G$ und $H \triangleleft G$, falls $H < G$.

Bemerkung 1.11.

(i) Genau dann ist $H \leq G$ normal, wenn $gH = Hg$ für alle $g \in G$ gilt.

(ii) Für $N \trianglelefteq G$ wird G/N mittels $(xN)(yN) := xyN$ für $x, y \in G$ zu einer Gruppe. Man nennt dann G/N die *Faktorgruppe* von G nach N (obwohl „Quotientengruppe“ passender wäre). Ist G abelsch, so auch G/N. Die Gleichheit $xN = yN$ schreiben wir auch in der Form $x \equiv y \pmod{N}$.

Beispiel 1.12.

(i) Untergruppen von abelschen Gruppen sind stets normal. Insbesondere ist $n\mathbb{Z} \trianglelefteq \mathbb{Z}$ und $\mathbb{Z}/n\mathbb{Z}$ ist zyklisch der Ordnung n, falls $n > 0$.

(ii) Untergruppen mit Index 2 sind normal (Aufgabe 1).

(iii) Für $H \leq G$ ist $\langle gHg^{-1} : g \in G\rangle$ der „kleinste“ Normalteiler von G, der H enthält. Analog ist $\bigcap_{g\in G} gHg^{-1}$ der „größte“ Normalteiler von G, der in H enthalten ist.

(iv) Für jede Familie von Normalteilern $(N_i)_{i\in I}$ von G ist $\bigcap_{i\in I} N_i \trianglelefteq G$ und $\langle N_i : i \in I\rangle \trianglelefteq G$. Insbesondere ist $NM \trianglelefteq G$ für $N, M \trianglelefteq G$.

Definition 1.13. Eine Abbildung $f : G \to H$ für Gruppen G und H heißt

(i) *Homomorphismus*, falls $f(xy) = f(x)f(y)$ für $x, y \in G$ gilt.

(ii) *Monomorphismus*, falls f ein injektiver Homomorphismus ist.

(iii) *Epimorphismus*, falls f ein surjektiver Homomorphismus ist.

(iv) *Isomorphismus*, falls f ein bijektiver Homomorphismus ist.

(v) *Endomorphismus*, falls f ein Homomorphismus mit $G = H$ ist.

(vi) *Automorphismus*, falls f ein bijektiver Endomorphismus ist.

Bemerkung 1.14.

(i) Für einen Homomorphismus $f : G \to H$ gilt offenbar $f(1_G) = 1_H$ und $f(x^{-1}) = f(x)^{-1}$ für $x \in G$. Ist $g : H \to K$ ein weiterer Homomorphismus, so ist auch $g \circ f : G \to K$ ein Homomorphismus. Für $U \leq G$ (bzw. $U \trianglelefteq G$) und $V \leq H$ (bzw. $V \trianglelefteq H$) ist außerdem $f(U) \leq H$ (bzw. $f(U) \trianglelefteq f(G)$) und $f^{-1}(V) := \{x \in G : f(x) \in V\} \leq G$ (bzw. $f^{-1}(V) \trianglelefteq G$). Insbesondere ist $f(G) \leq H$ und $\mathrm{Ker}(f) = f^{-1}(1) \leq G$. Genau dann ist f injektiv, wenn $\mathrm{Ker}(f) = 1$ gilt.

(ii) Ist $f : G \to H$ ein Isomorphismus, so auch $f^{-1} : H \to G$. Man sagt dann G und H sind *isomorph* und schreibt $G \cong H$. Offenbar ist die Isomorphie von Gruppen eine Äquivalenzrelation. Da isomorphe Gruppen die gleichen Eigenschaften haben, interessiert man sich in der Regel nur für Gruppen bis auf Isomorphie.

(iii) Nach (ii) bilden die Automorphismen von G eine Untergruppe $\mathrm{Aut}(G) \leq \mathrm{Sym}(G)$. Man nennt $\mathrm{Aut}(G)$ die *Automorphismengruppe* von G. Für $x \in G$ ist die Abbildung $f_x : G \to G$, $g \mapsto xgx^{-1}$ ein *innerer* Automorphismus von G. Wegen $f_x \circ f_y = f_{xy}$ für $x, y \in G$ ist $f : G \to \mathrm{Aut}(G)$, $x \mapsto f_x$ ein Homomorphismus mit Bild $\mathrm{Inn}(G) := f(G)$. Für $\alpha \in \mathrm{Aut}(G)$ gilt $(\alpha \circ f_x \circ \alpha^{-1})^{-1}(g) = \alpha(x\alpha^{-1}(g)x^{-1}) = \alpha(x)g\alpha(x)^{-1} = f_{\alpha(x)}(g)$. Daher ist $\mathrm{Inn}(G) \trianglelefteq \mathrm{Aut}(G)$. Man nennt $\mathrm{Out}(G) := \mathrm{Aut}(G)/\mathrm{Inn}(G)$ die *äußere* Automorphismengruppe von G.

(iv) Für $N \trianglelefteq G$ gibt es den *kanonischen* Epimorphismus $G \to G/N$, $g \mapsto gN$ mit Kern N.

Satz 1.15.

(i) (Homomorphiesatz) Für einen Homomorphismus $f : G \to H$ gilt $G/\mathrm{Ker}(f) \cong f(G)$.

(ii) (Korrespondenzsatz) Für $N \trianglelefteq G$ induziert der kanonische Epimorphismus $G \to G/N$ eine Bijektion zwischen der Menge der Untergruppen $H \leq G$ mit $N \leq H$ und der Menge der Untergruppen von G/N.

(iii) (1. Isomorphiesatz) Für $H \leq G$ und $N \trianglelefteq G$ gilt $N \trianglelefteq HN \leq G$, $H \cap N \trianglelefteq H$ und $HN/N \cong H/H \cap N$.

(iv) (2. Isomorphiesatz) Für $N \trianglelefteq G$ und $N \leq H \leq G$ ist $H \trianglelefteq G$ genau dann wenn $H/N \trianglelefteq G/N$. Ggf. ist $G/H \cong (G/N)/(H/N)$.

Beweis. Algebra. □

Definition 1.16. Eine *Operation* (engl. *action*) von G auf einer nichtleeren Menge Ω ist eine Abbildung $G \times \Omega \to \Omega$, $(x, \omega) \mapsto {}^x\omega$ mit folgenden Eigenschaften:

- $\forall \omega \in \Omega : {}^1\omega = \omega$.
- $\forall x, y \in G, \omega \in \Omega : {}^x({}^y\omega) = {}^{xy}\omega$.

Man sagt dann auch G operiert auf Ω oder Ω ist eine G-Menge. Die Mächtigkeit $|\Omega|$ ist der *Grad* der Operation. Sofern die Operation im Kontext klar ist, werden wir im Folgenden manchmal Eigenschaften von Operationen auch den entsprechenden Gruppen zuordnen (z. B. der Grad von G).

Bemerkung 1.17.

(i) Operiert G auf Ω, so ist die Abbildung $f_x : \Omega \to \Omega$, $\omega \mapsto {}^x\omega$ für $x \in G$ eine Bijektion, d. h. $f_x \in \mathrm{Sym}(\Omega)$. Außerdem ist die Abbildung $f : G \to \mathrm{Sym}(\Omega)$, $x \mapsto f_x$ ein Homomorphismus.

Sei nun umgekehrt ein Homomorphismus $f : G \to \mathrm{Sym}(\Omega)$ gegeben. Dann erhält man durch ${}^x\omega := (f(x))(\omega)$ offenbar eine Operation. Operationen sind also nichts anderes als Homomorphismen

in die symmetrische Gruppe. Die Operation heißt *treu* (bzw. *trivial*), falls $\operatorname{Ker}(f) = 1$ (bzw. $\operatorname{Ker}(f) = G$) gilt.

(ii) Durch
$$\alpha \sim \beta :\Longleftrightarrow \exists x \in G : {}^x\alpha = \beta \qquad (\alpha, \beta \in \Omega)$$
erhält man eine Äquivalenzrelation auf Ω. Die Äquivalenzklassen heißen *Bahnen* (engl. *orbits*). Für eine Bahn $\Delta \subseteq \Omega$ ist $|\Delta|$ die *Länge* von Δ. Für $\omega \in \Omega$ sei ${}^G\omega$ die Bahn, die ω enthält. Existiert nur eine Bahn, so ist die Operation *transitiv*.

(iii) Für $\omega \in \Omega$ ist $G_\omega := \{x \in G : {}^x\omega = \omega\} \leq G$ der *Stabilisator* von ω in G. Für $g \in G$ gilt dabei
$$G_{{}^g\omega} = \{x \in G : {}^{xg}\omega = {}^g\omega\} = \{x \in G : g^{-1}xg \in G_\omega\} = gG_\omega g^{-1}.$$

Beispiel 1.18.

(i) Jede Untergruppe $H \leq G$ operiert auf G durch Linksmultiplikation, d. h. ${}^hg := hg$ für $g \in G$, $h \in H$. Die Bahnen Hg heißen *Rechtsnebenklassen*. Analog operiert H von rechts durch ${}^hg := gh^{-1}$ und man erhält Linksnebenklassen gH.

(ii) G operiert auf sich selbst durch *Konjugation* ${}^xg := xgx^{-1}$ für $x, g \in G$. Die Bahnen heißen dabei *Konjugationsklassen* und der Stabilisator von $x \in G$ ist der *Zentralisator* $\mathrm{C}_G(x) := \{g \in G : gx = xg\}$. Zwei Elemente in der gleichen Konjugationsklasse nennt man *konjugiert*. Der Kern der Operation ist das *Zentrum* $\mathrm{Z}(G) := \{x \in G : \forall y \in G : xy = yx\}$ von G und das Bild ist $\operatorname{Inn}(G)$. Nach dem Homomorphiesatz ist
$$G/\mathrm{Z}(G) \cong \operatorname{Inn}(G) \leq \operatorname{Aut}(G) \leq \operatorname{Sym}(G).$$

(iii) Analog operiert G durch Konjugation auf der Menge der Untergruppen von G. Die Bahnen heißen auch hier Konjugationsklassen und der Stabilisator von $H \leq G$ ist der *Normalisator* $\mathrm{N}_G(H) := \{x \in G : xHx^{-1} = H\}$. Die Bahnen der Länge 1 entsprechen den Normalteilern. Allgemeiner operiert $\mathrm{N}_G(X)$ durch Konjugation auf X mit Kern $\mathrm{C}_G(X) := \bigcap_{x \in X} \mathrm{C}_G(x)$. Insbesondere ist $\mathrm{N}_G(X)/\mathrm{C}_G(X)$ zu einer Untergruppe von $\operatorname{Aut}(X)$ isomorph.

Satz 1.19. *Für eine Operation von G auf Ω und $\omega \in \Omega$ ist die Abbildung $G/G_\omega \to {}^G\omega$, $xG_\omega \mapsto {}^x\omega$ wohldefiniert und bijektiv. Insbesondere ist $|G/G_\omega| = |{}^G\omega|$. Ist $|G| < \infty$, so ist also jede Bahnenlänge ein Teiler von $|G|$. Ist G zusätzlich transitiv, so ist $|\Omega| \mid |G|$.*

Beweis. Wohldefiniertheit und Injektivität:
$$xG_\omega = yG_\omega \Longleftrightarrow y^{-1}x \in G_\omega \Longleftrightarrow {}^{y^{-1}x}\omega = \omega \Longleftrightarrow {}^x\omega = {}^y({}^{y^{-1}x}\omega) = {}^y\omega.$$
Die Surjektivität ist offensichtlich. Die letzten beiden Aussagen folgen nach Lagrange. □

Bemerkung 1.20. Sind $(\omega_i)_{i \in I}$ Repräsentanten für die Bahnen von G auf Ω, so gilt die *Bahnengleichung*
$$|\Omega| = \sum_{i \in I} |{}^G\omega_i| = \sum_{i \in I} |G : G_{\omega_i}|.$$
Im Spezialfall der Konjugationsoperation erhält man die *Klassengleichung*
$$|G| = \sum_{i \in I} |G : \mathrm{C}_G(x_i)|,$$

wobei $(x_i)_{i\in I}$ ein Repräsentantensystem für die Konjugationsklassen von G ist. Ist $J := \{i \in I : x_i \notin \mathrm{Z}(G)\}$, so gilt auch

$$|G| = |\mathrm{Z}(G)| + \sum_{j\in J} |G : \mathrm{C}_G(x_j)|.$$

Satz 1.21 (Frattini-Argument)**.** *Gegeben sei eine Operation von G auf Ω und $H \leq G$. Operiert H transitiv auf Ω, so gilt $G = HG_\omega$ für alle $\omega \in \Omega$.*

Beweis. Sei $g \in G$ beliebig. Dann existiert ein $h \in H$ mit ${}^g\omega = {}^h\omega$. Also ist $h^{-1}g \in G_\omega$ und $g = h(h^{-1}g) \in HG_\omega$. Umgekehrt ist sicher auch $HG_\omega \subseteq G$. □

Bemerkung 1.22. Hat jedes nicht-triviale Element in G unendliche Ordnung, so heißt G *torsionsfrei*. Hat hingegen jedes Element endliche Ordnung, so ist G eine *Torsionsgruppe*. Sind die Ordnungen der Elemente beschränkt, so ist G *periodisch* und $\exp(G) := \min\{k \geq 1 : \forall x \in G : x^k = 1\}$ ist der *Exponent* von G. Burnside hat 1902 gefragt, ob jede endlich erzeugte periodische Gruppe endlich ist (*Burnside Problem*). Man weiß heute, dass dies im Allgemeinen falsch ist. Andererseits weiß man nicht, ob jede Gruppe mit zwei Erzeugern und Exponent 5 endlich ist.

2 Abelsche und auflösbare Gruppen

Lemma 2.1. *Sei $x \in G$ mit $n := |\langle x \rangle| < \infty$. Dann ist*

$$|\langle x^k \rangle| = \frac{n}{\mathrm{ggT}(n,k)}$$

für $k \in \mathbb{Z}$. Insbesondere ist $x^k = 1$ genau dann, wenn $n \mid k$. Für $y \in \mathrm{C}_G(x)$ mit $m := |\langle y \rangle| < \infty$ und $\mathrm{ggT}(n,m) = 1$ gilt $|\langle xy \rangle| = mn$.

Beweis. Für $l := \frac{n}{\mathrm{ggT}(n,k)} \geq 1$ gilt $(x^k)^l = (x^n)^{\frac{k}{\mathrm{ggT}(n,k)}} = 1$. Also ist $s := |\langle x^k \rangle| \leq l$. Umgekehrt ist $x^{ks} = 1$. Division mit Rest liefert $a \in \mathbb{Z}$ und $0 \leq r < n$ mit $ks = an + r$. Es folgt $x^r = x^r(x^n)^a = x^{an+r} = x^{ks} = 1$ und $r = 0$. Also ist $n \mid ks$ und $s \geq l$.

Dies impliziert

$$x^k = 1 \iff n = \mathrm{ggT}(n,k) \iff k \mid n.$$

Sei nun $y \in \mathrm{C}_G(x)$ wie angegeben. Wegen $xy = yx$ ist $\langle xy \rangle \subseteq \langle x, y \rangle = \langle x \rangle \langle y \rangle$. Nach dem euklidischen Algorithmus existieren $\alpha, \beta \in \mathbb{Z}$ mit $\alpha n + \beta m = 1$. Es gilt dann $x = x^{\alpha n + \beta m} = x^{\alpha n} x^{\beta m} = x^{\beta m} = x^{\beta m} y^{\beta m} = (xy)^{\beta m} \in \langle xy \rangle$ und analog $y \in \langle xy \rangle$. Dies zeigt $\langle xy \rangle = \langle y \rangle \langle y \rangle$. Nach Lagrange ist $|\langle x \rangle \cap \langle y \rangle| \mid \mathrm{ggT}(n,m) = 1$. Lemma 1.9 zeigt daher $|\langle x \rangle \langle y \rangle| = nm$. □

Definition 2.2. Wir bezeichnen eine zyklische Gruppe der Ordnung $n \in \mathbb{N} \cup \{\infty\}$ mit C_n.

Bemerkung 2.3.

(i) Für $G = \langle g \rangle \cong C_n$ ist die Abbildung $\mathbb{Z} \to G$, $i \mapsto g^i$ ein Epimorphismus mit Kern $n\mathbb{Z}$ nach Lemma 2.1. Dies zeigt $C_n \cong \mathbb{Z}/n\mathbb{Z}$ und $C_\infty \cong \mathbb{Z}$.

(ii) Aus Lemma 2.1 folgt $C_n \times C_m \cong C_{nm}$, falls $\mathrm{ggT}(n,m) = 1$ (*Chinesischer Restsatz*).

Satz 2.4.

(i) Für jedes $d \mid n$ besitzt C_n genau eine Untergruppe (bzw. Faktorgruppe) der Ordnung d. Diese ist zu C_d isomorph.

(ii) $\mathrm{Aut}(C_n) \cong (\mathbb{Z}/n\mathbb{Z})^\times$. Insbesondere ist $\mathrm{Aut}(C_n)$ abelsch der Ordnung $\varphi(n)$.

Beweis. Sei $\langle x \rangle \cong C_n$.

(i) Für $d \mid n$ ist $\langle x^{n/d} \rangle$ eine Untergruppe der Ordnung d nach Lemma 2.1. Sei umgekehrt $H \leq \langle x \rangle$ mit $1 < d = |H| \,\big|\, n$. Sei $i \geq 1$ minimal mit $x^i \in H$. Sei $x^j \in H$ beliebig. Division mit Rest liefert dann $j = ai + r$ mit $a \in \mathbb{Z}$ und $0 \leq r < i$. Es gilt $x^r = x^{j-ai} = x^j (x^i)^{-a} \in H$ und die Wahl von i zeigt $r = 0$. Also ist $i \mid j$ und $H = \langle x^i \rangle$. Nach Lemma 2.1 ist $\mathrm{ggT}(i,n) = \frac{n}{d}$. Es folgt $x^i \in \langle x^{n/d} \rangle$ und $H = \langle x^{n/d} \rangle$. Wegen $\langle x \rangle / H = \langle xH \rangle \cong C_{n/d}$ ist auch die Behauptung über Faktorgruppen klar.

(ii) Für $\alpha \in \mathrm{Aut}(\langle x\rangle)$ ist $\alpha(x) = x^i$ mit $i \in \mathbb{Z}$. Im Fall $\mathrm{ggT}(n,i) > 1$ wäre $\langle x^i\rangle < \langle x\rangle$ nach Lemma 2.1. Man erhält somit eine Abbildung $\Phi : \mathrm{Aut}(\langle x\rangle) \to (\mathbb{Z}/n\mathbb{Z})^\times$, $\alpha \mapsto i + n\mathbb{Z}$. Für $\beta \in \mathrm{Aut}(\langle x\rangle)$ mit $\beta(x) = x^j$ gilt $\alpha(\beta(x)) = \alpha(x^j) = \alpha(x)^j = x^{ij}$. Dies zeigt, dass Φ ein Homomorphismus ist. Gilt $i + n\mathbb{Z} = 1 + n\mathbb{Z}$, so ist $\alpha(x) = x^i = x$ und $\alpha = 1$. Also ist Φ injektiv. Hat man umgekehrt $i + n\mathbb{Z} \in (\mathbb{Z}/n\mathbb{Z})^\times$ gegeben, so sieht man leicht, dass die Abbildung $x \mapsto x^i$ ein Automorphismus von $\langle x\rangle$ induziert. Also ist Φ ein Isomorphismus. □

Lemma 2.5. *Für $N, M \trianglelefteq G$ mit $N \cap M = 1$ gilt $xy = yx$ für alle $x \in N$ und $y \in M$. Dies gilt insbesondere, wenn* $\mathrm{ggT}(|N|, |M|) = 1$.

Beweis. Für $x \in N$ und $y \in M$ gilt

$$\underbrace{\overbrace{xyx^{-1}}^{\in N}y^{-1}}_{\in M} \in N \cap M = 1,$$

d. h. $xy = yx$. Nach Lagrange ist $|N \cap M|$ ein Teiler von $\mathrm{ggT}(|N|, |M|)$. Daher folgt die zweite Aussage aus der ersten. □

Definition 2.6. Man nennt G eine *direkte Summe* von Normalteilern $N_1, \ldots, N_k \trianglelefteq G$, falls folgende Aussagen gelten:

- $G = N_1 \ldots N_k$.
- $N_i \cap N_1 \ldots N_{i-1} = 1$ für $i = 2, \ldots, k$.

Wir schreiben in diesem Fall $G = N_1 \oplus \ldots \oplus N_k$.

Lemma 2.7. *Es gilt $N_1 \oplus \ldots \oplus N_k \cong N_1 \times \ldots \times N_k$.*

Beweis. Wir zeigen, dass die Abbildung

$$\begin{aligned} F : N_1 \times \ldots \times N_k &\to G, \\ (x_1, \ldots, x_k) &\mapsto x_1 \ldots x_k \end{aligned}$$

ein Isomorphismus ist. Nach Voraussetzung gilt $N_i \cap N_j \subseteq N_i \cap \prod_{l \neq i} N_l = 1$ für $i \neq j$. Lemma 2.5 zeigt $xy = yx$ für $x \in N_i$ und $y \in N_j$. Seien nun $x_i, y_i \in N_i$ für $i = 1, \ldots, k$. Dann gilt

$$F(x_1, \ldots, x_k)F(y_1, \ldots, y_k) = x_1 \ldots x_k y_1 \ldots y_k = x_1 y_1 x_2 y_2 \ldots x_k y_k = F((x_1, \ldots, x_k)(y_1, \ldots, y_k)).$$

Also ist F ein Homomorphismus. Wegen $G = N_1 \ldots N_k$ ist F surjektiv. Für $x_1 \ldots x_k = y_1 \ldots y_k$ gilt

$$y_1^{-1}x_1 = y_2 x_2^{-1} \ldots y_k x_k^{-1} \in N_1 \cap \prod_{i=2}^{k} N_i = 1,$$

d h. $x_1 = y_1$ und $x_2 \ldots x_k = y_2 \ldots y_k$. Induktiv folgt leicht $x_i = y_i$ für $i = 1, \ldots, k$. Damit ist F auch injektiv. □

Beispiel 2.8. Sei G eine Gruppe der Ordnung 15. Nach Sylow besitzt G eine normale 3-Sylowgruppe N und eine normale 5-Sylowgruppe M. Wegen $\mathrm{ggT}(3,5) = 1$ ist $G = N \oplus M \cong N \times M \cong C_3 \times C_5 \cong C_{15}$.

Bemerkung 2.9. Offenbar ist $G_1 \oplus G_2 = G_2 \oplus G_1$. Sei nun $G = G_1 \oplus G_2 \oplus G_3$. Dann ist sicher $G_1G_2 = G_1 \oplus G_2 \trianglelefteq G$ und $G = (G_1 \oplus G_2) \oplus G_3$. Sei nun umgekehrt $G = (G_1 \oplus G_2) \oplus G_3$. Dann ist $G_3 \subseteq \mathrm{C}_G(G_1G_2)$. Dies zeigt $G_1, G_2 \trianglelefteq G$ und $G = G_1 \oplus G_2 \oplus G_3$. Direkte Summen sind also kommutativ und assoziativ.

Satz 2.10 (Hauptsatz über endlich erzeugte abelsche Gruppen)**.** *Für eine endlich erzeugte abelsche Gruppe G gilt:*

(i) Es existieren eindeutig bestimmte Zahlen $s, t \geq 0$ und $d_1 \mid \ldots \mid d_t$ mit

$$G \cong C_\infty^s \times C_{d_1} \times \ldots \times C_{d_t}.$$

(ii) Es existieren eindeutig bestimmte Primzahlpotenzen $p_1^{a_1}, \ldots, p_t^{a_t}$ und ein $s \geq 0$ mit

$$G \cong C_\infty^s \times C_{p_1^{a_1}} \times \ldots \times C_{p_t^{a_t}}.$$

Beweis.

(i) **Schritt 1:** Existenz.
Wir wählen ein minimales Erzeugendensystem $x_1, \ldots, x_r$, d.h. G lässt sich nicht durch $r-1$ Elemente erzeugen. Da G abelsch ist, kann man jedes $g \in G$ in der Form $g = x_1^{n_1}x_2^{n_2}\ldots x_r^{n_r}$ mit $n_1, \ldots, n_r \in \mathbb{Z}$ schreiben. Eine Gleichung der Form $x_1^{n_1}x_2^{n_2}\ldots x_r^{n_r} = 1$ nennt man *Relation*. Gibt es nur die triviale Relation mit $n_1 = \ldots = n_r = 0$, so wird der Homomorphismus $\mathbb{Z}^r \to G$, $(n_1, \ldots, n_r) \mapsto x_1^{n_1}x_2^{n_2}\ldots x_r^{n_r}$ injektiv. Offenbar ist er auch surjektiv, und wir sehen, dass G isomorph zu C_∞^r ist.

Nehmen wir nun an, dass auch nicht-triviale Relationen existieren. Wir wählen nun $x_1, \ldots, x_r$ unter allen minimalen Erzeugendensystemen so, dass eine Relation mit minimalem positivem Exponenten gilt. O.B.d.A. sei m_1 dieser minimale Exponent, und es gelte die Relation $x_1^{m_1}x_2^{n_2}\ldots x_r^{n_r} = 1$. Wir zeigen $m_1 \mid n_2$. Division mit Rest ergibt zunächst $n_2 = qm_1 + u$ mit $0 \leq u < m_1$, und die Relation wird zu

$$1 = x_1^{m_1}x_2^{qm_1+u}\ldots x_r^{n_r} = (x_1x_2^q)^{m_1}x_2^u x_3^{n_3}\ldots x_r^{n_r}. \tag{2.1}$$

Da man jedes Element $x_1^{l_1}\ldots x_r^{l_r}$ auch in der Form $(x_1x_2^q)^{l_1}x_2^{l_2-ql_1}x_3^{l_3}\ldots x_r^{l_r}$ schreiben kann, ist $x_1x_2^q, x_2, \ldots, x_r$ ebenfalls ein minimales Erzeugendensystem. Aus der Wahl von m_1 sowie (2.1) folgt $u = 0$ und damit $m_1 \mid n_2$. Analog zeigt man $m_1 \mid n_3, \ldots, m_1 \mid n_r$, und wir können $n_i = q_im_1$ für $i = 3, \ldots, r$ schreiben. Setzt man nun $z := x_1x_2^qx_3^{q_3}\ldots x_r^{q_r}$, so ist $z, x_2, \ldots, x_r$ wieder ein minimales Erzeugendensystem, und die Relation wird zu $1 = z^{m_1}$. Damit hat z die Ordnung m_1, denn wäre $1 = z^l = z^lx_2^0\ldots x_r^0$ mit $0 < l < m_1$, so hätten wir einen Widerspruch zur Wahl vom m_1. Setzt man nun $H := \langle z\rangle$ und $G_1 := \langle x_2, \ldots, x_r\rangle$, so folgt $G = HG_1$. Im Fall $H \cap G_1 \neq 1$ gäbe es $l_1, \ldots, l_r \in \mathbb{Z}$ mit $1 \neq z^{l_1} = x_2^{l_2}\ldots x_r^{l_r}$ und $0 < l_1 < m_1$. Dann wäre aber $z^{l_1}x_2^{-l_2}\ldots x_r^{-l_r} = 1$ ein Widerspruch zur Wahl von m_1. Folglich ist $H \cap G_1 = 1$ und $G = H \oplus G_1 \cong H \times G_1 \cong C_{m_1} \times G_1$.

Nun kann man den Prozess mit G_1 wiederholen und es gibt die Möglichkeiten $G_1 \cong C_\infty^{r-1}$ oder $G_1 \cong C_{m_2} \times G_2$. Im ersten Fall ist dann $G \cong C_\infty^{r-1} \times C_{m_1}$, und wir sind fertig. Im zweiten Fall ist $G \cong C_{m_1} \times C_{m_2} \times G_2$, wobei m_2 als Exponent einer Relation $y_2^{m_2}y_3^{n_3'}\ldots y_r^{n_r'} = 1$ mit einem minimalen Erzeugendensystem $y_2, \ldots, y_r$ von G_1 auftritt. Nun ist $z, y_2, \ldots, y_r$ offenbar ein minimales Erzeugendensystem von G, und es gilt die Relation $z^{m_1}y_2^{m_2}y_3^{n_3'}\ldots y_r^{n_r'} = 1$. Wie oben zeigt man dann $m_1 \mid m_2$. Man iteriert nun den Prozess mit G_2. Da in jedem Schritt die (endliche) Zahl der Erzeuger um eins reduziert wird, muss der Prozess terminieren, und am Ende die gewünschte Form von G liefern.

Schritt 2: Eindeutigkeit.
Sei $C_\infty^s \times C_{d_1} \times \ldots \times C_{d_t} \cong G \cong C_\infty^{s'} \times C_{e_1} \times \ldots \times C_{e_{t'}}$ mit $d_1 \mid \ldots \mid d_t$ und $e_1 \mid \ldots \mid e_{t'}$. Die Elemente endlicher Ordnung bilden eine Untergruppe $H \leq G$ mit $C_{d_1} \times \ldots \times C_{d_t} \cong H \cong C_{e_1} \times \ldots \times C_{e_{t'}}$. O. B. d. A. sei $t \geq t'$. Wir argumentieren durch Induktion nach $|H|$. Sei $K := \{x \in H : x^{d_1} = 1\} \leq H$. Dann ist $K \cong C_{d_1}^t$ und wegen $t' \leq t$ folgt $d_1 \mid e_1$. Dies zeigt auch $t = t'$. Nun ist $C_{\frac{d_2}{d_1}} \times \ldots \times C_{\frac{d_t}{d_1}} \cong H/K \cong C_{\frac{e_1}{d_1}} \times \ldots \times C_{\frac{e_{t'}}{d_1}}$. Induktion liefert $d_i = e_i$ für $i = 1, \ldots, t$. Wir betrachten nun $C_\infty^s \cong G/H \cong C_\infty^{s'}$. Für $\overline{G} := G/H$ und $\overline{G}_2 := \{x^2 : x \in \overline{G}\} \leq \overline{G}$ ist $2^s = |\overline{G}/\overline{G}_2| = 2^{s'}$ und $s = s'$.

(ii) Ist $n = p_1^{a_1} \ldots p_k^{a_k}$ die Primfaktorzerlegung von n, so gilt $C_n \cong C_{p_1^{a_1}} \times \ldots \times C_{p_k^{a_k}}$ nach Lemma 2.1. Die Behauptung folgt daher aus (i). □

Beispiel 2.11. Es gilt $C_\infty \times C_2 \times C_6 \times C_{18} \cong C_\infty \times C_2^3 \times C_3 \times C_9$. Andererseits ist $C_4 \ncong C_2^2$.

Definition 2.12.

(i) Die Gruppe C_∞^s heißt *freie abelsche Gruppe* vom Rang s. Offenbar ist diese Gruppe auch torsionsfrei.

(ii) Eine endliche abelsche Gruppe G heißt *elementarabelsch*, falls eine Primzahl p mit $x^p = 1$ für alle $x \in G$ existiert.

Bemerkung 2.13. Nach Satz 2.10 hat jede elementarabelsche Gruppe E die Form C_p^n für eine Primzahl p und $n \geq 0$. Man kann dann E als Vektorraum über $\mathbb{F}_p$ auffassen:

$$\begin{aligned} x + y &:= xy && (x, y \in E), \\ (k + p\mathbb{Z}) \cdot x &:= x^k && (k + p\mathbb{Z} \in \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p,\ x \in E). \end{aligned}$$

Man nennt $n = \dim_{\mathbb{F}_p} E$ den *Rang* von E. Jeder Automorphismus von E ist offenbar auch $\mathbb{F}_p$-linear. Dies zeigt $\mathrm{Aut}(E) \cong \mathrm{GL}(n, p)$.

Definition 2.14. Eine Gruppe $G \neq 1$ heißt *einfach*, falls 1 und G die einzigen Normalteiler von G sind. Eine *Subnormalreihe* σ von G ist eine Folge von Untergruppe $1 = G_0 \trianglelefteq G_1 \trianglelefteq \ldots \trianglelefteq G_k = G$. Dabei ist k die *Länge* von σ. Sind die Faktoren G_i/G_{i-1} für $i = 1, \ldots, k$ einfach, so ist σ eine *Kompositionsreihe*. Sind die Faktoren G_i/G_{i-1} für $i = 1, \ldots, k$ abelsch, so ist G *auflösbar*.

Bemerkung 2.15. Jede endliche Gruppe G besitzt eine Kompositionsreihe: Für $G = 1$ wähle man $k = 0$. Für $G \neq 1$ wähle man einen maximalen Normalteiler $N \lhd G$. Nach dem Korrespondenzsatz ist G/N einfach. Nach Induktion besitzt N eine Kompositionsreihe $1 = N_0 \lhd \ldots N_k = N$. Offenbar ist nun $N_0 \lhd \ldots \lhd N \lhd G$ eine Kompositionsreihe von G.

Satz 2.16 (Jordan-Hölder). *Seien $1 = G_k \trianglelefteq \ldots \trianglelefteq G_0 = G$ und $1 = H_l \trianglelefteq \ldots \trianglelefteq H_0 = G$ Kompositionsreihen von G. Dann ist $k = l$ und es existiert ein $\pi \in S_k$ mit $G_{i-1}/G_i \cong H_{\pi(i)-1}/H_{\pi(i)}$ für $i = 1, \ldots, k$. Man nennt $G_0/G_1, \ldots, G_{k-1}/G_k$ die* Kompositionsfaktoren *von G.*

Beweis. Induktion nach k: Im Fall $k = 0$ ist $G = G_0 = 1 = H_0$ und $l = 0$. Sei also $k \geq 1$. Im Fall $G_1 = H_1$ folgt die Behauptung mit Induktion. Sei also $G_1 \neq H_1$. Wegen $G_1, H_1 \trianglelefteq G$ ist auch $G_1 H_1 = H_1 G_1 \trianglelefteq G$. Da G/G_1 einfach ist, folgt $G = G_1 H_1$. Der erste Isomorphiesatz zeigt

$$G/G_1 = H_1 G_1/G_1 \cong H_1/H_1 \cap G_1, \qquad G/H_1 = G_1 H_1/H_1 \cong G_1/G_1 \cap H_1. \tag{2.2}$$

Sei $1 = K_s \trianglelefteq \ldots \trianglelefteq K_2 = G_1 \cap H_1$ eine beliebige Kompositionsreihe. Nach Induktion sind dann die Kompositionsreihen $G_k \trianglelefteq \ldots \trianglelefteq G_1$ und $K_s \trianglelefteq \ldots \trianglelefteq K_2 \trianglelefteq G_1$ gleich lang (d. h. $k = s$) und ihre Faktoren sind (bis auf die Reihenfolge) isomorph. Nun sind auch die Kompositionsreihen $1 = K_k \trianglelefteq \ldots \trianglelefteq K_2 \trianglelefteq H_1$ und $1 = H_l \trianglelefteq \ldots \trianglelefteq H_1$ gleich lang mit isomorphen Faktoren. Also ist $k = s = l$ und nach (2.2) haben die Kompositionsreihen

$$\begin{aligned} &G_k \trianglelefteq \ldots \trianglelefteq G_0, \\ &K_k \trianglelefteq \ldots \trianglelefteq K_2 \trianglelefteq G_1 \trianglelefteq G_0, \\ &K_k \trianglelefteq \ldots \trianglelefteq K_2 \trianglelefteq H_1 \trianglelefteq H_0, \\ &H_k \trianglelefteq \ldots \trianglelefteq H_0 \end{aligned}$$

isomorphe Faktoren. □

Beispiel 2.17.

(i) Sei G eine einfache abelsche Gruppe und $1 \neq x \in G$. Dann ist $\langle x \rangle \trianglelefteq G$ und daher $G = \langle x \rangle$. Außerdem ist $\langle x^k \rangle \trianglelefteq G$ für alle $k \in \mathbb{Z}$. Dies zeigt, dass G Primzahlordnung hat.

(ii) Die Gruppe S_3 besitzt nur eine Kompositionsreihe $1 \lhd A_3 \lhd S_3$.

(iii) C_∞ besitzt keine Kompositionsreihe, denn nach (i) wären die Kompositionsfaktoren endlich.

(iv) Jede abelsche Gruppe G ist auflösbar mittels $1 = G_0 \trianglelefteq G_1 = G$.

(v) Die Kompositionsfaktoren einer endlichen auflösbaren Gruppe haben Primzahlordnung.

(vi) Jede nichtabelsche einfache Gruppe ist nicht auflösbar.

Bemerkung 2.18. Nach Jordan-Hölder sind die einfachen Gruppen die „Primzahlen“ der endlichen Gruppentheorie. Die Klassifikation der endlichen einfachen Gruppen war mit über 10.000 Journalseiten von über 100 Mathematikern eines der größten mathematischen Projekte überhaupt. Erst 2002 wurde die letzte bekannte(!) Lücke im Beweis geschlossen. Um alle endlichen Gruppen zu klassifizieren, muss man Erweiterungen einfacher Gruppen untersuchen. Gibt man sich einfache Gruppen $K_1, \ldots, K_n$ vor, so gibt es beispielsweise stets eine endliche Gruppe mit Kompositionsfaktoren $K_1, \ldots, K_n$, nämlich $K_1 \times \ldots \times K_n$. Andererseits kann es nicht-isomorphe Gruppen mit den gleichen Kompositionsfaktoren geben, zum Beispiel $C_2 \times C_2$ und C_4. Das Erweiterungsproblem ist im Allgemeinen noch ungelöst.

Definition 2.19. Eine *Normalreihe* $\sigma : 1 = G_0 \trianglelefteq G_1 \trianglelefteq \ldots \trianglelefteq G_k = G$ ist eine Subnormalreihe mit $G_i \trianglelefteq G$ für $i = 0, \ldots, k$. Sei zusätzlich $G_0 < \ldots < G_k$. Lässt sich σ nicht weiter verfeinern (d. h. zwischen G_i und G_{i+1} liegen keine Normalteiler von G), so ist σ eine *Hauptreihe*. Analog zu Satz 2.16 zeigt man, dass die Faktoren einer Hauptreihe bis auf Isomorphie und Reihenfolge eindeutig bestimmt sind. Dies sind die *Hauptfaktoren* von G.

Beispiel 2.20. Die Normalreihe $1 \lhd V_4 \lhd A_4$ ist eine Hauptreihe von A_4, aber keine Kompositionsreihe, da $V_4 \cong C_2^2$ nicht einfach ist.

Lemma 2.21. *Sei $H \leq G$ und $N \trianglelefteq G$. Ist G auflösbar, so auch H. Genau dann ist G auflösbar, wenn N und G/N auflösbar sind.*

Beweis. Sei $1 = G_0 \trianglelefteq \ldots \trianglelefteq G_k = G$ mit abelschen Faktoren. Dann ist $1 = G_0 \cap H \trianglelefteq \ldots \trianglelefteq G_k \cap H = H$ mit $G_i \cap H/G_{i-1} \cap H \cong G_{i-1}(G_i \cap H)/G_{i-1} \leq G_i/G_{i-1}$ für $i = 1, \ldots, k$. Also ist auch H auflösbar. Insbesondere ist auch N auflösbar. Außerdem gilt $1 = G_0N/N \trianglelefteq \ldots \trianglelefteq G_kN/N = G/N$ mit $(G_iN/N)/(G_{i-1}N/N) \cong G_iN/G_{i-1}N \cong G_i/G_i \cap G_{i-1}N = G_i/G_{i-1}(G_i \cap N) \cong (G_i/G_{i-1})/(G_{i-1}(G_i \cap N)/G_{i-1})$. Somit ist auch G/N auflösbar.

Nehmen wir umgekehrt an, dass N und G/N auflösbar sind. Dann existieren $1 = N_0 \trianglelefteq \ldots \trianglelefteq N_k = N$ und $1 = G_0/N \trianglelefteq \ldots \trianglelefteq G_l/N = G/N$ mit abelschen Faktoren. Setzt man die Reihen aneinander, so erhält man $1 = N_0 \trianglelefteq \ldots \trianglelefteq N_k = G_0 \trianglelefteq \ldots \trianglelefteq G_l = G$ mit $G_i/G_{i-1} \cong (G_i/N)/(G_{i-1}/N)$. Also sind alle Faktoren dieser Reihe abelsch und G ist auflösbar. □

Beispiel 2.22.

(i) Sind G und H auflösbar, so auch $G \times H$.

(ii) Sind $N, M \trianglelefteq G$ auflösbar, so auch NM, denn $NM/N \cong M/M \cap N$. In einer endlichen Gruppe gibt es daher einen eindeutig bestimmten größten auflösbaren Normalteiler, den man als *auflösbares Radikal* bezeichnet.

Definition 2.23. Eine Untergruppe $H \leq G$ ist *charakteristisch* in G, falls $\alpha(H) = H$ für alle $\alpha \in \mathrm{Aut}(G)$. Eine Gruppe $G \neq 1$ heißt *charakteristisch einfach*, falls 1 und G die einzigen charakteristischen Untergruppen sind.

Beispiel 2.24.

(i) Wegen $\mathrm{Inn}(G) \leq \mathrm{Aut}(G)$ ist jede charakteristische Untergruppe normal.

(ii) Offenbar ist $\mathrm{Z}(G)$ charakteristisch in G (Aufgabe 8).

(iii) In einer zyklischen Gruppe ist nach Satz 2.4 jede Untergruppe charakteristisch (Aufgabe 8).

Lemma 2.25. *Sei H charakteristisch in $N \trianglelefteq G$. Dann ist $H \trianglelefteq G$. Ist zusätzlich N charakteristisch in G, so ist H charakteristisch in G.*

Beweis. Sei $g \in G$. Dann ist $N \to N$, $x \mapsto gxg^{-1}$ ein Automorphismus von N. Also gilt $gHg^{-1} = H$. Sei nun N charakteristisch in G und $\alpha \in \mathrm{Aut}(G)$. Dann ist die Einschränkung von α auf N ein Automorphismus von N. Daher gilt $\alpha(H) = H$. □

Satz 2.26. *Eine endliche Gruppe G ist genau dann charakteristisch einfach, wenn G direkte Summe von isomorphen einfachen Gruppen ist.*

Beweis. Sei zunächst G charakteristisch einfach. Sei N ein minimaler Normalteiler von G. Für $\alpha \in \mathrm{Aut}(G)$ ist dann auch $\alpha(N)$ ein minimaler Normalteiler von G. Sei $\widetilde{N}$ eine möglichst große direkte Summe von Untergruppen der Form $\alpha(N)$ (im Zweifel $\widetilde{N} = N$). Nehmen wir $\alpha(N) \not\subseteq \widetilde{N}$ für ein $\alpha \in \mathrm{Aut}(G)$ an. Wegen $\alpha(N) \cap \widetilde{N} \trianglelefteq N$ folgt $\alpha(N) \cap \widetilde{N} = 1$ aus der Minimalität von $\alpha(N)$. Also ist $\alpha(N)\widetilde{N} = \alpha(N) \oplus \widetilde{N}$ im Widerspruch zur Wahl von $\widetilde{N}$. Dies zeigt $\widetilde{N} = \langle \alpha(N) : \alpha \in \mathrm{Aut}(G) \rangle$. Insbesondere ist $\widetilde{N}$ charakteristisch in G. Da G charakteristisch einfach ist, folgt $G = \widetilde{N}$. Somit ist G ist eine direkte Summe von Gruppen, die zu N isomorph sind. Nehmen wir nun an, dass ein Normalteiler $1 \neq M \trianglelefteq N$ existiert. Für $\alpha \in \mathrm{Aut}(G)$ mit $\alpha(N) \neq N$ ist $\alpha(N) \leq \mathrm{C}_G(N)$ nach Lemma 2.5. Dies zeigt $M \trianglelefteq \widetilde{N} = G$ und die Minimalität von N liefert $M = N$. Also ist N einfach.

Sei nun $G = N_1 \oplus \ldots \oplus N_k$ mit isomorphen einfachen Gruppen $N_1, \ldots, N_k$. Sei $H \neq 1$ charakteristisch in G. Wir betrachten zunächst den Fall, in dem die N_i abelsch sind. Dann ist G elementarabelsch und $\mathrm{Aut}(G) \cong \mathrm{GL}(k, p)$ für eine Primzahl p. Aus der linearen Algebra weiß man, dass für $x, y \in G \setminus \{1\}$ ein $\alpha \in \mathrm{Aut}(G)$ mit $\alpha(x) = y$ existiert. Dies zeigt $H = G$. Sei nun N_i nichtabelsch und $1 \neq x_1 \ldots x_k \in H$ mit $x_i \in N_i$ für $i = 1, \ldots, k$. O. B. d. A. sei $x_1 \neq 1$. Wegen $\mathrm{Z}(N_1) = 1$ existiert ein $y \in N_1$ mit $x_1 y \neq y x_1$. Es gilt dann

$$1 \neq y x_1 y^{-1} x_1^{-1} = y(x_1 \ldots x_k) y^{-1} (x_1 \ldots x_k)^{-1} \in H \cap N_1 \trianglelefteq N_1.$$

Da N_1 einfach ist, folgt $N_1 \leq H$. Für jede Permutation $\sigma \in S_k$ existiert ein $\alpha \in \mathrm{Aut}(G)$ mit $\alpha(N_i) = N_{\sigma(i)}$ für $i = 1, \ldots, k$. Dies zeigt $N_i \leq H$ für $i = 1, \ldots, k$, d. h. $H = G$. Somit ist G charakteristisch einfach. □

Satz 2.27. *Hauptfaktoren sind stets charakteristisch einfach. Jeder Hauptfaktor einer endlichen auflösbaren Gruppe G ist elementarabelsch. Insbesondere ist jeder minimale Normalteiler von G elementarabelsch.*

Beweis. Sei N/M ein Hauptfaktor mit $N, M \trianglelefteq G$, und sei K/M charakteristisch in G/M. Nach Lemma 2.25 ist dann $K/M \trianglelefteq G/N$ und $K \trianglelefteq G$. Dies zeigt $K \in \{N, M\}$. Also ist N/M charakteristisch einfach. Sei nun G endlich und auflösbar. Jeder Hauptfaktor von G ist dann charakteristisch einfach und auflösbar nach Lemma 2.21. Die zweite Behauptung folgt nun aus Satz 2.26. Da man jeden minimalen Normalteiler zu einer Hauptreihe fortsetzen kann, ist auch die dritte Behauptung klar. □

Bemerkung 2.28.

(i) Eine Normalreihe mit charakteristisch einfachen Faktoren ist *nicht* unbedingt eine Hauptreihe!

(ii) Besitzt G eine Normalreihe mit zyklischen Faktoren, so heißt G *überauflösbar*. Nach Beispiel 2.24 haben die Hauptfaktoren von G dann Primzahlordnung. Jede überauflösbare Gruppe ist offenbar auflösbar, aber die Umkehrung ist falsch (Beispiel: A_4). Nach Satz 2.10 sind abelsche Gruppen überauflösbar (jede Kompositionsreihe ist eine Normalreihe).

3 Kommutatoren und nilpotente Gruppen

Definition 3.1. Für $x, y \in G$ sei $[x, y] := xyx^{-1}y^{-1}$ der *Kommutator* von x und y. Induktiv sei $[x_1, \ldots, x_n] := [x_1, [x_2, \ldots, x_n]]$ für $x_1, \ldots, x_n \in G$. Für $X, Y \subseteq G$ sei analog $[X, Y] := \langle [x, y] : x \in X, y \in Y \rangle$ und $[X_1, \ldots, X_n] := [X_1, [X_2, \ldots, X_n]]$. Insbesondere ist $G' := G^{(1)} := [G, G]$ die *Kommutatorgruppe* von G. Wir setzen $G'' := (G')'$ und allgemeiner $G^{(i)} := (G^{(i-1)})'$ für $i \geq 2$. Außerdem sei $G^{[1]} := G$ und $G^{[i]} := [G^{[i-1]}, G]$ für $i \geq 2$.[1]

Bemerkung 3.2.

(i) Leichte Rechnungen zeigen

$$\boxed{\begin{aligned} [x, y]^{-1} &= [y, x], & {}^{z}[x, y] &= [{}^{z}x, {}^{z}y], \\ [x, yz] &= [x, y] \cdot {}^{y}[x, z], & [xy, z] &= {}^{x}[y, z][x, z]. \end{aligned}}$$

Insbesondere ist $[X, Y] = [Y, X]$.

(ii) Für einen Homomorphismus $f : G \to H$ gilt $f([x, y]) = [f(x), f(y)]$. Insbesondere ist $[X, Y]N/N = [XN/N, YN/N]$ für $N \trianglelefteq G$. Sind X, Y normal (bzw. charakteristisch) in G, so auch $[X, Y]$. Insbesondere sind $G^{(k)}$ und $G^{[k]}$ charakteristisch in G.

(iii) Für $x, y \in G$ gilt $xyG' = yx[x^{-1}, y^{-1}]G' = yxG'$. Also ist G/G' abelsch. Sei nun $N \trianglelefteq G$, sodass G/N abelsch ist. Dann ist $[x, y]N = xyx^{-1}y^{-1}N = 1$ und $[x, y] \in N$ für alle $x, y \in G$. Dies zeigt $G' \subseteq N$. Also ist G' der kleinste Normalteiler mit abelscher Faktorgruppe. Insbesondere ist G genau dann abelsch, wenn $G' = 1$ gilt.

Lemma 3.3. *Für $X, Y \leq G$ gilt $[X, Y] \trianglelefteq \langle X, Y \rangle$.*

Beweis. Sicher ist $[X, Y] \leq \langle X, Y \rangle$. Für $x, z \in X$ und $y \in Y$ gilt ${}^{z}[x, y] = [zx, y][z, y]^{-1} \in [X, Y]$ nach Bemerkung 3.2. Dies zeigt $X \leq \mathrm{N}_G([X, Y])$. Analog ist $Y \leq \mathrm{N}_G([Y, X]) = \mathrm{N}_G([X, Y])$. □

Satz 3.4. *Genau dann ist G auflösbar, wenn ein $k \in \mathbb{N}$ mit $G^{(k)} = 1$ existiert.*

Beweis. Sei $1 = G_0 \trianglelefteq \ldots \trianglelefteq G_k = G$ mit abelschen Faktoren. Wir argumentieren durch Induktion nach k. Der Fall $k = 0$ ist klar. Sei also $k \geq 1$. Da G/G_{k-1} abelsch ist, gilt $G' \subseteq G_{k-1}$. Also gibt es eine Reihe $1 = G_0 \cap G' \trianglelefteq \ldots \trianglelefteq G_{k-1} \cap G' = G'$. Nach Induktion existiert ein $l \in \mathbb{N}$ mit $G^{(l+1)} = (G')^{(l)} = 1$.

Sei nun umgekehrt $G^{(k)} = 1$. Dann ist $1 = G^{(k)} \trianglelefteq G^{(k-1)} \trianglelefteq \ldots \trianglelefteq G' \trianglelefteq G$ eine (Sub)normalreihe mit abelschen Faktoren. Also ist G auflösbar. □

Bemerkung 3.5. Das kleinste $k \geq 1$ mit $G^{(k)} = 1$ nennt man *Auflösbarkeitsstufe* von G. Im Fall $G'' = 1$ heißt G *metabelsch*. Gruppen G mit $G' = G$ heißen *perfekt*. Offenbar ist jede nichtabelsche, einfache Gruppe perfekt.

[1] Diese Bezeichnung ist in der Literatur nicht einheitlich. Man bentutzt auch G^i (Verwechselung mit direktem Produkt), $K_i(G)$ oder $\gamma_i(G)$.

Lemma 3.6 (3-Untergruppen-Lemma)**.** *Seien $X, Y, Z \leq G$ mit $[X,Y,Z] = [Y,Z,X] = 1$. Dann ist $[Z,X,Y] = 1$.*

Beweis. Wir müssen zeigen, dass $[z,x,y] = 1$ für $z \in Z$, $x \in X$ und $y \in Y$ gilt. Dafür genügt es, die *Hall-Witt-Identität*

$$\boxed{{}^y[x,y^{-1},z] \cdot {}^z[y,z^{-1},x] \cdot {}^x[z,x^{-1},y] = 1} \tag{3.1}$$

nachzuprüfen. Es gilt ${}^y[x,y^{-1},z] = yx[y^{-1},z]x^{-1}[z,y^{-1}]y^{-1} = yxy^{-1}zyz^{-1}x^{-1}zy^{-1}z^{-1}$. Die linke Seite von (3.1) ist also

$$yxy^{-1}zy\underbrace{z^{-1}x^{-1}zy^{-1}z^{-1}\cdot zyz^{-1}xz}_{=1}\underbrace{x^{-1}y^{-1}xz^{-1}x^{-1}\cdot xzx^{-1}yx}_{=1}y^{-1}z^{-1}yx^{-1}y^{-1} = 1. \qquad \square$$

Definition 3.7. Sei $\mathrm{Z}_0(G) := 1$ und $\mathrm{Z}_i(G)/Z_{i-1}(G) := \mathrm{Z}(G/\mathrm{Z}_{i-1}(G))$ für $i \geq 1$. Existiert ein $k \geq 0$ mit $\mathrm{Z}_k(G) = G$, so heißt G *nilpotent* Das kleinste k mit dieser Eigenschaft ist die *(Nilpotenz)klasse* von G. Ggf. $1 = \mathrm{Z}_0(G) < \ldots < \mathrm{Z}_k(G) = G$ die *obere Zentralreihe* von G.

Beispiel 3.8.

(i) Abelsche Gruppen sind nilpotent mit Klasse ≤ 1.

(ii) Nilpotente Gruppen sind auflösbar, denn die obere Zentralreihe hat abelsche Faktoren. Da zentrale Untergruppen stets normal sind, lässt sich die obere Zentralreihe zu einer Normalreihe mit zyklischen Faktoren verfeinern. Nilpotente Gruppen sind daher sogar überauflösbar (und die Hauptfaktoren haben Primzahlordnung).

Primzahlordnung $\Longrightarrow$ zyklisch $\Longrightarrow$ abelsch $\Longrightarrow$ nilpotent $\Longrightarrow$ überauflösbar $\Longrightarrow$ auflösbar

Satz 3.9. *Genau dann ist $G \neq 1$ nilpotent mit Klasse k, falls $G^{[k]} > G^{[k+1]} = 1$ gilt.*

Beweis. Sei G nilpotent mit Klasse k. Wir zeigen induktiv $G^{[i+1]} \subseteq \mathrm{Z}_{k-i}(G)$ für $i \geq 0$. Dies ist klar für $i = 0$. Sei also $i \geq 1$. Nehmen wir an, dass die Behauptung für $i-1$ gilt. Dann ist

$$\begin{aligned} G^{[i+1]}\,\mathrm{Z}_{k-i}(G)/\mathrm{Z}_{k-i}(G) &= [G^{[i]},G]\,\mathrm{Z}_{k-i}(G)/\mathrm{Z}_{k-i}(G) = [G^{[i]}\,\mathrm{Z}_{k-i}(G)/\mathrm{Z}_{k-i}(G), G/\mathrm{Z}_{k-i}(G)] \\ &\subseteq [\mathrm{Z}_{k-i+1}(G)/\mathrm{Z}_{k-i}(G), G/\mathrm{Z}_{k-i}(G)] = [\mathrm{Z}(G/\mathrm{Z}_{k-i}(G)), G/\mathrm{Z}_{k-i}(G)] = 1, \end{aligned}$$

d. h. $G^{[i+1]} \subseteq \mathrm{Z}_{k-i}(G)$. Insbesondere ist $G^{[k+1]} \subseteq \mathrm{Z}_0(G) = 1$.

Nehmen wir nun umgekehrt $G^{[l]} = 1$ für ein $l \geq 0$ an. Wir zeigen induktiv $G^{[l-i]} \subseteq \mathrm{Z}_i(G)$ für $i \geq 0$. Da dies für $i = 0$ gilt, dürfen wir voraussetzen, dass die Behauptung für $i - 1 \geq 0$ stimmt. Dann ist

$$[G^{[l-i]}\,\mathrm{Z}_{i-1}(G)/\mathrm{Z}_{i-1}(G), G/\mathrm{Z}_{i-1}(G)] = [G^{[l-i]},G]\,\mathrm{Z}_{i-1}(G)/\mathrm{Z}_{i-1}(G) = G^{[l-i+1]}\,\mathrm{Z}_{i-1}(G)/\mathrm{Z}_{i-1}(G) = 1$$

und $G^{[l-i]}\,\mathrm{Z}_{i-1}(G)/\mathrm{Z}_{i-1}(G) \leq \mathrm{Z}(G/\mathrm{Z}_{i-1}(G)) = \mathrm{Z}_i(G)/\mathrm{Z}_{i-1}(G)$. Also ist $G^{[l-i]} \subseteq \mathrm{Z}_i(G)$ und $\mathrm{Z}_{l-1}(G) = G$. Dies zeigt, dass G nilpotent mit Klasse höchstens $l-1$ ist. Die Behauptung folgt. $\square$

Bemerkung 3.10.

(i) Ist G nilpotent mit Klasse k, so nennt man $1 = G^{[k+1]} < \ldots < G^{[1]} = G$ die *untere Zentralreihe* von G. Die unteren und oberen Zentralreihen sind also zwei Normalreihen der gleichen Länge.

(ii) Sei G nilpotent mit Klasse k und $H \leq G$ sowie $N \trianglelefteq G$. Dann ist $H^{[k+1]} \leq G^{[k+1]} = 1$ und $(G/N)^{[k+1]} = G^{[k+1]}N/N = 1$. Daher sind auch H und G/N nilpotent, wobei die Klasse jeweils durch k beschränkt ist. Sind umgekehrt $N \trianglelefteq G$ und G/N nilpotent, so muss G nicht unbedingt nilpotent sein! Ein Beispiel ist $G = S_3$ mit $N = A_3$.

Lemma 3.11. *Für $n, m \geq 1$ gilt $[G^{[n]}, G^{[m]}] \subseteq G^{[n+m]}$.*

Beweis. Induktion nach n: Im Fall $n = 1$ ist $[G, G^{[m]}] = [G^{[m]}, G] = G^{[m+1]}$. Sei also $n \geq 2$ und die Aussage für $n-1$ bereits bewiesen. Für $\overline{G} := G/G^{[n+m]}$ gilt nach Induktion $[\overline{G}, \overline{G}^{[n-1]}, \overline{G}^{[m]}] \subseteq [\overline{G}, \overline{G}^{[n+m-1]}] = \overline{G}^{[n+m]} = 1$ und $[\overline{G}^{[n-1]}, \overline{G}^{[m]}, \overline{G}] = [\overline{G}^{[n-1]}, \overline{G}^{[m+1]}] \subseteq \overline{G}^{[n+m]} = 1$. Lemma 3.6 impliziert daher $[G^{[m]}, G^{[n]}]G^{[n+m]}/G^{[n+m]} = [\overline{G}^{[m]}, \overline{G}^{[n]}] = [\overline{G}^{[m]}, \overline{G}, \overline{G}^{[n-1]}] = 1$. Dies zeigt die Behauptung. □

Satz 3.12. *Ist k die Nilpotenzklasse von $G \neq 1$, so ist die Auflösbarkeitsstufe von G höchstens $\log_2(k)+1$.*

Beweis. Wir zeigen $G^{(i)} \subseteq G^{[2^i]}$ durch Induktion nach $i \geq 0$. Im Fall $i = 0$ gilt Gleichheit. Sei also $i \geq 1$ und die Behauptung für $i-1$ bereits bewiesen. Dann ist $G^{(i)} = [G^{(i-1)}, G^{(i-1)}] \subseteq [G^{[2^{i-1}]}, G^{[2^{i-1}]}] \subseteq G^{[2^i]}$ nach Lemma 3.11. Für $l := \lfloor \log_2(k) \rfloor + 1 \geq \log_2(k+1)$ ist nun $G^{(l)} \subseteq G^{[2^l]} \subseteq G^{[k+1]} = 1$. □

Beispiel 3.13. Es gibt metabelsche Gruppen mit beliebig hoher Nilpotenzklasse (Diedergruppen der Form D_{2^n}, siehe Satz 9.3).

Satz 3.14. *Sei G nilpotent, $H < G$ und $1 \neq N \trianglelefteq G$. Dann ist $H < \mathrm{N}_G(H)$, $[G, N] < N$ und $N \cap \mathrm{Z}(G) \neq 1$.*

Beweis. Sei $k \geq 1$ minimal mit $G^{[k]} \subseteq H$. Wegen $H < G$ ist $k \geq 2$. Es gilt $[G^{[k-1]}, H] \subseteq [G^{[k-1]}, G] = G^{[k]} \subseteq H$. Für $x \in G^{[k-1]}$ und $h \in H$ ist also $xhx^{-1}h^{-1} \in H$ und $xhx^{-1} \in H$. Dies zeigt $G^{[k-1]} \subseteq \mathrm{N}_G(H)$. Andererseits gilt $G^{[k-1]} \nsubseteq H$ wegen der Minimalität von k.

Sei $N_1 := N$ und $N_{i+1} := [G, N_i]$ für $i \geq 1$. Induktiv sieht man leicht $N_i \subseteq G^{[i]}$. Es gibt also ein $k \geq 1$ mit $N_k = 1$. Insbesondere ist $[G, N] = N_2 < N_1$, denn anderenfalls wäre $N_3 = [G, N_2] = [G, N] = N$, $N_4 = N$ usw. Für die letzten Aussage wählen wir $l \geq 1$ minimal mit $N_l \neq 1$. Dann ist $[G, N_l] = N_{l+1} = 1$ und $N_l \subseteq N \cap \mathrm{Z}(G)$. □

Satz 3.15 (Fitting)**.** *Sind N und M nilpotente Normalteiler von G, so ist auch NM nilpotent. Hat N Klasse n und M Klasse m, so hat NM höchstens Klasse $n + m$.*

Beweis. Für beliebige Normalteiler $X, Y, Z \trianglelefteq G$ und $x \in X$, $y \in Y$ und $z \in Z$ gilt $[x, yz] = [x, y] \cdot {}^y[x, z] \in [X, Y][X, Z]$ nach Bemerkung 3.2. Dies zeigt $[X, YZ] \subseteq [X, Y][X, Z] \subseteq [X, YZ]$ und somit $[X, YZ] = [X, Y][X, Z]$. Analog ist $[XY, Z] = [X, Z][Y, Z]$. Daher ist $(NM)^{[n+m+1]}$ ein Produkt von Normalteilern der Form $[X_0, \ldots, X_{n+m}]$ mit $X_0, \ldots, X_{n+m} \in \{N, M\}$. O. B. d. A. können wir annehmen, dass N mindestens $n + 1$ Mal unter den X_i auftritt (anderenfalls betrachte M). Wir zeigen durch Induktion nach $n + m$, dass dann $[X_0, \ldots, X_{n+m}] \subseteq N^{[n+1]}$ gilt. Ist $X_0 = M$, so gilt induktiv bereits $[X_1, \ldots, X_{n+m}] \subseteq N^{[n+1]}$ und die Behauptung folgt. Gilt hingegen $X_0 = N$, so ist $[X_1, \ldots, X_{n+m}] \subseteq N^{[n]}$ und $[X_0, \ldots, X_{n+m}] \subseteq [N, N^{[n]}] = N^{[n+1]}$. Die Behauptung folgt nun aus Satz 3.9. □

Definition 3.16. Die *Fittinggruppe* $\mathrm{F}(G)$ einer endlichen Gruppe G ist das Produkt aller nilpotenten Normalteiler von G. Nach Satz 3.15 ist $\mathrm{F}(G)$ der größte nilpotente Normalteiler von G.

Bemerkung 3.17. Offenbar ist $\mathrm{F}(G)$ charakteristisch in G.

Beispiel 3.18. Sei $G \neq 1$ auflösbar und N ein minimaler Normalteiler von G. Nach Satz 2.27 ist N (elementar)abelsch und daher nilpotent. Dies zeigt $\mathrm{F}(G) \neq 1$. Beispielsweise ist $\mathrm{F}(S_3) = A_3$.

Satz 3.19. *Ist G endlich und auflösbar, so gilt* $\mathrm{C}_G(\mathrm{F}(G)) \leq \mathrm{F}(G)$.

Beweis. Sei $C := \mathrm{C}_G(\mathrm{F}(G)) \trianglelefteq G$. Wir nehmen indirekt $\overline{C} := C/\mathrm{Z}(\mathrm{F}(G)) = C/C \cap \mathrm{F}(G) \neq 1$ an. Da $\overline{C}$ auflösbar ist, gilt $N/\mathrm{Z}(\mathrm{F}(G)) := \mathrm{F}(\overline{C}) \neq 1$. Dabei ist $\mathrm{Z}(\mathrm{F}(G)) \leq N \cap \mathrm{Z}(C) \leq \mathrm{Z}(N)$ und $N/\mathrm{Z}(N) \cong (N/\mathrm{Z}(\mathrm{F}(G)))/(\mathrm{Z}(N)/\mathrm{Z}(\mathrm{F}(G)))$ ist nilpotent. Also ist auch N nilpotent. Da $\mathrm{Z}(\mathrm{F}(G))$ charakteristisch in $\mathrm{F}(G)$ ist, gilt $\mathrm{Z}(\mathrm{F}(G)) \trianglelefteq G$ nach Lemma 2.25. Außerdem ist $\mathrm{F}(\overline{C})$ charakteristisch in $\overline{C} \trianglelefteq G/\mathrm{Z}(\mathrm{F}(G))$. Dies zeigt $N \trianglelefteq G$ und man erhält den Widerspruch $N \leq \mathrm{F}(G) \cap C = \mathrm{Z}(\mathrm{F}(G))$. □

Bemerkung 3.20. Für endliche, auflösbare Gruppen G gilt $G/\mathrm{Z}(\mathrm{F}(G)) = \mathrm{N}_G(\mathrm{F}(G))/\mathrm{C}_G(\mathrm{F}(G)) \leq \mathrm{Aut}(\mathrm{F}(G))$ nach Satz 3.19.

Definition 3.21.

(i) Eine Gruppe $G \neq 1$ heißt *unzerlegbar*, falls G nicht die direkte Summe von echten Untergruppen ist.

(ii) Sei $\mathrm{End}(G)$ die Menge der Endomorphismen von G.

(iii) Ein $\alpha \in \mathrm{End}(G)$ heißt *normal*, falls $g\alpha(x)g^{-1} = \alpha(gxg^{-1})$ für alle $g, x \in G$ gilt. Die Menge der normalen Endomorphismen bezeichnen wir mit $\mathrm{End}_n(G)$ (analog $\mathrm{Aut}_n(G)$).

(iv) Man nennt $\alpha, \beta \in \mathrm{End}(G)$ *addierbar*, falls $\alpha + \beta \in \mathrm{End}(G)$ mit $(\alpha + \beta)(g) := \alpha(g)\beta(g)$ für $g \in G$.

Lemma 3.22. *Seien $\alpha, \beta, \gamma \in \mathrm{End}(G)$. Dann gilt*

(i) $\alpha + \beta \in \mathrm{End}(G) \iff [\alpha(G), \beta(G)] = 1 \implies \alpha + \beta = \beta + \alpha$.

(ii) $\alpha + \beta \in \mathrm{End}(G) \implies \alpha \circ \gamma + \beta \circ \gamma = (\alpha + \beta) \circ \gamma \in \mathrm{End}(G)$.

(iii) $\alpha + \beta \in \mathrm{End}(G) \implies \gamma \circ \alpha + \gamma \circ \beta = \gamma \circ (\alpha + \beta) \in \mathrm{End}(G)$.

(iv) $\alpha, \beta \in \mathrm{End}_n(G) \implies \alpha \circ \beta \in \mathrm{End}_n(G)$.

(v) Sind $\alpha, \beta \in \mathrm{End}_n(G)$ addierbar, so ist $\alpha + \beta \in \mathrm{End}_n(G)$.

(vi) $\alpha \in \mathrm{Aut}_n(G) \implies \alpha^{-1} \in \mathrm{Aut}_n(G)$.

Beweis.

(i) Es gilt

$$\begin{aligned}\alpha + \beta \in \mathrm{End}(G) &\iff \alpha(g)\alpha(h)\beta(g)\beta(h) = \alpha(gh)\beta(gh) = \alpha(g)\beta(g)\alpha(h)\beta(h)\ \forall g, h \in G \\ &\iff \alpha(h)\beta(g) = \beta(g)\alpha(h)\ \forall g, h \in G \iff [\alpha(G), \beta(G)] = 1 \implies \alpha + \beta = \beta + \alpha\end{aligned}$$

(ii)–(vi) Trivial. □

Lemma 3.23 (FITTING)**.** *Ist G endlich und $\alpha \in \mathrm{End}_n(G)$, so existiert ein $k \geq 1$ mit $G = \mathrm{Ker}(\alpha^k) \oplus \alpha^k(G)$.*

Beweis. Es gilt $\alpha(G) \supseteq \alpha^2(G) \supseteq \ldots$. Wegen $|G| < \infty$ existiert ein $k \geq 1$ mit $\alpha^k(G) = \alpha^{k+1}(G) = \ldots$. Nach dem Homomorphiesatz gilt dann auch $\mathrm{Ker}(\alpha^k) = \mathrm{Ker}(\alpha^{k+1}) = \ldots$. Sei $x \in \mathrm{Ker}(\alpha^k) \cap \alpha^k(G)$. Dann existiert ein $g \in G$ mit $x = \alpha^k(g)$ und $1 = \alpha^k(x) = \alpha^{2k}(g)$. Dies zeigt $g \in \mathrm{Ker}(\alpha^{2k}) = \mathrm{Ker}(\alpha^k)$ und $x = 1$. Also ist $\mathrm{Ker}(\alpha^k) \cap \alpha^k(G) = 1$. Da α normal ist, gilt $\alpha^k(G) \trianglelefteq G$ ($\mathrm{Ker}(\alpha^k) \trianglelefteq G$ gilt sowieso). Außerdem ist $|G/\mathrm{Ker}(\alpha^k)| = |\alpha^k(G)|$. Dies zeigt die Behauptung. □

Definition 3.24. Man nennt $\alpha \in \mathrm{End}(G)$ *nilpotent*, falls ein $k \geq 0$ mit $\alpha^k = 0$ existiert, d. h. $\alpha^k(g) = 1$ für alle $g \in G$.

Lemma 3.25. *Sei G endlich und unzerlegbar und seien $\alpha, \beta \in \mathrm{End}_n(G)$ mit $\alpha + \beta \in \mathrm{Aut}(G)$. Dann ist $\alpha \in \mathrm{Aut}_n(G)$ oder $\beta \in \mathrm{Aut}_n(G)$.*

Beweis. Sei $\alpha' := (\alpha + \beta)^{-1} \circ \alpha \in \mathrm{End}_n(G)$ und $\beta' := (\alpha + \beta)^{-1} \circ \beta \in \mathrm{End}_n(G)$ (Lemma 3.22). Dann ist $\alpha' + \beta' = (\alpha + \beta)^{-1}(\alpha + \beta) = \mathrm{id}_G$. Für $g \in G$ gilt daher

$$\begin{aligned}\alpha'(\beta'(g)) &= \alpha'(\alpha'(g^{-1})\alpha'(g)\beta'(g)) = \alpha'(\alpha'(g^{-1})g) = \alpha'(\alpha'(g^{-1}))\alpha'(g)\\ &= \alpha'(\alpha'(g^{-1}))(\alpha' + \beta')(\alpha'(g)) = \alpha'(\alpha'(g^{-1}))\alpha'(\alpha'(g))\beta'(\alpha'(g)) = \beta'(\alpha'(g)).\end{aligned}$$

Dies zeigt $\alpha' \circ \beta' = \beta' \circ \alpha'$. Ist die Behauptung falsch, so sind α' und β' nicht bijektiv. Da G unzerlegbar ist, sind α' und β' nilpotent nach Lemma 3.23. Sei $k \geq 0$ mit $(\alpha')^k = (\beta')^k = 0$. Dann ist $\mathrm{id}_G = (\alpha' + \beta')^{2k} = \sum_{i=0}^{2k} \binom{2k}{i} (\alpha')^i \circ (\beta')^{2k-i} = 0$ nach Lemma 3.22. Widerspruch. □

Satz 3.26 (KRULL-SCHMIDT)**.** *Sei G endlich und $G = G_1 \oplus \ldots \oplus G_s = H_1 \oplus \ldots \oplus H_t$ mit unzerlegbaren Gruppen $G_1, \ldots, G_s, H_1, \ldots, H_t$. Dann ist $s = t$ und bei geeigneter Nummerierung gilt $G_i \cong H_i$ für $i = 1, \ldots, s$.*

Beweis. Induktion nach $\max\{s, t\}$: Der Fall $s = t = 1$ ist klar. Sei also $\max\{s, t\} \geq 2$. Wir dürfen annehmen, dass $|H_1| \geq |G_i|$ für $i = 1, \ldots, s$ gilt. Die Endomorphismen $\alpha_i : G \to G$, $g_1 \ldots g_s \mapsto g_i$ ($g_j \in G_j$) sind offenbar normal und paarweise addierbar mit $\alpha_1 + \ldots + \alpha_s = \mathrm{id}_G$. Sei $\beta : G \to H_1$, $h_1 \ldots h_t \mapsto h_1$ ($h_i \in H_i$). Dann ist

$$\mathrm{id}_{H_1} = \beta \circ (\alpha_1 + \ldots + \alpha_s)_{|H_1} = \beta \circ (\alpha_1)_{|H_1} + \ldots + \beta \circ (\alpha_s)_{|H_1}.$$

Die Endomorphismen $\beta \circ (\alpha_i)_{|H_1}$ von H_1 sind offenbar auch paarweise addierbar und normal. Nach Lemma 3.25 existiert ein $i \in \{1, \ldots, s\}$ mit $\beta \circ (\alpha_i)_{H_1} \in \mathrm{Aut}(H_1)$. Sei o. B. d. A. $i = 1$. Dann ist $(\alpha_1)_{|H_1}$ injektiv und $H_1 \cong \alpha_1(H_1) = G_1$ nach Wahl von H_1. Für $x \in H_1 \cap G_2 \ldots G_s$ ist $\alpha_1(x) \in \alpha_1(G_2 \ldots G_s) = 1$ und daher $x = 1$. Es gilt also $G = H_1 \oplus G_2 \oplus \ldots \oplus G_s$ und $G_2 \oplus \ldots \oplus G_s \cong G/H_1 \cong H_2 \oplus \ldots \oplus H_t$. Die Behauptung folgt nun mit Induktion. □

4 p-Gruppen

Ab jetzt sei G stets eine endliche Gruppe.

Definition 4.1. Sei π eine Menge von Primzahlen. Ein Element $x \in G$ heißt π-*Element*, falls jeder Primteiler von $|\langle x\rangle|$ in π liegt. Ist jedes Element in G ein π-Element, so nennt man G eine π-Gruppe. Ist $\pi = \{p\}$, so spricht man von p-Elementen und p-Gruppen. Die Menge der Primzahlen, die nicht in π liegen, wird mit π' bezeichnet (analog p').

Satz 4.2 (Sylow)**.** *Sei $|G| = p^a m$ für eine Primzahl $p \nmid m$. Für $0 \leq b \leq a$ besitzt G eine Untergruppe U der Ordnung p^b und U ist enthalten in einer Untergruppe der Ordnung p^a. Die Untergruppen der Ordnung p^a nennt man* p-Sylowgruppen *von G. Die Menge der p-Sylowgruppen sei $\mathrm{Syl}_p(G)$. Für $P \in \mathrm{Syl}_p(G)$ gilt dann $|\mathrm{Syl}_p(G)| = |G : \mathrm{N}_G(P)| \equiv 1 \pmod p$. Insbesondere sind alle p-Sylowgruppen in G konjugiert.*

Beweis. Algebra. □

Folgerung 4.3 (Cauchy)**.** *Für jeden Primteiler p von $|G|$ besitzt ein Element der Ordnung p.*

Bemerkung 4.4.

(i) Nach Lagrange und Cauchy ist G genau dann eine π-Gruppe, falls jeder Primteiler von $|G|$ in π liegt.

(ii) Für π-Normalteiler $N, M \trianglelefteq G$ ist auch $NM \trianglelefteq G$ ein π-Normalteiler, denn $|NM| \mid |N||M|$. Es gibt also einen größten π-Normalteiler $\mathrm{O}_\pi(G)$, den man π-*Kern* oder π-*Radikal* nennt. Für $\pi = \{p\}$ schreibt man $\mathrm{O}_p(G)$.

(iii) Sind $N, M \trianglelefteq G$ mit π-Faktorgruppen G/N und G/M, so ist auch $G/N \cap M$ eine π-Gruppe, denn $|G/N \cap M| = |G/N||N/N \cap M| = |G/N||NM/M| \mid |G/N||G/M|$. Es gibt daher einen kleinsten Normalteiler $\mathrm{O}^\pi(G)$ mit π-Faktorgruppe $G/\mathrm{O}^\pi(G)$. Man nennt $\mathrm{O}^\pi(G)$ das π-*Residuum* von G (analog $\mathrm{O}^p(G)$).

(iv) Für $P \in \mathrm{Syl}_p(G)$ und $N \trianglelefteq G$ ist $p \nmid |PN : P| = |N : N \cap P|$ und $p \nmid |G : PN| = |G/N : PN/N|$. Dies zeigt $P \cap N \in \mathrm{Syl}_p(N)$ und $PN/N \in \mathrm{Syl}_p(G/N)$.

(v) Sei $N \trianglelefteq G$ und $P \in \mathrm{Syl}_p(N)$. Dann operiert G auf $\mathrm{Syl}_p(N)$ durch Konjugation und N operiert transitiv. Das Frattini-Argument zeigt also $G = N\,\mathrm{N}_G(P)$.

Satz 4.5. *Es gilt $\mathrm{O}_p(G) = \bigcap_{P \in \mathrm{Syl}_p(G)} P$ und $\mathrm{O}^{p'}(G) = \langle P : P \in \mathrm{Syl}_p(G)\rangle$.*

Beweis. Offenbar ist $\bigcap_{P\in\mathrm{Syl}_p(G)} P$ ein p-Normalteiler und daher in $\mathrm{O}_p(G)$ enthalten. Nach Sylow existiert umgekehrt ein $P \in \mathrm{Syl}_p(G)$ mit $\mathrm{O}_p(G) \leq P$. Für $g \in G$ ist $\mathrm{O}_p(G) = g\,\mathrm{O}_p(G)g^{-1} \leq gPg^{-1}$. Da alle p-Sylowgruppen konjugiert sind, folgt die erste Behauptung.

Da jedes p-Element in einer p-Sylowgruppe liegt, ist $G/\langle P : P \in \mathrm{Syl}_p(G)\rangle$ eine p'-Gruppe. Also gilt $\mathrm{O}^{p'}(G) \leq \langle P : P \in \mathrm{Syl}_p(G)\rangle$. Sei nun $P \in \mathrm{Syl}_p(\mathrm{O}^{p'}(G))$. Da $G/\,\mathrm{O}^{p'}(G)$ eine p'-Gruppe ist, gilt $P \in \mathrm{Syl}_p(G)$. Wegen $\mathrm{O}^{p'}(G) \trianglelefteq G$ ist dann auch $gPg^{-1} \leq \mathrm{O}^{p'}(G)$. Dies liefert $\langle P : P \in \mathrm{Syl}_p(G)\rangle \leq \mathrm{O}^{p'}(G)$. □

Satz 4.6. *Jede p-Gruppe ist nilpotent.*

Beweis. Sei P eine p-Gruppe. Wir argumentieren durch Induktion nach $|P|$. Sei o. B. d. A. $P \neq 1$. Betrachtet man die Klassengleichung modulo p, so erhält man $|\mathrm{Z}(P)| \equiv 0 \pmod p$. Insbesondere ist $\mathrm{Z}(P) \neq 1$. Nach Induktion ist $P/\,\mathrm{Z}(P)$ nilpotent und daher auch P. □

Bemerkung 4.7. Aus statistischer Sicht sind fast alle Gruppen p-Gruppen. Unter den Gruppen der Ordnung ≤ 2000 haben beispielsweise über 99% die Ordnung 2^{10}. Die Anzahl der Gruppen der Ordnung 2^{11} ist unbekannt (siehe Bemerkung 2.18).

Satz 4.8. *Die folgenden Aussagen sind äquivalent:*

(i) *G ist nilpotent.*

(ii) *Für alle $H < G$ ist $H < \mathrm{N}_G(H)$.*

(iii) *Jede maximale Untergruppe von G ist normal.*

(iv) *Für jede Primzahl p enthält G genau eine p-Sylowgruppe.*

(v) *G ist die direkte Summe seiner Sylowgruppen.*

Beweis.

(i)$\Longrightarrow$(ii): Satz 3.14.

(ii)$\Longrightarrow$(iii): Trivial.

(iii)$\Longrightarrow$(iv): Sei $P \in \mathrm{Syl}_p(G)$. Ist $\mathrm{N}_G(P) < G$, so liegt $\mathrm{N}_G(P)$ in einer maximalen Untergruppe $H < G$. Nach (iii) ist $H \trianglelefteq G$. Aus Bemerkung 4.4 folgt nun der Widerspruch $G = H\,\mathrm{N}_G(P) = H$.

(iv)$\Longrightarrow$(v): Seien $p_1, \ldots, p_n$ die Primteiler von $|G|$ und $\mathrm{Syl}_{p_i}(G) = \{P_i\}$. Dann ist $P_i \trianglelefteq G$ und $|P_1 \ldots P_n| = |P_1| \ldots |P_n|$. Es folgt leicht $G = P_1 \oplus \ldots \oplus P_n$.

(v)$\Longrightarrow$(i): Nach Satz 4.6 ist jede Sylowgruppe nilpotent und daher auch G (Satz 3.15).

□

Satz 4.9. *Es gilt* $\mathrm{F}(G) = \bigoplus_{p||G|} \mathrm{O}_p(G)$.

Beweis. Die rechte Seite ist ein nilpotenter Normalteiler und daher in $\mathrm{F}(G)$ enthalten. Nach Satz 4.8 ist $\mathrm{F}(G) = Q_1 \oplus \ldots \oplus Q_n$ mit $Q_i \in \mathrm{Syl}_{p_i}(\mathrm{F}(G))$. Als einzige p_i-Sylowgruppe von $\mathrm{F}(G)$ muss Q_i charakteristisch in $\mathrm{F}(G)$ sein. Nach Lemma 2.25 ist also $Q_i \trianglelefteq G$ und somit $Q_i \leq \mathrm{O}_{p_i}(G)$. □

Definition 4.10. Die *Frattinigruppe* $\Phi(G)$ ist der Durchschnitt aller maximalen Untergruppen von G. Für $G = 1$ setzt man $\Phi(G) = 1$.

Bemerkung 4.11. Für $G \neq 1$ ist sicher $\Phi(G) < G$. Außerdem ist $\Phi(G)$ charakteristisch in G.

Lemma 4.12. *Für $H \leq G$ und $N \trianglelefteq G$ gilt:*

(i) $G = H\Phi(G) \Longrightarrow G = H$.

(ii) $N \leq \Phi(H) \Longrightarrow N \leq \Phi(G)$.

(iii) $\Phi(N) \trianglelefteq \Phi(G)$.

(iv) $\Phi(G)N/N \leq \Phi(G/N)$.

(v) $N \leq \Phi(G) \Longrightarrow \Phi(G/N) = \Phi(G)/N$.

Beweis.

(i) Im Fall $H < G$ liegt H in einer maximalen Untergruppe $M < G$. Nach Definition ist aber auch $\Phi(G) \leq M$ und man erhält den Widerspruch $G = H\Phi(G) \leq M$.

(ii) Im Fall $N \not\leq \Phi(G)$ existiert eine maximale Untergruppe $M < G$ mit $N \not\leq M$ und daher $G = MN$. Nach Dedekind ist $H = NM \cap H = N(M \cap H) = \Phi(H)(M \cap H)$. Nach (i) ist also $H = M \cap H \leq M$ und man hat den Widerspruch $N \leq M$.

(iii) Da $\Phi(N)$ charakteristisch in N ist, gilt $\Phi(N) \trianglelefteq G$. Man kann also (ii) mit $\Phi(N)$ statt N und N statt H anwenden. Die Behauptung folgt.

(iv) Ist M/N eine maximale Untergruppe von G/N, so ist auch M maximal in G. Dies zeigt $\Phi(G)N/N \subseteq MN/N$ und die Behauptung folgt.

(v) Nach (iv) müssen wir nur $\Phi(G/N) \leq \Phi(G)/N$ zeigen. Ist $M < G$ maximal, so ist $N \leq \Phi(G) \leq M$ und $M/N < G/N$ ist ebenfalls maximal. Dies zeigt $\Phi(G/N) \leq M/N$ und die Behauptung folgt. □

Satz 4.13 (Frattini)**.** *Es gilt:*

(i) $\Phi(G)$ *ist nilpotent.*

(ii) Ist $G/\Phi(G)$ *nilpotent, so auch* G.

(iii) $G' \cap \mathrm{Z}(G) \leq \Phi(G)$.

Beweis.

(i) Sei $P \in \mathrm{Syl}_p(\Phi(G))$. Nach Bemerkung 4.4 ist $G = \Phi(G)\,\mathrm{N}_G(P)$ und Lemma 4.12 zeigt $G = \mathrm{N}_G(P)$, d. h. $P \trianglelefteq G$. Dann ist auch $P \trianglelefteq \Phi(G)$ und die Behauptung folgt aus Satz 4.8.

(ii) Für $P \in \mathrm{Syl}_p(G)$ ist $P\Phi(G)/\Phi(G) \in \mathrm{Syl}_p(G/\Phi(G))$. Nach Satz 4.8 ist $P\Phi(G)/\Phi(G) \trianglelefteq G/\Phi(G)$ und somit $P\Phi(G) \trianglelefteq G$. Wegen $P \in \mathrm{Syl}_p(P\Phi(G))$ ist $G = \mathrm{N}_G(P)P\Phi(G) = \mathrm{N}_G(P)\Phi(G)$ nach Bemerkung 4.4. Lemma 4.12 zeigt nun $G = \mathrm{N}_G(P)$ und $P \trianglelefteq G$. Die Behauptung folgt mit Satz 4.8.

(iii) Ist $D := G' \cap \mathrm{Z}(G) \not\leq \Phi(G)$, so existiert eine maximale Untergruppe $M < G$ mit $D \not\leq M$, also $G = DM$. Wegen $D \leq \mathrm{Z}(G)$ ist $M \trianglelefteq G$. Nach Cauchy muss $|G/M|$ eine Primzahl sein. Insbesondere ist G/M abelsch und daher $D \leq G' \leq M$. Widerspruch. □

Satz 4.14 (Wielandt)**.** *Genau dann ist G nilpotent, wenn $G' \leq \Phi(G)$ gilt.*

Beweis. Ist G nilpotent, so ist jede maximale Untergruppe $M < G$ normal in G (Satz 4.8). Insbesondere ist $|G/M|$ eine Primzahl und G/M ist abelsch. Dies zeigt $G' \leq M$ und daher $G' \leq \Phi(G)$.

Sei nun umgekehrt $G' \leq \Phi(G)$. Dann ist $G/\Phi(G)$ abelsch und daher nilpotent. Die Behauptung folgt nun aus Satz 4.13. □

Satz 4.15. *Für jede p-Gruppe P ist $\Phi(P) = P'\langle x^p : x \in P\rangle$. Insbesondere ist $P/\Phi(P)$ elementarabelsch. Ist $N \trianglelefteq P$ mit elementarabelscher Faktorgruppe P/N, so gilt $\Phi(P) \leq N$. Also ist $\Phi(P)$ der kleinste Normalteiler mit elementarabelscher Faktorgruppe.*

Beweis. Nach Wielandt ist $P' \leq \Phi(P)$. Für jede maximale Untergruppe $M < P$ ist $M \trianglelefteq P$ und daher $|P/M| = p$. Dies zeigt $\langle x^p : x \in P\rangle \leq M$ und es folgt $P'\langle x^p : x \in P\rangle \leq \Phi(P)$. Sei nun $N \trianglelefteq P$, sodass P/N elementarabelsch ist. Nehmen wir $\Phi(P) \nsubseteq N$ an. Dann existiert ein $x \in \Phi(P) \setminus N$. Insbesondere ist $1 \neq xN \in P/N$. Wie üblich ist P/N ein Vektorraum über $\mathbb{F}_p$. Wir können also xN zu einer Basis $xN, x_2N, \ldots, x_rN$ von P/N ergänzen. Offenbar ist dann $P = \langle x, x_2, \ldots, x_r\rangle N = \Phi(P)\langle x_2, \ldots, x_r\rangle N$. Es folgt $P = \langle x_2, \ldots, x_r\rangle N$ und $P/N = \langle x_2N, \ldots, x_rN\rangle$. Dies widerspricht der Wahl von $x_2, \ldots, x_r$. Also ist $\Phi(P) \leq N$. Offenbar ist $N := P'\langle x^p : x \in P\rangle$ ein Normalteiler mit elementarabelscher Faktorgruppe. Daher gilt auch $\Phi(P) \leq P'\langle x^p : x \in P\rangle$. □

Satz 4.16 (Burnsides Basissatz)**.** *Für eine p-Gruppe P gilt $P = \langle x_1, \ldots, x_n\rangle$ genau dann, wenn $P/\Phi(P) = \langle x_1\Phi(P), \ldots, x_n\Phi(P)\rangle$. Ist also $|P/\Phi(P)| = p^r$, so lässt sich P mit r Elementen erzeugen, aber nicht mit weniger als r.*

Beweis. Es gilt

$$P = \langle x_1, \ldots, x_n\rangle \iff P = \langle x_1, \ldots, x_n\rangle\Phi(P) \iff P/\Phi(P) = \langle x_1\Phi(P), \ldots, x_n\Phi(P)\rangle.$$

Die zweite Aussage ergibt sich, indem man $P/\Phi(P)$ wieder als Vektorraum über $\mathbb{F}_p$ auffasst. □

Folgerung 4.17. *Besitzt G nur eine maximale Untergruppe, so ist G zyklisch.*

Beweis. Offenbar ist $\Phi(G)$ maximal in G. Ist G keine p-Gruppe, so müsste $\Phi(G)$ alle Sylowgruppen von G enthalten. Dann wäre aber $G = \Phi(G)$. Also ist G eine p-Gruppe und $|G/\Phi(G)| = p$. Die Aussage folgt nun mit Satz 4.16. □

Satz 4.18. *Sei $\alpha \in \mathrm{Aut}(G)$ mit $\mathrm{ggT}(|\langle\alpha\rangle|, |\Phi(G)|) = 1$ und $\alpha(x) \equiv x \pmod{\Phi(G)}$. Dann ist $\alpha = \mathrm{id}_G$.*

Beweis. Sei $x_1, \ldots, x_n \in G$ ein Erzeugendensystem von G und $\Omega := x_1\Phi(G) \times \ldots \times x_n\Phi(G)$. Nach Voraussetzung operiert $\langle\alpha\rangle$ komponentenweise auf Ω. Für $\omega = (y_1, \ldots, y_n) \in \Omega$ gilt dabei $G = \langle y_1, \ldots, y_n\rangle\Phi(G) = \langle y_1, \ldots, y_n\rangle$ und $\langle\alpha\rangle_\omega = 1$ (Stabilisator). Die Bahnengleichung liefert nun $|\langle\alpha\rangle| \mid |\Omega| = |\Phi(G)|^n$. Wegen $\mathrm{ggT}(|\langle\alpha\rangle|, |\Phi(G)|) = 1$ ist $\alpha = \mathrm{id}_G$. □

Bemerkung 4.19. Sei P eine p-Gruppe und α ein nicht-trivialer p'-Automorphismus von P. Dann besagt Satz 4.18, dass α nicht-trivial auf $P/\Phi(P)$ operiert. Insbesondere ist der Kern des kanonischen Homomorphismus $\mathrm{Aut}(P) \to \mathrm{Aut}(P/\Phi(P))$ eine p-Gruppe.

Beispiel 4.20. Sei P eine nichtabelsche p-Gruppe der Ordnung p^3. Dann ist $1 \neq P' \leq \Phi(P) < P$ und $|P : \Phi(P)| = p^2$ nach Satz 4.16. Dies zeigt $P' = \Phi(P)$. Nach Satz 3.14 ist $P' \leq \mathrm{Z}(P)$ und nach Aufgabe 4 ist $P/\mathrm{Z}(P)$ nicht zyklisch. Also gilt $P' = \Phi(P) = \mathrm{Z}(P)$. Wir werden diese Gruppen später vollständig klassifizieren (Satz 9.7). Sei nun $\alpha \in \mathrm{Aut}(P)$ ein p'-Automorphismus. Nach Bemerkung 4.19 operiert α treu auf $P/\Phi(P)$. Wir können also $\alpha \in \mathrm{Aut}(P/\Phi(P)) \cong \mathrm{GL}(2,p)$ annehmen. Wegen $|\mathrm{GL}(2,p)| = (p^2-1)(p^2-p) = (p-1)^2p(p+1)$ ist $|\langle\alpha\rangle|$ ein Teiler von $(p-1)^2(p+1)$.

Satz 4.21. *Seien p, q Primzahlen und $n \geq 1$. Dann ist jede Gruppe der Ordnung p^nq auflösbar.*

Beweis. Sei G ein minimales Gegenbeispiel. Sicher ist dann $p \neq q$. Sei $P \in \mathrm{Syl}_p(G)$. Im Fall $P \trianglelefteq G$ wäre G auflösbar, da P und G/P auflösbar sind. Also ist $\mathrm{N}_G(P) = P$. Wir wählen $Q \in \mathrm{Syl}_p(G) \setminus \{P\}$, sodass $|P \cap Q|$ möglichst groß ist. Nehmen wir zunächst $P \cap Q = 1$ an. Dann schneiden sich je zwei p-Sylowgruppen trivial und es gibt $1 + (|P|-1)|G : \mathrm{N}_G(P)| = |G| - q + 1$ viele p-Elemente in G. Somit ist nur noch Platz für eine q-Sylowgruppe, die dann normal sein muss. Dann wäre aber G wieder auflösbar. Also ist $D := P \cap Q \neq 1$. Sei $N := \langle \mathrm{N}_P(D), \mathrm{N}_Q(D)\rangle$. Ist N in einer p-Sylowgruppe S von G enthalten, so hat man $D < \mathrm{N}_P(D) \leq P \cap S$ und $D < \mathrm{N}_Q(D) \leq Q \cap S$ nach Satz 4.8. Die Wahl von P und Q liefert dann den Widerspruch $P = S = Q$. Also enthält N eine q-Sylowgruppe T von G. Aus Ordnungsgründen ist dann $G = PT$. Für jedes $g \in G$ existieren daher $x \in P$ und $y \in T \leq N$ mit $g = xy$ und $gDg^{-1} = xyDy^{-1}x^{-1} = xDx^{-1} \leq P$. Folglich ist $K := \langle gDg^{-1} : g \in G\rangle \leq P$ und $K \trianglelefteq G$. Nach Wahl von G sind K und G/K auflösbar. Also ist auch G auflösbar. □

5 Komplemente und Hallgruppen

Definition 5.1. Sei $N \trianglelefteq G$. Eine Untergruppe $H \leq G$ mit $G = NH$ und $H \cap N = 1$ nennt man *Komplement* von N in G.

Bemerkung 5.2.

(i) Man beachte, dass ein Komplement im obigen Sinn kein mengentheoretisches Komplement ist!

(ii) Ist H ein Komplement von $N \trianglelefteq G$, so lässt sich jedes Element $g \in G$ eindeutig in der Form $g = xh$ mit $x \in N$ und $h \in H$ schreiben. Ist nämlich auch $g = x'h'$ mit $x' \in N$ und $h' \in H$, so folgt $(x')^{-1}x = h'h^{-1} \in N \cap H = 1$.

(iii) Eine *exakte Folge* ist eine Folge von Gruppenhomomorphismen

$$\cdots \longrightarrow G_i \xrightarrow{\alpha_i} G_{i+1} \xrightarrow{\alpha_{i+1}} G_{i+2} \longrightarrow \cdots$$

mit $\alpha_i(G_i) = \operatorname{Ker}(\alpha_{i+1})$ für alle i. Eine *kurze exakte Folge* hat die Form

$$1 \longrightarrow N \xrightarrow{\alpha} G \xrightarrow{\beta} H \longrightarrow 1.$$

Es gilt dann $N \cong \alpha(N) = \operatorname{Ker}(\beta) \trianglelefteq G$ und $G/N = G/\operatorname{Ker}(\beta) \cong \beta(G) = H$ (α ist injektiv und β ist surjektiv). Die Folge *zerfällt*, falls ein Homomorphismus $\gamma : H \to G$ mit $\beta \circ \gamma = \mathrm{id}_H$ existiert. Ggf. ist $\gamma(H) \cong H$ mit $\gamma(H) \cap \operatorname{Ker}(\beta) = 1$ und $G = \operatorname{Ker}(\beta)\gamma(H)$.

(iv) Hat $N \trianglelefteq G$ ein Komplement H, so erhält man durch Einbettung eine zerfallende exakte Folge $1 \to N \hookrightarrow G \twoheadrightarrow H \to 1$.

Beispiel 5.3.

(i) In einer elementarabelschen Gruppe hat jede Untergruppe (Normalteiler) ein Komplement (lineare Algebra).

(ii) Nach Satz 4.8 hat jede Sylowgruppe einer nilpotenten Gruppe ein Komplement.

(iii) $\langle (1,2) \rangle$ ist ein Komplement von A_3 in S_3.

(iv) Die Untergruppe C_2 von C_4 besitzt *kein* Komplement, denn $C_4 \ncong C_2^2$.

Bemerkung 5.4. Im Folgenden betrachten wir Homomorphismen der Form $G \to \operatorname{Aut}(H)$, wobei G und H Gruppen sind. Wegen $\operatorname{Aut}(H) \leq \operatorname{Sym}(H)$ operiert dann G auf H. Für $g \in G$ und $x, y \in H$ gilt dabei ${}^g(xy) = ({}^gx)({}^gy)$.

Lemma 5.5. *Sei $\varphi : H \to \operatorname{Aut}(N)$ ein Homomorphismus für Gruppen H, N. Dann wird $G := N \times H$ mittels*

$$\boxed{(x,g) * (y,h) := (x({}^gy), gh)} \qquad (x, y \in N,\ g, h \in H).$$

zu einer Gruppe.

Beweis. Für $x, y, z \in N$ und $g, h, k \in H$ gilt

$$\begin{aligned}((x,g)*(y,h))*(z,k) &= (x({}^{g}y), gh)*(z,k) = (x({}^{g}y)({}^{gh}z), ghk) = (x({}^{g}(y({}^{h}z))), ghk)\\ &= (x,g)*(y({}^{h}z), hk) = (x,g)*((y,h)*(z,k)).\end{aligned}$$

Also ist G assoziativ. Außerdem ist $(1,1)*(x,g) = (x,g)$ und $(1,1)$ ist neutrales Element. Schließlich ist

$$({}^{g^{-1}}(x^{-1}), g^{-1})(x,g) = ({}^{g^{-1}}(x^{-1})({}^{g^{-1}}x), 1) = ({}^{g^{-1}}(x^{-1}x), 1) = (1,1). \qquad \square$$

Definition 5.6. Man nennt G das *semidirekte Produkt* von N mit H und schreibt $G = N \rtimes_\varphi H$.

Bemerkung 5.7.

(i) Ist die Operation φ im Kontext klar oder unwesentlich, so schreibt man auch $N \rtimes H$. Insbesondere wählt man im Fall $H \leq \mathrm{Aut}(N)$ oft die Inklusionsabbildung $\varphi : H \hookrightarrow \mathrm{Aut}(N)$.

(ii) Ist φ trivial, so ist offensichtlich $N \rtimes_\varphi H \cong N \times H$.

(iii) Im Gegensatz zum direkten Produkt kann man beim semidirekten Produkt die Faktoren nicht vertauschen.

(iv) Wir beweisen nun die nicht-kommutative Version von Lemma 2.7.

Lemma 5.8. *Sei $N \trianglelefteq G$ mit Komplement $H \leq G$. Dann ist $G \cong N \rtimes H$. Ist umgekehrt ein semidirektes Produkt $G = N \rtimes_\varphi H$ gegeben, so existiert ein Normalteiler $\widetilde{N} \trianglelefteq G$ mit Komplement $\widetilde{H} \leq G$, sodass $\widetilde{N} \cong N$ und $\widetilde{H} \cong H$ gilt.*

Beweis. Sei $\varphi : H \to \mathrm{Aut}(N)$ die Konjugationsabbildung. Wir zeigen, dass die Abbildung

$$F : G \to N \rtimes_\varphi H, \quad xh \mapsto (x,h) \quad (x \in N, h \in H)$$

ein Isomorphismus ist. Für $x, y \in N$ und $h, k \in H$ gilt

$$F(xh \cdot yk) = F(x(hyh^{-1}) \cdot hk) = (x(hyh^{-1}), hk) = (x({}^{h}y), hk) = (x,h)*(y,k) = F(x,h)*F(y,k).$$

Also ist F ein Homomorphismus. Offenbar ist F auch bijektiv.

Für die zweite Behauptung betrachten wir die kurze exakte Folge

$$1 \to N \overset{x \mapsto (x,1)}{\longrightarrow} G \overset{(x,h) \mapsto h}{\longrightarrow} H \to 1$$

Nach Bemerkung 5.2 genügt es zu zeigen, dass diese Folge zerfällt. Dies sieht man mit dem Homomorphismus $H \to G$, $h \mapsto (1,h)$. $\square$

Beispiel 5.9. Nach Aufgabe 1 besitzt jede abelsche Gruppe A den Automorphismus $x \mapsto x^{-1}$ $(x \in A)$. Ist $\varphi : C_2 \to \mathrm{Aut}(A)$ der entsprechende Homomorphismus, so kann man $A \rtimes_\varphi C_2$ konstruieren. Für $n \geq 3$ nennt man $D_{2n} := C_n \rtimes_\varphi C_2$ die *Diedergruppe* der Ordnung $2n$. Offenbar ist dann φ nicht-trivial und D_{2n} ist nicht-abelsch. Andererseits ist $D'_{2n} \leq C_n$ und D_{2n} ist metabelsch.

Satz 5.10. *Sei $|G| = pq$ mit Primzahlen $p \leq q$. Dann gilt einer der folgenden Aussagen:*

(i) $G \cong C_{pq}$.

(ii) $G \cong C_p^2$.

(iii) $p \mid q-1$ *und* $G \cong C_q \rtimes C_p$.

Beweis. Im Fall $p = q$ ist G abelsch zum Beispiel nach Satz 4.16. Dann folgt die Behauptung aus Satz 2.10. Sei nun also $p < q$. Sei $P \in \mathrm{Syl}_p(G)$ und $Q \in \mathrm{Syl}_q(G)$. Nach Lagrange ist $|G : \mathrm{N}_G(Q)| \mid p$ und nach Sylow ist $|G : \mathrm{N}_G(Q)| \equiv 1 \pmod{q}$. Dies zeigt $Q \trianglelefteq G$. Offenbar ist P ein Komplement von Q, d. h. $G = Q \rtimes P$. Nun ist $|\mathrm{Aut}(Q)| = \varphi(q) = q-1$ nach Satz 2.4. Im Fall $p \nmid q-1$ kann P also nur trivial auf Q operieren und man erhält $G = P \oplus Q \cong C_{pq}$. Im Fall $p \mid q-1$ kann man P in $\mathrm{Aut}(Q)$ einbetten und die nichtabelsche Gruppe $Q \rtimes P$ konstruieren. □

Beispiel 5.11. Nach Satz 5.10 sind Gruppen der Ordnung 15 sind zyklisch.

Satz 5.12 (Schur-Zassenhaus)**.** *Sei* $N \trianglelefteq G$ *mit* $\mathrm{ggT}(|N|, |G/N|) = 1$. *Dann besitzt* N *ein Komplement in* G. *Ist* N *oder* G/N *auflösbar, so sind je zwei Komplemente von* N *in* G *unter* N *konjugiert.*

Beweis.

Schritt 1: Existenz.
Induktion nach $|G|$: Wir dürfen sicher $1 < N < G$ annehmen. Sei $1 \neq P \in \mathrm{Syl}_p(N)$. Dann ist $\mathrm{N}_N(P) \trianglelefteq \mathrm{N}_G(P)$ und $\mathrm{N}_G(P)/\mathrm{N}_N(P) = \mathrm{N}_G(P)/\mathrm{N}_G(P) \cap N \cong \mathrm{N}_G(P)N/N \leq G/N$. Im Fall $\mathrm{N}_G(P) < G$ besitzt $\mathrm{N}_N(P)$ nach Induktion ein Komplement K in $\mathrm{N}_G(P)$. Nach Bemerkung 4.4 ist $G = N\,\mathrm{N}_G(P) = N\,\mathrm{N}_N(P)K = NK$ und $N \cap K = N \cap \mathrm{N}_G(P) \cap K = \mathrm{N}_N(P) \cap K = 1$. Wir können also $P \trianglelefteq G$ annehmen. Nach Satz 4.6 ist auch $1 \neq \mathrm{Z}(P) \trianglelefteq G$. Nach Induktion besitzt $N/\mathrm{Z}(P)$ ein Komplement $K/\mathrm{Z}(P)$ in $G/\mathrm{Z}(P)$. Dann ist $G = NK$ und $N \cap K = \mathrm{Z}(P)$. Es genügt also zu zeigen, dass $\mathrm{Z}(P)$ ein Komplement in K hat. Wir können daher annehmen, dass N abelsch ist.

Sei $\mathcal{R}$ die Menge aller Repräsentantensysteme für G/N. Für $R, S \in \mathcal{R}$ sei

$$(R, S) := \prod_{\substack{(x,y) \in R \times S, \\ xN = yN}} xy^{-1} \in N.$$

Die Reihenfolge der Faktoren spielt dabei keine Rolle, denn N ist abelsch. Außerdem ist $(R, R) = 1$, $(S, R) = (R, S)^{-1}$ und $(R, S)(S, T) = (R, T)$ für $R, S, T \in \mathcal{R}$. Folglich ist $\sim$ mit

$$R \sim S :\Longleftrightarrow (R, S) = 1$$

eine Äquivalenzrelation auf $\mathcal{R}$. Offenbar operiert G durch Linksmultiplikation auf $\mathcal{R}$. Dabei gilt $(gR, gS) = g(R, S)g^{-1}$ für $g \in G$ und $R, S \in \mathcal{R}$. Also operiert G auch auf der Menge $\overline{\mathcal{R}}$ der Äquivalenzklassen von $\mathcal{R}$ unter $\sim$. Wir zeigen, dass N transitiv operiert. Seien dafür $R, S \in \mathcal{R}$ beliebig. Der euklidische Algorithmus liefert ein $n \in \mathbb{N}$ mit $n|G/N| \equiv 1 \pmod{|N|}$. Sei $\alpha := (R, S)^{-n} \in N$. Dann gilt

$$(\alpha R, S) = \prod_{\substack{(x,y) \in R \times S, \\ xN = \alpha xN = yN}} \alpha x y^{-1} = \alpha^{|G/N|} \prod_{\substack{(x,y) \in R \times S, \\ xN = yN}} xy^{-1} = (R, S)^{-n|G/N|}(R, S) = 1.$$

Also ist N transitiv auf $\overline{\mathcal{R}}$ und Frattini zeigt $G = NG_{\overline{R}}$ für $\overline{R} \in \overline{\mathcal{R}}$. Sei $g \in N \cap G_{\overline{R}}$. Wie eben ist dann $1 = (gR, R) = g^{|G/N|}$ und $g = g^{n|G/N|} = 1$. Somit ist $G_{\overline{R}}$ ein Komplement von N in G.

Schritt 2: Eindeutigkeit.
Fall 1: N auflösbar.
Induktion nach $|N|$: Nehmen wir zunächst an, dass N abelsch ist. Jedes Komplement K von N in G liegt dann in $\mathcal{R}$ (siehe Schritt 1). Nach Bemerkung 1.17 genügt es zu zeigen, dass $K = G_{\overline{K}}$ gilt. Für $x \in K$ ist $(xK, K) = (K, K) = 1$ und es folgt $K \subseteq G_{\overline{K}}$. Andererseits ist $|K| = |G_{\overline{K}}|$ und wir sind fertig.

Sei nun $1 < N' < N$. Seien K_1 und K_2 Komplemente von N in G. Dann sind K_1N'/N' und K_2N'/N' Komplemente von N/N' in G/N'. Nach Induktion existiert ein $x \in N$ mit $xK_1x^{-1}N' = xK_1N'x^{-1} = K_2N'$. Also sind xK_1x^{-1} und K_2 Komplemente von N' in K_2N'. Nach Induktion existiert ein $y \in N'$ mit $yxK_1x^{-1}y^{-1} = K_2$.

Fall 2: G/N auflösbar.
Induktion nach $|G/N|$: Seien K_1 und K_2 Komplemente von N in G. Dann ist $K_1 \cong G/N \cong K_2$ auflösbar. Sei M_1 ein minimaler Normalteiler von K_1. Nach Satz 2.27 ist M_1 eine elementarabelsche p-Gruppe. Im Fall $M_1 = K_1$ sind K_1 und K_2 nach Sylow in G konjugiert. Wegen $G = NK_1 = K_1N$ sind K_1 und K_2 dann auch unter N konjugiert. Sei also $M_1 < K_1$ und $M_2 := K_2 \cap NM_1 \trianglelefteq K_2$. Nach Dedekind ist $NM_2 = N(K_2 \cap NM_1) = NK_2 \cap NM_1 = NM_1$. Induktion liefert ein $x \in N$ mit $xM_1x^{-1} = M_2$. Insbesondere ist $xK_1x^{-1} \leq x\,\mathrm{N}_G(M_1)x^{-1} = \mathrm{N}_G(M_2)$ und $K_2 \leq \mathrm{N}_G(M_2)$. Nach Dedekind sind xK_1x^{-1}/M_2 und K_2/M_2 Komplemente von $\mathrm{N}_N(M_2)M_2/M_2$ in $\mathrm{N}_G(M_2)/M_2$. Nach Induktion existiert also ein $y \in \mathrm{N}_N(M_2)$ mit $yxK_1x^{-1}y^{-1}/M_2 = K_2/M_2$. Die Behauptung folgt. □

Bemerkung 5.13. Aus der Bedingung $\mathrm{ggT}(|N|, |G/N|) = 1$ folgt, dass $|N|$ oder $|G/N|$ ungerade ist. Nach dem tiefliegenden Satz von Feit und Thompson ist die Auflösbarkeitsbedingung in Satz 5.12 also eigentlich überflüssig (der Beweis hat 250 Seiten).

Definition 5.14. Sei π eine Menge von Primzahlen. Eine Untergruppe $H \leq G$ heißt *(π-)Hallgruppe* von G, falls H eine π-Gruppe ist und kein Primteiler von $|G : H|$ in π liegt. In diesem Fall ist $\mathrm{ggT}(|H|, |G : H|) = 1$.

Beispiel 5.15.

(i) Die p-Hallgruppen sind genau die p-Sylowgruppen.

(ii) Ist G nilpotent, so ist $\mathrm{O}_\pi(G)$ die einzige π-Hallgruppe von G (Satz 4.8).

(iii) A_5 besitzt *keine* $\{3, 5\}$-Hallgruppe.

Satz 5.16 (Hall)**.** *Sei G auflösbar und π eine Primzahlmenge. Dann gilt*

(i) G besitzt eine π-Hallgruppe.

(ii) Je zwei π-Hallgruppen sind in G konjugiert.

(iii) Jede π-Untergruppe von G liegt in einer π-Hallgruppe.

Beweis. Wir können annehmen, dass alle Primzahlen in π die Gruppenordnung $|G|$ teilen. Wir schreiben $|G| = rs$ mit $\mathrm{ggT}(r, s) = 1$, wobei π die Menge der Primteiler von r ist. Wir zeigen zunächst (iii) durch Induktion nach $|G|$. Offenbar dürfen wir $G \neq 1$ annehmen. Sei $U \leq G$ mit $|U| \mid r$. Sei M ein minimaler Normalteiler von G. Da G auflösbar ist, ist $|M| = p^n$ für eine Primzahlpotenz $p^n > 1$. Sei zunächst $p^n \mid r$ und $r' := r/p^n$. Dann ist $|G/M| = r's$ und Induktion zeigt $UM/M \leq K/M \leq G/M$ mit $|K/M| = r'$. Sicher ist dann $U \leq K$ und $|K| = r$. Wir können nun $p^n \mid s$ voraussetzen. Dann ist nach Induktion wieder $UM/M \leq K/M \leq G/M$ mit $|K/M| = r$. Also hat man $|K| = p^nr$ und Schur-Zassenhaus liefert ein $L \leq K$ mit $|L| = r$. Offenbar ist $M(L \cap UM) = ML \cap UM = K \cap UM = UM$ und damit $|L \cap UM| = |U|$. Wieder nach Schur-Zassenhaus (angewendet auf $M \trianglelefteq MU$) existiert ein $g \in M$ mit $U = g(L \cap UM)g^{-1} \leq gLg^{-1}$. Damit ist (iii) bewiesen und mit $U = 1$ ergibt sich (i).

Seien nun H und K Untergruppen von G der Ordnung r. Wie oben nehmen wir zunächst $p^n \mid r$ an. Dann kann die Ordnung von $MH \leq G$ nicht größer als r sein. Dies zeigt $M \leq H$ und analog $M \leq K$. Nach Induktion sind H/M und K/M in G/M konjugiert. Sicher sind dann H und K in G konjugiert.

Sei nun $p^n \mid s$. Mit dem gleichen Argument sind dann HM und KM in G konjugiert. Insbesondere existiert ein $g \in G$ mit $gHg^{-1} \leq KM$. Nach Schur-Zassenhaus sind dann auch gHg^{-1} und K (in KM) konjugiert. Damit folgt (ii). □

Bemerkung 5.17. Man kann umgekehrt zeigen, dass G auflösbar ist, falls π-Hallgruppen für jede Primzahlmenge π existieren. Dies beinhaltet Burnside's p^aq^b-Satz (siehe Charaktertheorie). Der folgende Satz ist nützlich für die Konstruktion von minimalen Gegenbeispielen.

Satz 5.18 (Schmidt)**.** *Sei jede echte Untergruppe von G nilpotent, aber G selbst nicht. Dann ist $G \cong Q \rtimes C_{p^n}$ mit $Q \in \mathrm{Syl}_q(G)$ für Primzahlen p, q und $n \geq 1$.*

Beweis. Induktion nach $|G|$: O. B. d. A. sei $G \neq 1$. Nehmen wir zunächst an es existiert ein echter Normalteiler $N \neq 1$. Nach Voraussetzung ist N nilpotent. Für $U/N < G/N$ ist $U < G$ nilpotent und damit auch U/N. Nach Induktion ist also G/N auflösbar. Daher ist auch G auflösbar. Nehmen wir nun an, dass G nichtabelsch und einfach ist. Seien M_1 und M_2 zwei verschiedene maximale Untergruppe von G, sodass $D := M_1 \cap M_2$ möglichst groß ist. Nehmen wir $D \neq 1$ an. Nach Satz 4.8 ist dann

$$D < \mathrm{N}_{M_i}(D) \leq \mathrm{N}_G(D) < G$$

für $i = 1, 2$. Nun liegt $\mathrm{N}_G(D)$ in einer maximalen Untergruppe $M_3 < G$. Wegen $\mathrm{N}_{M_i}(D) \leq M_i \cap M_3$ ist dann $M_i = M_3$ nach Wahl von M_1 und M_2. Dies liefert aber den Widerspruch $M_1 = M_3 = M_2$. Also ist $D = 1$, d. h. je zwei verschiedene maximale Untergruppen von G schneiden sich trivial. Sei $M_1, \ldots, M_s$ ein Repräsentantensystem für die Konjugationsklassen von maximalen Untergruppen. Wegen $\mathrm{N}_G(M_i) = M_i$ hat M_i genau $|G : M_i|$ viele Konjugierte. Es gilt daher

$$|G| = 1 + \sum_{i=1}^{s}(|M_i| - 1)|G : M_i| = 1 + s|G| - \sum_{i=1}^{s}|G : M_i| \geq 1 + s|G| - s\frac{|G|}{2} = 1 + s\frac{|G|}{2}$$

und $s = 1$. Dann ist aber $|G| = 1 + |G| - |G : M_1|$ und $M_1 = G$. Dieser Widerspruch zeigt schließlich, dass G auflösbar ist.

Sei nun $|G| = p_1^{a_1} \ldots p_m^{a_m}$ die Primfaktorzerlegung von $|G|$. Da G nicht nilpotent ist, gilt $m \geq 2$. Sei N ein maximaler Normalteiler von G. Dann ist G/N einfach und auflösbar. Also ist $|G/N|$ eine Primzahl, sagen wir $|G/N| = p_1 =: p$. Nach Voraussetzung ist N nilpotent und besitzt daher normale Sylowgruppen $P_i \in \mathrm{Syl}_{p_i}(N)$ für $i = 2, \ldots, m$. Offenbar ist dann $P_i \in \mathrm{Syl}_{p_i}(G)$. Außerdem ist P_i charakteristisch in N und damit normal in G. Sei außerdem $P_1 \in \mathrm{Syl}_p(G)$. Nehmen wir indirekt $m \geq 3$ an. Für $i = 2, \ldots, m$ ist dann $P_1P_i < G$ nilpotent. Dies zeigt $P_i \leq \mathrm{N}_G(P_1)$ und $P_1 \trianglelefteq G$. Dann wäre aber G nilpotent. Also ist $m = 2$ und wir können $Q := P_2$ setzen. Nehmen wir schließlich an, dass P_1 nicht zyklisch ist. Für $x \in P_1$ gilt dann $\langle x \rangle P_2 < G$ und $P_2 \leq \mathrm{C}_G(x)$. Dann ist aber $P_2 \leq \mathrm{C}_G(P_1)$ und wieder $P_1 \trianglelefteq G$. Folglich muss P_1 zyklisch sein und die Behauptung ist bewiesen. □

Satz 5.19 (Wielandt)**.** *Sei $H \leq G$ eine nilpotente Hallgruppe und $U \leq G$ mit $|U| \mid |H|$. Dann existiert ein $g \in G$ mit $gUg^{-1} \leq H$.*

Beweis. Induktion nach $|U|$. O. B. d. A. sei $U \neq 1$. Jede echte Untergruppe von U ist dann zu einer Untergruppe von H konjugiert. Insbesondere ist jede echte Untergruppe von U nilpotent. Nach Satz 5.18 existiert eine Zerlegung $U = Q \rtimes P$ mit $1 \neq P \in \mathrm{Syl}_p(U)$ und $Q \trianglelefteq U$ (auch wenn U nilpotent ist). Analog ist $H = H_1 \oplus H_2$ mit $H_1 \in \mathrm{Syl}_p(H) \subseteq \mathrm{Syl}_p(G)$. Nach Induktion existiert ein $x \in G$ mit $xQx^{-1} \leq H$ und damit $xQx^{-1} \leq \mathrm{O}_{p'}(H) = H_2$. Es gilt dann $\langle H_1, xUx^{-1} \rangle \leq \mathrm{N}_G(xQx^{-1})$. Wegen $H_1 \in \mathrm{Syl}_p(\mathrm{N}_G(xQx^{-1}))$ existiert ein $y \in \mathrm{N}_G(xQx^{-1})$ mit $yxPx^{-1}y^{-1} \leq H_1$. Wegen $yxQx^{-1}y^{-1} = xQx^{-1} \leq H_2$ ist dann

$$yxUx^{-1}y^{-1} = (yxPx^{-1}y^{-1})(yxQx^{-1}y^{-1}) \leq H_1H_2 = H. \qquad \square$$

Satz 5.20 (Galois)**.** *Sei N ein minimaler Normalteiler der auflösbaren Gruppe G mit $\mathrm{C}_G(N) \leq N$. Dann besitzt N ein Komplement in G und je zwei Komplemente sind in G konjugiert.*

Beweis. Bekanntlich ist N eine elementarabelsche p-Gruppe für eine Primzahl p. Wir können $N < G$ annehmen. Sei M/N ein minimaler Normalteiler von G/N. Dann ist M/N eine elementarabelsche q-Gruppe für eine Primzahl q. Nehmen wir zunächst $q = p$ an. Dann ist M ein p-Normalteiler von G und M operiert durch Konjugation auf N. Die Bahnengleichung liefert

$$0 \equiv |N| \equiv |\mathrm{C}_N(M)| \pmod{p}.$$

Insbesondere ist $1 \neq \mathrm{C}_N(M) \trianglelefteq G$. Da N minimal ist, folgt $\mathrm{C}_N(M) = N$ und $M \subseteq \mathrm{C}_G(N) = N$. Dieser Widerspruch zeigt $q \neq p$. Sei $Q \in \mathrm{Syl}_q(M)$. Dann ist $M = QN$ und $G = \mathrm{N}_G(Q)M = \mathrm{N}_G(Q)QN = \mathrm{N}_G(Q)N$ nach Bemerkung 4.4. Offenbar ist $\mathrm{N}_G(Q) \cap N \trianglelefteq \mathrm{N}_G(Q)$. Da N abelsch ist, gilt auch $\mathrm{N}_G(Q) \cap N \trianglelefteq N$. Insgesamt ist also $\mathrm{N}_G(Q) \cap N \trianglelefteq G$. Die Minimalität von N zeigt $\mathrm{N}_G(Q) \cap N \in \{1, N\}$. Nehmen wir an, dass der Fall $N \subseteq \mathrm{N}_G(Q)$ eintritt. Wie oben ist dann $G = \mathrm{N}_G(Q)N = \mathrm{N}_G(Q)$, also $Q \trianglelefteq G$. Aus Ordnungsgründen ist $N \cap Q = 1$ und damit $Q \subseteq \mathrm{C}_G(N) = N$. Widerspruch. Also ist $\mathrm{N}_G(Q) \cap N = 1$ und $\mathrm{N}_G(Q)$ ist ein Komplement von N.

Sei nun $K \leq G$ ein beliebiges Komplement von N in G. Dann ist $L := K \cap M \trianglelefteq K$ und $M = NK \cap M = N(K \cap M) = NL$ nach Dedekind. Wegen $L \cap N \subseteq K \cap N = 1$ ist $|L| = |M : N| = |Q|$. Nach Sylow existiert ein $x \in M$ mit $xQx^{-1} = L$. Es folgt $K \leq \mathrm{N}_G(L) = \mathrm{N}_G(xQx^{-1}) = x\,\mathrm{N}_G(Q)x^{-1}$. Wegen $|K| = |\mathrm{N}_G(Q)|$ ist K zu $\mathrm{N}_G(Q)$ konjugiert. Dies zeigt die zweite Behauptung. □

6 Permutationsgruppen

Definition 6.1. Eine *Permutationsgruppe* G ist eine Untergruppe von $\mathrm{Sym}(\Omega)$ für eine nichtleere Menge Ω. Dabei ist $|\Omega|$ der *Grad* von G.

Bemerkung 6.2.

(i) Operiert G treu auf Ω, so erhält man einen Monomorphismus $f : G \to \mathrm{Sym}(\Omega)$. Man kann also G mit der Permutationsgruppe $f(G)$ identifizieren. Umgekehrt operiert jede Permutationsgruppe $G \leq \mathrm{Sym}(\Omega)$ treu auf Ω mittels $G \hookrightarrow \mathrm{Sym}(\Omega)$.

(ii) Ist $f : G \to \mathrm{Sym}(\Omega)$ eine beliebige Operation, so wird $G/\operatorname{Ker}(f)$ zu einer Permutationsgruppe.

Satz 6.3 (Cayley)**.** *Jede Gruppe operiert treu auf sich selbst und wird somit zur Permutationsgruppe.*

Beweis. Wir betrachten die Operation $f : G \to \mathrm{Sym}(\Omega)$ durch Linksmultiplikation. Für $x \in \operatorname{Ker}(f)$ gilt $1 = {}^x1 = x1 = x$. Also ist f treu. □

Satz 6.4 (Burnsides Lemma)**.** *Sei s die Anzahl der Bahnen einer Operation der endlichen Gruppe G auf Ω. Sei $f(g) := |\{\omega \in \Omega : {}^g\omega = \omega\}|$ die Anzahl der Fixpunkte von $g \in G$. Dann gilt*

$$s = \frac{1}{|G|} \sum_{g \in G} f(g).$$

Beweis. Seien $\omega_1, \ldots, \omega_s$ Repräsentanten für die Bahnen von G (beachte $|G| < \infty$). Für $x \in G$ und $\omega \in \Omega$ gilt $G_{{}^x\omega} = xG_\omega x^{-1}$. Insbesondere hängt $|G_{\omega_i}|$ nicht von der Wahl von ω_i ab. Es gilt nun

$$\sum_{g \in G} f(g) = |\{(g, \omega) \in G \times \Omega : {}^g\omega = \omega\}| = \sum_{\omega \in \Omega} |G_\omega| = \sum_{i=1}^{s} |{}^G\omega_i||G_{\omega_i}| = \sum_{i=1}^{s} |G : G_{\omega_i}||G_{\omega_i}| = s|G|. \quad \square$$

Beispiel 6.5. Wie viele verschiedene Halsketten mit drei Perlen kann man herstellen, wenn Perlen in drei verschiedenen Farben zur Verfügung stehen? Prinzipiell gibt es $3^3 = 27$ mögliche Anordnungen der Perlen. Sei $\Omega := \{1, 2, 3\}^3$ die entsprechende Menge. Dann stimmen beispielsweise die Halsketten $(1, 2, 3)$, $(2, 3, 1)$ und $(3, 2, 1)$ alle überein. Ordnet man die Perlen als regelmäßiges Dreieck an, so interessieren wir uns für die Anzahl der Bahnen unter der Symmetriegruppe S des Dreiecks. Offenbar besitzt S drei Drehungen und drei Spiegelungen. Man sieht leicht $S \cong D_6 \cong S_3$. Wir wenden Satz 6.4 mit S und Ω an. Die Identität $1 \in S$ hat offenbar 27 Fixpunkte. Jede nicht-triviale Drehung lässt nur die drei einfarbigen Ketten fest. Jede Spiegelung hat neun Fixpunkte (z. B. (a, b, a) mit $a, b \in \{1, 2, 3\}$). Die gesuchte Anzahl der Halsketten ist daher

$$\frac{1}{6}(27 + 3 + 3 + 9 + 9 + 9) = 10.$$

Bemerkung 6.6. Burnsides Lemma ist immer dann nützlich, wenn $|\Omega|$ zu groß ist, um die Bahnen explizit zu zählen. Beispielsweise gibt es 43.252.003.274.489.856.000 verschiedene Zustände des $3 \times 3 \times 3$-Zauberwürfels. Unter der Symmetriegruppe $S_4 \times C_2$ des Würfels reduziert sich diese Zahl auf 901.083.404.981.813.616.

Definition 6.7. Zwei Operationen $G \to \mathrm{Sym}(\Omega)$ und $G \to \mathrm{Sym}(\Omega')$ sind *isomorph* (oder *ähnlich*), falls es eine Bijektion $\varphi : \Omega \to \Omega'$ und ein $\alpha \in \mathrm{Aut}(G)$ mit ${}^{\alpha(g)}\varphi(\omega) = \varphi({}^g\omega)$ für $g \in G$ und $\omega \in \Omega$ gibt. Ggf. sind Ω und Ω' *isomorphe G-Mengen*. In den Anwendungen ist oft $\alpha = \mathrm{id}_G$.

Bemerkung 6.8. Wie üblich haben zwei isomorphe Operationen die gleichen Eigenschaften (trivial, treu, transitiv, ...). Man interessiert sich daher in der Regel nur für Operationen bis auf Isomorphie.

Satz 6.9. *Sei $\omega_1, \dots, \omega_s$ ein Repräsentantensystem für die Bahnen einer Operation $f : G \to \mathrm{Sym}(\Omega)$. Dann ist f isomorph zu der Operation von G auf $\Delta := \bigsqcup_{i=1}^{s} G/G_{\omega_i}$ (disjunkte Vereinigung) durch Linksmultiplikation.*

Beweis. Nach Satz 1.19 ist die Abbildung $\varphi : \Delta \to \Omega$, $gG_{\omega_i} \mapsto {}^g\omega_i$ eine wohldefinierte Bijektion. Für $g \in G$ und $xG_{\omega_i} \in \Delta$ gilt außerdem ${}^g\varphi(xG_{\omega_i}) = {}^g({}^x\omega_i) = {}^{gx}\omega_i = \varphi(gxG_{\omega_i}) = \varphi({}^g(xG_{\omega_i}))$. □

Bemerkung 6.10. Man kann jede Operation von G also auch durch Angabe von Untergruppen beschreiben (je eine Untergruppe pro Bahn).

Definition 6.11. Eine transitive Operation $G \to \mathrm{Sym}(\Omega)$ heißt *regulär*, falls $|G| = |\Omega|$ gilt.

Bemerkung 6.12. Sei $f : G \to \mathrm{Sym}(\Omega)$ regulär und sei $\omega \in \Omega$. Da f transitiv ist, gilt $|G| = |\Omega| = |G : G_\omega|$, d. h. $G_\omega = 1$. Insbesondere ist f treu. Nach Satz 6.9 ist f isomorph zu der Operation aus Satz 6.3. Man kann also von „der“ regulären Operation von G sprechen.

Definition 6.13. Sei $f : G \to \mathrm{Sym}(\Omega)$ eine transitive, nicht-triviale Operation. Eine Teilmenge $\Delta \subseteq \Omega$ mit $1 < |\Delta| < |\Omega|$ heißt *Block* von f, falls für jedes $g \in G$ die Mengen ${}^g\Delta$ und Δ entweder gleich oder disjunkt sind. Existieren Blöcke, so heißt f *imprimitiv* und anderenfalls *primitiv*.

Bemerkung 6.14.

(i) Sei Δ ein Block einer Operation $G \to \mathrm{Sym}(\Omega)$ und sei $x \in G$. Dann ist sicher $|{}^x\Delta| = |\Delta|$. Für $g \in G$ gilt ${}^g({}^x\Delta) \cap {}^x\Delta = {}^{gx}\Delta \cap {}^x\Delta = {}^x({}^{x^{-1}gx}\Delta \cap \Delta) \in \{{}^x\Delta, \varnothing\}$. Daher ist auch ${}^x\Delta$ ein Block. Da G transitiv auf Ω operiert, ist $\mathcal{B} := \{{}^g\Delta : g \in G\}$ ein Partition von Ω. Insbesondere ist $|\Omega| = |\Delta||\mathcal{B}|$ und $\boxed{|\Delta| \mid |\Omega| \mid |G|.}$ Außerdem operiert G sicher transitiv auf $\mathcal{B}$.

(ii) Beachte: Für nicht-transitive Operationen sind Blöcke nicht definiert!

Beispiel 6.15.

(i) Nach Bemerkung 6.14 ist jede transitive Operation mit Primzahlgrad primitiv.

(ii) Nach (i) sind die natürlichen Operationen von S_2, S_3 und A_3 primitiv. Sei nun $n \geq 4$ und $\Delta \subseteq \{1, \dots, n\}$ mit $1 < |\Delta| < n$. Für verschiedene Elemente $\alpha, \beta \in \Delta$ existiert dann ein 3-Zyklus $g \in A_n$ mit ${}^g\alpha = \alpha$ und ${}^g\beta \in \Omega \setminus \Delta$. Also ist Δ kein Block und S_n und A_n sind primitiv.

(iii) Die *Kleinsche Vierergruppe* $V_4 := \langle (1,2)(3,4), (1,3)(2,4) \rangle$ operiert regulär und imprimitiv auf $\{1,2,3,4\}$ (jede 2-elementige Teilmenge ist ein Block).

Satz 6.16. *Eine transitive Operation $G \to \mathrm{Sym}(\Omega)$ ist genau dann primitiv, falls G_ω für ein (oder alle) $\omega \in \Omega$ eine maximale Untergruppe von G ist.*

Beweis. Sei zunächst Δ ein Block von G und $\omega \in \Delta$. Für $g \in G_\omega$ ist $\omega = {}^g\omega \in \Delta \cap {}^g\Delta \neq \varnothing$ und damit ${}^g\Delta = \Delta$. Dies zeigt $G_\omega \leq \{g \in G : {}^g\Delta = \Delta\} =: G_{(\Delta)}$. Wegen $|\Delta| > 1$ ist $G_\omega < G_{(\Delta)}$. Andererseits ist $G_{(\Delta)} < G$, da $G_{(\Delta)}$ intransitiv auf Ω operiert ($\Delta \neq \Omega$). Also ist G_ω nicht maximal. Sei nun $\omega' \in \Omega$ beliebig. Dann existiert ein $g \in G$ mit ${}^g\omega = \omega'$ und $G_{\omega'} = gG_\omega g^{-1}$. Somit ist kein Stabilisator maximal.

Sei nun umgekehrt G_ω nicht maximal für ein $\omega \in \Omega$. Im Fall $G_\omega = G$ operiert G trivial und damit nicht primitiv. Sei also $G_\omega < H < G$. Wir setzen $\Delta := {}^H\omega$. Wegen $G_\omega < H$ ist $|\Delta| > 1$. Außerdem ist $|\Delta| = |{}^H\omega| = |H : H_\omega| = |H : G_\omega| < |G : G_\omega| = |\Omega|$. Sei nun $g \in G$ mit $\delta \in \Delta \cap {}^g\Delta$. Dann existieren $h, h' \in H$ mit $\delta = {}^h\omega = {}^{gh'}\omega$. Es folgt $h^{-1}gh' \in G_\omega \subseteq H$ und $g \in H$. Also ist ${}^g\Delta = \Delta$ und die Operation ist imprimitiv. □

Satz 6.17. *Sei $G \to \mathrm{Sym}(\Omega)$ eine imprimitive Operation mit Block Δ, der maximal bzgl. Inklusion gewählt ist. Dann ist die Operation von G auf $\mathcal{B} := \{{}^g\Delta : g \in G\}$ primitiv.*

Beweis. Nehmen wir indirekt an, dass ein Block $\mathcal{C} \subseteq \mathcal{B}$ existiert. Wir können $\Delta \in \mathcal{C}$ annehmen. Setze $\Gamma := \bigcup_{C \in \mathcal{C}} C$. Dann ist $|\Delta| < |\Delta||\mathcal{C}| = |\Gamma| < |\Delta||\mathcal{B}| = |\Omega|$. Sei $g \in G$ und $\omega \in \Gamma \cap {}^g\Gamma$. Dann existieren $x, y \in G$ mit $\omega \in {}^x\Delta \cap {}^{gy}\Delta$. Also ist ${}^x\Delta = {}^{gy}\Delta \in \mathcal{C} \cap {}^g\mathcal{C}$ und ${}^g\mathcal{C} = \mathcal{C}$. Dies zeigt ${}^g\Gamma = \Gamma$. Also ist Γ ein Block von G, der Δ echt enthält. Dies widerspricht aber das Maximalität von Δ. □

Bemerkung 6.18. Sei $G \neq 1$ eine Permutationsgruppe auf Ω. Nach Bemerkung 6.2 existiert ein Normalteiler $N_1 \trianglelefteq G$, sodass $G/N_1 \neq 1$ eine transitive Permutationsgruppe ist. Weiter existiert nach Satz 6.17 ein Normalteiler $N_2/N_1 \trianglelefteq G/N_1$, sodass $(G/N_1)/(N_2/N_1) \cong G/N_2$ eine primitive Permutationsgruppe ist. Da auch N_2 treu auf Ω operiert, kann man diesen Prozess mit N_2 statt G wiederholen. Dies liefert eine Folge von Untergruppen $1 = G_1 \trianglelefteq G_2 \trianglelefteq \ldots \trianglelefteq G_k = G$, sodass die Faktoren G_i/G_{i-1} primitive Permutationsgruppen sind. Im Unterschied zu Kompositionsfaktoren oder Hauptfaktoren sind die Faktoren G_i/G_{i-1} aber in keiner Weise eindeutig.

Satz 6.19. *Sei $G \to \mathrm{Sym}(\Omega)$ eine Operation und sei $N \trianglelefteq G$ regulär. Für $\omega \in \Omega$ ist dann die Operation von G_ω auf Ω isomorph zur Operation auf N durch Konjugation.*

Beweis. Nach Voraussetzung ist die Abbildung $\varphi : N \to \Omega$, $x \mapsto {}^x\omega$ eine Bijektion. Für $g \in G_\omega$ und $x \in N$ gilt ${}^g\varphi(x) = {}^{gx}\omega = {}^{(gxg^{-1})g}\omega = {}^{gxg^{-1}}\omega = \varphi({}^g x)$. □

Satz 6.20. *Sei $G \to \mathrm{Sym}(\Omega)$ eine primitive Operation und $N \trianglelefteq G$. Dann operiert N trivial oder transitiv auf Ω.*

Beweis. Sei $\Delta \subseteq \Omega$ eine nicht-triviale Bahn von N (d. h. $|\Delta| > 1$). Für $g \in G$ ist dann ${}^g\Delta$ eine Bahn von $gNg^{-1} = N$. Also ist ${}^g\Delta \cap \Delta \in \{\Delta, \varnothing\}$. Die Primitivität von G liefert $\Delta = \Omega$, d. h. N ist transitiv. □

Satz 6.21. *Sei G eine primitive Permutationsgruppe auf Ω und sei $N \neq 1$ ein auflösbarer Normalteiler von G. Dann besitzt G genau einen minimalen Normalteiler A. Dabei ist $\mathrm{C}_G(A) = A$ und $|\Omega| = |A| = p^n$ für eine Primzahlpotenz p^n. Schließlich ist $G = A \rtimes G_\omega$ für $\omega \in \Omega$.*

Beweis. Sei $A := N^{(k)} > N^{(k+1)} = 1$. Dann ist A abelsch und charakteristisch in N. Also ist $A \trianglelefteq G$. Nach Satz 6.20 operiert A transitiv. Für $\omega \in \Omega$ gilt daher

$$A_\omega = \bigcap_{a \in A} aA_\omega a^{-1} = \bigcap_{a \in A} A_{a\omega} = \bigcap_{\alpha \in \Omega} A_\alpha = 1.$$

Also ist A regulär und $|A| = |\Omega|$. Für jeden weiteren abelschen Normalteiler $1 \neq B \trianglelefteq G$ muss ebenfalls $|B| = |\Omega|$ gelten. Insbesondere ist A minimal und $|A|$ ist eine Primzahlpotenz. Außerdem ist $A \subseteq \mathrm{C}_G(A) =: C$. Für $\omega \in \Omega$ und $a \in A$ gilt wie eben $C_\omega = aC_\omega a^{-1} = C_{a\omega}$. Daher ist auch C regulär und $A = C = \mathrm{C}_G(A)$. Gäbe es einen weiteren minimalen Normalteiler $B \trianglelefteq G$, so wäre $A \cap B = 1$ und $B \leq \mathrm{C}_G(A) = A$. Also ist A der einzige minimale Normalteiler. Nach Frattini ist $G = AG_\omega$ und $A \cap G_\omega = A_\omega = 1$. Dies zeigt $G = A \rtimes G_\omega$. □

Bemerkung 6.22.

(i) In der Situation von Satz 6.21 ist A ein n-dimensionaler Vektorraum über $\mathbb{F}_p$. Wegen $\mathrm{C}_G(A) = A$ operiert G_ω treu auf A, d. h. $G_\omega \leq \mathrm{GL}(n, p)$. Da A minimal ist, operiert G_ω *irreduzibel* auf $A \cong \mathbb{F}_p^n$, d. h. 1 und A sind die einzigen G_ω-invarianten Untervektorräume von A.

(ii) Wir beschäftigen uns mit der Umkehrung von Satz 6.21. Sei $V \cong \mathbb{F}_p^n$ und $H \leq \mathrm{GL}(n, p)$ irreduzibel auf V. Wir wollen zeigen, dass dann $G := V \rtimes H$ eine primitive Permutationsgruppe ist. Da H treu auf V operiert, ist $\mathrm{C}_G(V) = V$. Wir betrachten die Operation $\varphi : G \to \mathrm{Sym}(G/H)$ durch Linksmultiplikation. Für $x \in \mathrm{Ker}(\varphi)$ gilt dann $H = 1H = xH$ und $x \in H$. Somit ist $\mathrm{Ker}(\varphi) \subseteq H$. Wegen $\mathrm{Ker}(\varphi) \cap V \leq H \cap V = 1$ ist dann $\mathrm{Ker}(\varphi) \leq \mathrm{C}_G(V) \leq V$ und $\mathrm{Ker}(\varphi) = 1$. Also ist G eine Permutationsgruppe auf G/H. Offenbar ist H der Stabilisator der trivialen Nebenklasse $1H$. Um zu zeigen, dass G primitiv ist, können wir nach Satz 6.16 beweisen, dass H maximal in G ist. Sei also $H < M \leq G$. Dann ist $1 \neq M \cap V \trianglelefteq M$. Da V abelsch ist, gilt auch $M \cap V \trianglelefteq V$. Insgesamt ist $M \cap V \trianglelefteq VM = VH = G$. Da H irreduzibel operiert, ist $V \leq M$. Dann ist aber $G = VH \leq M$. Somit ist H maximal und G ist eine primitive Permutationsgruppe.

Beispiel 6.23. Sei $V \cong C_p^n$. Nach linearer Algebra operiert $\mathrm{GL}(n, p)$ irreduzibel auf V. Daher ist die *affine Gruppe* $\mathrm{Aff}(n, p) := V \rtimes \mathrm{GL}(n, p)$ primitiv. Wir versuchen nun kleinere Gruppen zu konstruieren. Dafür fassen wir V als additive Gruppe des Körpers $\mathbb{F}_{p^n}$ auf. Für $\gamma \in \mathbb{F}_{p^n}^\times$ ist die Abbildung $f_\gamma : V \to V$, $v \mapsto \gamma v$ sicher linear und bijektiv. Also gibt es einen Monomorphismus $f : \mathbb{F}_{p^n}^\times \to \mathrm{Aut}(V) \cong \mathrm{GL}(n, p)$, $\gamma \mapsto f_\gamma$ mit Bild S. Bekanntlich ist $S \cong \mathbb{F}_{p^n}^\times \cong C_{p^n-1}$ (Algebra). Sei $s \in S$ ein Erzeuger. Da jede nicht-triviale Potenz von s nur den trivialen Fixpunkt 0 auf V hat, entspricht s einem Zyklus der Länge $p^n - 1$ in $\mathrm{Sym}(V)$. Insbesondere operiert S transitiv auf $V \setminus \{0\}$. Insbesondere ist S irreduzibel und $V \rtimes S$ ist eine primitive Permutationsgruppe. Man nennt S *Singer-Zyklus*. Im Fall $n = 1$ ist sicher $V \rtimes S = \mathrm{Aff}(1, p) \cong C_p \rtimes C_{p-1}$.

Definition 6.24. Eine Operation $G \to \mathrm{Sym}(\Omega)$ heißt *k-transitiv*, falls $|\Omega| \geq k$ und für je zwei k-Tupel $(\alpha_1, \ldots, \alpha_k), (\beta_1, \ldots, \beta_k) \in \Omega^k$ von paarweise verschiedenen Elementen ein $g \in G$ mit ${}^g\alpha_i = \beta_i$ für $i = 1, \ldots, k$ existiert.

Beispiel 6.25.

(i) Die 1-transitiven Operationen sind genau die transitiven Operationen.

(ii) Jede k-transitive Operation ist offenbar auch l-transitiv für $1 \leq l \leq k$.

(iii) S_n ist n-transitiv (auf $\{1, \ldots, n\}$).

(iv) Sei $n \geq 3$ und $k := n-2$. Für k-Tupel $(\alpha_1, \ldots, \alpha_k), (\beta_1, \ldots, \beta_k) \in \{1, \ldots, n\}^k$ mit paarweise verschiedenen Elementen sei $\{x, y\} = \{1, \ldots, n\} \setminus \{\alpha_1, \ldots, \alpha_k\}$ und $\{x', y'\} = \{1, \ldots, n\} \setminus \{\beta_1, \ldots, \beta_k\}$. Dann ist genau eine der beiden Permutationen

$$\begin{pmatrix} \alpha_1 & \cdots & \alpha_k & x & y \\ \beta_1 & \cdots & \beta_k & x' & y' \end{pmatrix} \qquad \text{oder} \qquad \begin{pmatrix} \alpha_1 & \cdots & \alpha_k & x & y \\ \beta_1 & \cdots & \beta_k & y' & x' \end{pmatrix}$$

in A_n. Also ist A_n $(n-2)$-transitiv.

(v) Für eine Primzahlpotenz q und $n \geq 2$ operiert $\mathrm{GL}(n, q)$ 2-transitiv auf der Menge der eindimensionalen Untervektorräume von $\mathbb{F}_q^n$ (lineare Algebra).

Lemma 6.26. *Sei $\varphi : G \to \mathrm{Sym}(\Omega)$ eine transitive Operation, $\omega \in \Omega$ und $k \geq 2$. Genau dann ist φ k-transitiv, wenn G_ω $(k-1)$-transitiv auf $\Omega \setminus \{\omega\}$ operiert.*

Beweis. Sei G k-transitiv und seien $(\alpha_1, \ldots, \alpha_{k-1}), (\beta_1, \ldots, \beta_{k-1}) \in (\Omega \setminus \{\omega\})^{k-1}$ mit paarweise verschiedenen Elementen. Dann existiert ein $g \in G$ mit ${}^g\alpha_i = \beta_i$ für $i = 1, \ldots, k-1$ und ${}^g\omega = \omega$. Also ist $g \in G_\omega$ und G_ω ist $(k-1)$-transitiv auf $\Omega \setminus \{\omega\}$.

Sei nun G_ω $(k-1)$-transitiv auf $\Omega \setminus \{\omega\}$. Seien $(\alpha_1, \ldots, \alpha_k), (\beta_1, \ldots, \beta_k) \in \Omega^k$ mit paarweise verschiedenen Elementen. Da φ transitiv ist, existieren $x, y \in G$ mit ${}^x\alpha_k = \omega = {}^y\beta_k$. Dann sind ${}^x\alpha_i, {}^y\beta_i \in \Omega \setminus \{\omega\}$ für $i = 1, \ldots, k-1$. Es existiert also ein $h \in G_\omega$ mit ${}^{hx}\alpha_i = {}^y\beta_i$ für $i = 1, \ldots, k$. Für $g := y^{-1}hx \in G$ gilt also ${}^g\alpha_i = \beta_i$ für $i = 1, \ldots, k$. Also ist G k-transitiv. □

Lemma 6.27. *Ist $G \to S_n$ k-transitiv, so ist $n(n-1)\ldots(n-k+1) \mid |G|$.*

Beweis. Induktion nach k: Im Fall $k = 1$ ist G transitiv und die Bahnengleichung liefert $n \mid |G|$. Sei nun $k \geq 2$. Dann ist G transitiv und nach Lemma 6.26 ist G_1 $(k-1)$-transitiv auf $\{2, \ldots, n\}$. Nach Induktion ist also $(n-1)\ldots(n-k+1) \mid |G_1|$. Wegen $|G : G_1| = n$ folgt die Behauptung. □

Satz 6.28. *Jede 2-transitive Operation ist primitiv.*

Beweis. Sei $\varphi : G \to \mathrm{Sym}(\Omega)$ eine 2-transitive Operation. Nehmen wir an, dass es einen Block $\Delta \subseteq \Omega$ gibt. Seien $\alpha, \beta \in \Delta$ mit $\alpha \neq \beta$ und $\gamma \in \Omega \setminus \Delta$. Nach Voraussetzung existiert ein $g \in G$ mit ${}^g\alpha = \alpha$ und ${}^g\beta = \gamma$. Insbesondere ist $\varnothing \neq \Delta \cap {}^g\Delta \neq \Delta$. Widerspruch. □

Satz 6.29. *Sei $1 \neq N \trianglelefteq G$ und $\varphi : G \to \mathrm{Sym}(N \setminus \{1\})$ die Operation durch Konjugation. Dann gilt:*

(i) Ist φ transitiv, so ist N eine elementarabelsche p-Gruppe.

(ii) Ist φ sogar 2-transitiv, so ist $p = 2$ oder $|N| = 3$.

(iii) Ist φ sogar 3-transitiv, so ist $|N| = 4$.

(iv) φ ist nie 4-transitiv.

Beweis. Sei p ein Primteiler von $|N|$ und $x \in N$ ein Element der Ordnung p (Cauchy). Ist φ transitiv, so ist jedes nicht-triviale Element von N zu x konjugiert. Insbesondere ist $y^p = 1$ für alle $y \in N$. Also ist N eine p-Gruppe und damit auflösbar. Außerdem ist N ein minimaler Normalteiler. Aus Satz 2.26 folgt (i).

Sei nun φ 2-transitiv und $p \neq 2$. Dann ist $x^{-1} \neq x$. Sei $y \in N \setminus \{1, x\}$. Dann existiert ein $g \in G$ mit $gxg^{-1} = x$ und $gx^{-1}g^{-1} = y$. Dies zeigt $y = x^{-1}$ und $N = \{1, x, x^{-1}\}$. Also gilt (ii). Ist φ 3-transitiv, so muss also $p = 2$ gelten, da $|N \setminus \{1\}| \geq 3$. Sei $U := \{1, a, b, c\} \leq N$. Dann ist $c = ab$. Für ein $g \in G$ mit ${}^g a = a$ und ${}^g b = b$ muss also auch ${}^g c = c$ gelten. Dies zeigt $U = N$ und (iii) folgt. Wäre die Operation 4-transitiv, so wäre $|N \setminus \{1\}| \geq 4$ im Widerspruch zu (iii). □

Satz 6.30. *Für $n \geq 5$ ist A_n einfach.*

Beweis. Sei $1 \neq N \trianglelefteq G := A_n$. Nach Beispiel 6.15 operiert A_n treu und primitiv auf $\Omega := \{1, \ldots, n\}$. Daher operiert N transitiv auf Ω nach Satz 6.20. Wir argumentieren nun durch Induktion nach n. Sei $n = 5$. Dann ist $5 \mid |N|$. Da $|G/N|$ nicht mehr durch 5 teilbar ist, muss N alle Elemente der Ordnung 5 enthalten, d. h. alle 5-Zyklen. Jeder 5-Zyklus lässt sich eindeutig in der Form $(1, a, b, c, d)$ mit $\{a, b, c, d\} = \{2, 3, 4, 5\}$ schreiben. Also gibt es genau $4! = 24$ solche Elemente und wir erhalten $|N| \geq 24$. Wegen $|N| \mid |G|$ bleiben nur die Möglichkeiten $|N| \in \{30, 60\}$. Also ist $|G/N|$ auch nicht mehr durch 3 teilbar und N muss auch alle 3-Zyklen enthalten. Von diesen gibt es $\binom{5}{3} \cdot 2! = 20$ Stück. Also ist $|N| \geq 24 + 20 = 44$ und somit $N = G$.

Sei nun $n \geq 6$ und die Behauptung für $n - 1$ bereits gezeigt. Der Stabilisator $G_n = A_{n-1}$ ist nach Induktion einfach. Nach Frattini ist $G = NG_n$. Wir können also $G_n \not\leq N$ annehmen. Insbesondere ist $N \cap G_n \lhd G_n$ und damit $N_n = N \cap G_n = 1$. Also operiert N regulär auf Ω und $|N| = n$. Nach Beispiel 6.25 operiert G_n $(n-3)$-transitiv auf $\Omega \setminus \{n\}$. Nach Satz 6.19 ist diese Operation isomorph zur Operation auf $N \setminus \{1\}$ durch Konjugation. Satz 6.29 liefert nun $n = 6$ und $|N| = 4$. Dies widerspricht aber $|N| = n$. □

Satz 6.31. *Für $n \geq 5$ sind 1, A_n und S_n die einzigen Normalteiler von S_n. Insbesondere ist $S_n' = A_n$.*

Beweis. Sei $1 \neq N \lhd S_n$. Dann ist $N \cap A_n \trianglelefteq A_n$. Aus Satz 6.30 folgt $N \cap A_n \in \{1, A_n\}$. Im zweiten Fall ist $N = A_n$. Im ersten Fall ist $|G| = |A_n N| = |A_n||N|$ und $|N| = 2$. Dies widerspricht aber Satz 6.20. □

Satz 6.32. *Ist G eine einfache Gruppe der Ordnung 60, so ist $G \cong A_5$.*

Beweis. Wir konstruieren zunächst eine Untergruppe $H \leq G$ vom Index 5. Sei $P \in \mathrm{Syl}_2(G)$. Offenbar ist $\mathrm{N}_G(P) < G$. Im Fall $|G : \mathrm{N}_G(P)| = 3$ gäbe es einen nicht-trivialen Homomorphismus $G \to S_3$ im Widerspruch zur Einfachheit von G. Wir können also $\mathrm{N}_G(P) = P$ annehmen (anderenfalls setze man $H := \mathrm{N}_G(P)$). Schneiden sich je zwei verschiedene 2-Sylowgruppen trivial, so besitzt die Vereinigung aller 2-Sylowgruppen 46 Elemente. Andererseits muss es nach Sylow aber mindestens sechs 5-Sylowgruppen geben, die sich ebenfalls trivial schneiden. Dieser Widerspruch zeigt, dass es ein $Q \in \mathrm{Syl}_2(G)$ mit $|P \cap Q| = 2$ gibt. Dann ist $P, Q \leq \mathrm{N}_G(P \cap Q)$. Wie oben ist $|G : \mathrm{N}_G(P \cap Q)| = 3$ ausgeschlossen. Man kann also $H := \mathrm{N}_G(P \cap Q)$ wählen.

Die Operation auf den Nebenklassen G/H liefert nun einen Monomorphismus $G \to S_5$. Da A_5 die einzige Untergruppe der Ordnung 60 in S_5 ist (Satz 6.31), folgt $G \cong A_5$. □

Bemerkung 6.33. Mit Hilfe der Klassifikation der endlichen einfachen Gruppen kann man zeigen, dass jede 4-transitive Permutationsgruppe zu einer der folgenden Familien gehört:

(i) S_n mit $n \geq 4$.

(ii) A_n mit $n \geq 6$.

(iii) M_{11}, M_{12}, M_{23}, M_{24} (sporadisch einfache *Mathieugruppen*).

7 Verlagerung

Definition 7.1. Für eine Primzahl p heißt G *p-nilpotent*, falls ein p'-Normalteiler $N \trianglelefteq G$ mit p-Faktorgruppe G/N existiert.

Bemerkung 7.2.

(i) In der Situation von Definition 7.1 ist offenbar $N = \mathrm{O}_{p'}(G) = \mathrm{O}^p(G)$. Umgekehrt ist jede Gruppe G mit $\mathrm{O}_{p'}(G) = \mathrm{O}^p(G)$ sicher p-nilpotent. Ist $P \in \mathrm{Syl}_p(G)$, so gilt in diesem Fall $G = \mathrm{O}_{p'}(G)P$ und $P \cap \mathrm{O}_{p'}(G) = 1$. Also ist $G = \mathrm{O}_{p'}(G) \rtimes P$.

(ii) Ist G p-nilpotent für ein $p \mid |G| \neq p$, so ist G nicht einfach. Außerdem ist dann $\mathrm{O}_{p'}(G)$ die Menge der p'-Elemente von G.

Beispiel 7.3. Wegen $A_3 \trianglelefteq S_3$ ist S_3 2-nilpotent, aber nicht 3-nilpotent.

Satz 7.4. *Genau dann ist G nilpotent, wenn G für jede Primzahl p p-nilpotent ist.*

Beweis. Ist G nilpotent und p eine Primzahl, so ist $\mathrm{O}_{p'}(G) = \bigoplus_{q \neq p} \mathrm{O}_q(G)$. Also ist $G/\mathrm{O}_{p'}(G)$ eine p-Gruppe und G ist p-nilpotent. Sei nun umgekehrt G p-nilpotent für jede Primzahl p. Dann ist $D := \times_{p||G|} G/\mathrm{O}_{p'}(G)$ nilpotent. Andererseits hat der Homomorphismus $G \to D$, $g \mapsto (g\,\mathrm{O}_{p'}(G))_{p||G|}$ Kern $\bigcap_{p||G|} \mathrm{O}_{p'}(G) = 1$. Wegen $|G| = |D|$ ist G zur nilpotenten Gruppe D isomorph. □

Lemma 7.5. *Untergruppen und Faktorgruppen p-nilpotenter Gruppen sind wieder p-nilpotent.*

Beweis. Sei G p-nilpotent und $H \leq G$. Dann ist $\mathrm{O}_{p'}(G) \cap H \leq \mathrm{O}_{p'}(H)$ und $H/H \cap \mathrm{O}_{p'}(G) \cong H\,\mathrm{O}_{p'}(G)/\mathrm{O}_{p'}(G) \leq G/\mathrm{O}_{p'}(G)$ ist bereits eine p-Gruppe. Also ist H p-nilpotent. Sei nun $N \trianglelefteq G$. Dann ist $\mathrm{O}_{p'}(G)N/N \leq \mathrm{O}_{p'}(G/N)$ und $(G/N)/(\mathrm{O}_{p'}(G)N/N) \cong G/\mathrm{O}_{p'}(G)N \cong (G/\mathrm{O}_{p'}(G))/(\mathrm{O}_{p'}(G)N/\mathrm{O}_{p'}(G))$ ist eine p-Gruppe. Also ist auch G/N p-nilpotent. □

Definition 7.6. Sei $K \trianglelefteq H \leq G$ mit abelscher Faktorgruppe H/K und sei R ein Repräsentantensystem für G/H. Für $g \in G$ sei $\overline{g} \in R$ mit $gH = \overline{g}H$. Die Abbildung

$$\begin{aligned} V_{H/K} : G &\to H/K, \\ g &\mapsto \prod_{r \in R} (gr)^{-1}\overline{gr}K \end{aligned}$$

heißt *Verlagerung* (engl. transfer) von G nach H/K. Da H/K abelsch ist, kommt es in dem Produkt nicht auf die Reihenfolge der Faktoren an.

Lemma 7.7. *Die Verlagerung hängt nicht von der Wahl von R ab und ist ein Homomorphismus.*

Beweis. Wir verwenden eine ähnliche Konstruktion wie im Beweis von Satz 5.12. Für Repräsentantensysteme R und S von G/H sei

$$(R,S) := \prod_{\substack{(x,y)\in R\times S,\\ xH=yH}} x^{-1}yK \in H/K.$$

Dann gilt $V_{H/K}(g) = (gR, R)$ für $g \in G$. Wir müssen $(gR, R) = (gS, S)$ zeigen. Wegen $(gR, gS) = (R, S)$ und $(R, S)(S, T) = (R, T)$ ist

$$\begin{aligned}(gR, R)(gS, S)^{-1} &= (gR, R)(R, gS)(R, gS)^{-1}(gS, S)^{-1}\\ &= (gR, gS)((R, gS)(gS, S))^{-1} = (gR, gS)(R, S)^{-1} = 1.\end{aligned}$$

Also hängt $V_{H/K}$ nicht von der Wahl von R ab. Für $g, h \in G$ ist

$$V_{H/K}(gh) = (ghR, R) = (g(hR), (hR))(hR, R) = (gR, R)(hR, R) = V_{H/K}(g)V_{H/K}(h). \qquad \square$$

Bemerkung 7.8. Wir wollen ein Repräsentantensystem R finden, sodass $V_{H/K}$ leicht zu berechnen ist. Sei $g \in G$ und seien $x_1H, \ldots, x_nH$ Repräsentanten für die Bahnen von $\langle g\rangle$ auf G/H durch Linksmultiplikation. Dann ist $R := \{g^j x_i : i = 1, \ldots, n,\ j = 0, \ldots, t_i - 1\}$ ein Repräsentantensystem für G/H, wobei t_i die Bahnenlänge von x_iH unter $\langle g\rangle$ ist. Im Fall $0 \le j < t_i - 1$ ist $(g(g^j x_i))^{-1}\overline{g(g^j x_i)} = 1$ (bzgl. R). Also ist

$$V_{H/K}(g) = \prod_{i=1}^{n} x_i^{-1} g^{-t_i} x_i K$$

mit $t_1 + \ldots + t_n = |G : H|$ und $x_i^{-1}g^{-t_i}x_i \in H$ für $i = 1, \ldots, n$.

Beispiel 7.9. Für $g \in \mathrm{Z}(G)$ ist also $V_{H/K}(g) = g^{-|G:H|}K$. Außerdem erhält man für $H = \mathrm{Z}(G)$ und $K = 1$ einen Homomorphismus $G \to \mathrm{Z}(G)$, $g \mapsto g^{|G:\mathrm{Z}(G)|}$.

Definition 7.10. Für $H \le G$ sei $\mathrm{Foc}_G(H) := \langle [g, h] : g \in G, h, [g, h] \in H\rangle$ die *Fokalgruppe* von H in G.

Bemerkung 7.11. Offenbar ist $H' \le F := \mathrm{Foc}_G(H) \le H \cap G'$ und $F \trianglelefteq H$ mit abelscher Faktorgruppe H/F. Für $g \in G$ und $h \in H$ mit $[g, h] \in H$ ist $ghg^{-1}F = ghg^{-1}h^{-1}Fh = [g, h]Fh = Fh = hF$. Dies zeigt $V_{H/F}(h) = h^{-|G:H|}F$ für alle $h \in H$ nach Bemerkung 7.8.

Satz 7.12. *Sei $H \le G$ und $F := \mathrm{Foc}_G(H)$ mit $\mathrm{ggT}(|G : H|, |H : F|) = 1$. Dann gilt*

(i) $H \cap \mathrm{Ker}(V_{H/F}) = H \cap G' = F$.

(ii) $H\,\mathrm{Ker}(V_{H/F}) = G$.

(iii) $G/G' = HG'/G' \oplus \mathrm{Ker}(V_{H/F})/G'$.

(iv) $G/\mathrm{Ker}(V_{H/F}) \cong H/F$.

Beweis.

(i) Da $G/\mathrm{Ker}(V_{H/F})$ zu einer Untergruppe von H/F isomorph ist, gilt $G' \le \mathrm{Ker}(V_{H/F}) =: N$ und $F \le H \cap G' \le H \cap N$. Für $h \in H \cap N$ ist andererseits $1 = V_{H/F}(h) = h^{-|G:H|}F$ und $h^{|G:H|} \in F$. Andererseits ist auch $h^{|H:F|} \in F$. Wegen $\mathrm{ggT}(|G : H|, |H : F|) = 1$ existieren $a, b \in \mathbb{Z}$ mit $a|G : H| + b|H : F| = 1$. Es folgt $h = h^{a|G:H|+b|H:F|} \in F$. Somit gilt auch $H \cap N \le F$.

(ii) Nach (i) ist $|G/N| \geq |HN/N| = |H/H \cap N| = |H/F| \geq |G/N|$ und daher $G = HN$.

(iii) Nach (ii) ist $G/G' = HN/G' = (HG'/G')(N/G')$ und nach (i) ist $HG' \cap N = G'(H \cap N) = G'F = G'$.

(iv) Der Beweis von (ii) zeigt, dass $V_{H/F}$ surjektiv ist. □

Bemerkung 7.13. Die Voraussetzung $\mathrm{ggT}(|G : H|, |H : F|) = 1$ in Satz 7.12 ist zum Beispiel für Hallgruppen H erfüllt.

Folgerung 7.14 (Satz von der Fokalgruppe)**.** *Für $P \in \mathrm{Syl}_p(G)$ gilt $\mathrm{Foc}_G(P) = G' \cap P$.*

Beweis. Wähle $H = P$ in Satz 7.12. □

Definition 7.15. Für $H \leq G$ definieren wir $H_1 := H$ und $H_{i+1} := \mathrm{Foc}_G(H_i)$ für $i \geq 1$. Man nennt H *hyperfokal*, falls $H_n = 1$ für ein $n \geq 1$ gilt.

Bemerkung 7.16. Ist $H \leq G$ hyperfokal, so ist auch jede Untergruppe $K \leq H$ hyperfokal in G, denn $\mathrm{Foc}_G(K) \leq \mathrm{Foc}_G(H)$. Ist $H \leq U \leq G$, so ist H auch hyperfokal in U, denn $\mathrm{Foc}_U(H) \leq \mathrm{Foc}_G(H)$. Wegen $H^n \leq H_n$ ist H nilpotent.

Satz 7.17. *Jede hyperfokale Hallgruppe $H \leq G$ besitzt ein normales Komplement in G (d. h. es existiert $N \trianglelefteq G$ mit $G = NH$ und $H \cap N = 1$).*

Beweis. Induktion nach $|G|$: O. B. d. A. sei $H \neq 1$. Dann ist $\mathrm{Foc}_G(H) = H_2 < H$. Nach Satz 7.12 ist $N := \mathrm{Ker}(V_{H/H_2}) \trianglelefteq G$ mit $G/N \cong H/H_2 \neq 1$. Die nilpotente Hallgruppe $H \cap N$ von N ist nach obiger Bemerkung hyperfokal (in N). Nach Induktion besitzt $H \cap N$ ein normales Komplement $K \trianglelefteq N$. Dann ist K als Hallnormalteiler charakteristisch in N (es gilt $K = \mathrm{O}_\pi(N)$ für eine gewisse Primzahlmenge π). Dies zeigt $K \trianglelefteq G$. Außerdem gilt $HK = H(H \cap N)K = HN = G$ nach Satz 7.12 und $K \cap H \leq K \cap (N \cap H) = 1$. □

Satz 7.18. *Sei H eine nilpotente Hallgruppe von G, sodass je zwei in G konjugierte Elemente $x, y \in H$ bereits in H konjugiert sind. Dann besitzt H ein normales Komplement in G.*

Beweis. Nach Satz 7.17 genügt es $H_n \leq H^n$ für $n \geq 1$ zu zeigen. Dies ist trivial für $n = 1$. Sei induktiv $H_{n-1} \leq H^{n-1}$. Sei $g \in G$ und $h \in H_{n-1}$ mit $[g, h] \in H_{n-1} \leq H^{n-1} \leq H$. Dann ist auch $ghg^{-1} \in H$. Nach Voraussetzung existiert ein $x \in H$ mit $xhx^{-1} = ghg^{-1}$. Es folgt $[g, h] = xhx^{-1}h^{-1} = [x, h] \in [H, H^{n-1}] = H^n$. Damit ist $H_n = \mathrm{Foc}_G(H_{n-1}) \leq H^n$. □

Folgerung 7.19. *Sei $P \in \mathrm{Syl}_p(G)$, sodass je zwei in G konjugierte Elemente $x, y \in P$ bereits in P konjugiert sind. Dann ist G p-nilpotent.*

Beweis. Setze $H = P$ in Satz 7.18. □

Lemma 7.20. *Sei $P \in \mathrm{Syl}_p(G)$ abelsch. Sind $x, y \in P$ in G konjugiert, so auch in $\mathrm{N}_G(P)$.*

Beweis. Sei $g \in G$ mit $gxg^{-1} = y$. Nach Voraussetzung ist $P \leq \mathrm{C}_G(P) \leq \mathrm{C}_G(x) \cap \mathrm{C}_G(y) = \mathrm{C}_G(x) \cap g\,\mathrm{C}_G(x)g^{-1}$. Also ist $P, g^{-1}Pg \in \mathrm{Syl}_p(\mathrm{C}_G(x))$ und nach Sylow existiert ein $c \in \mathrm{C}_G(x)$ mit $cPc^{-1} = g^{-1}Pg$. Dies impliziert $gc \in \mathrm{N}_G(P)$ und $gcx(gc)^{-1} = gxg^{-1} = y$. □

Satz 7.21 (BURNSIDEs Verlagerungssatz)**.** *Sei $P \in \mathrm{Syl}_p(G)$ mit $\mathrm{N}_G(P) = \mathrm{C}_G(P)$. Dann ist G p-nilpotent.*

Beweis. Wegen $P \leq \mathrm{N}_G(P) = \mathrm{C}_G(P)$ ist P abelsch. Die Behauptung folgt nun aus Lemma 7.20 und Folgerung 7.19. □

Satz 7.22. *Sei p der kleinste Primteiler von $|G|$. Besitzt G eine zyklische p-Sylowgruppe, so ist G p-nilpotent.*

Beweis. Sei $P \in \mathrm{Syl}_p(G)$ zyklisch der Ordnung p^n. Dann ist $|\mathrm{Aut}(P)| = \varphi(p^n) = p^{n-1}(p-1)$ nach Satz 2.4. Bekanntlich ist $\mathrm{N}_G(P)/\mathrm{C}_G(P)$ zu einer Untergruppe von $\mathrm{Aut}(P)$ isomorph. Wegen $P \leq \mathrm{C}_G(P)$ ist daher $|\mathrm{N}_G(P)/\mathrm{C}_G(P)| \mid p-1$. Nach Lagrange ist andererseits $|\mathrm{N}_G(P)/\mathrm{C}_G(P)| \mid |G|$. Da p der kleinste Primteiler von $|G|$ ist, erhalten wir $\mathrm{N}_G(P) = \mathrm{C}_G(P)$. Die Behauptung folgt nun aus Satz 7.21. □

Bemerkung 7.23. Ist $|G|$ nur einmal durch 2 teilbar, so ist G nach Satz 7.22 2-nilpotent. Nach Feit-Thompson ist G sogar auflösbar.

Satz 7.24. *Sind alle Sylowgruppen von G zyklisch, so sind auch G' und G/G' zyklisch. Insbesondere ist G metabelsch.*

Beweis. Wir zeigen zunächst durch Induktion nach $|G|$, dass G auflösbar ist. Sei p der kleinste Primteiler von $|G|$. Nach Satz 7.22 ist $G/\mathrm{O}_{p'}(G)$ eine p-Gruppe und damit auflösbar. Offenbar sind auch die Sylowgruppen von $\mathrm{O}_{p'}(G)$ zyklisch. Nach Induktion ist also auch $\mathrm{O}_{p'}(G)$ auflösbar. Die Behauptung folgt nun aus Lemma 2.21.

Nun ist G/G' abelsch und alle Sylowgruppen von G/G' sind zyklisch. Also ist auch G/G' zyklisch. Mit dem gleichen Argument genügt es zu zeigen, dass G' abelsch ist. Nehmen wir indirekt $G'' \neq 1$ an. Ersetzt man G durch G/G''', so kann man annehmen, dass G'' abelsch ist. Sicher ist dann G'' zyklisch. Also ist $G/\mathrm{C}_G(G'') \leq \mathrm{Aut}(G'') \cong (\mathbb{Z}/|G''|\mathbb{Z})^\times$ abelsch (Satz 2.4). Dies zeigt $G' \leq \mathrm{C}_G(G'')$ und $G'' \leq \mathrm{Z}(G')$. Da auch G'/G'' zyklisch ist, muss schließlich G' abelsch sein (Aufgabe 4(a)). Dies widerspricht aber $G'' \neq 1$. □

Beispiel 7.25. Gruppen quadratfreier Ordnung sind metabelsch.

Satz 7.26. *Für jede abelsche Hallgruppe $H \leq G$ und $N := \mathrm{N}_G(H)$ gilt:*

(i) $H = (H \cap \mathrm{Z}(N)) \oplus [H, N]$.

(ii) $[H, N] = \mathrm{Foc}_G(H) = H \cap \mathrm{Ker}(V_{H/1})$.

(iii) $H \cap \mathrm{Z}(N) = V_{H/1}(H)$.

Beweis. Wir fassen $V_{H/1}$ als Abbildung nach H auf und schreiben $V_H := V_{H/1}$. Sei $g \in H$ und $V_H(g) = \prod_{i=1}^n x_i^{-1} g^{-t_i} x_i \in H$ wie in Bemerkung 7.8. Für $i = 1, \ldots, n$ ist dann $g^{t_i}, x_i^{-1} g^{t_i} x_i \in H$ und $\langle H, x_i H x_i^{-1} \rangle \leq \mathrm{C}_G(g^{t_i})$, da H abelsch ist. Nach Wielandt sind die nilpotenten Hallgruppen H und $x_i H x_i^{-1}$ in $\mathrm{C}_G(g^{t_i})$ konjugiert. Sei also $c_i \in \mathrm{C}_G(g^{t_i})$ mit $c_i x_i H x_i^{-1} c_i^{-1} = H$ für $i = 1, \ldots, n$. Dann ist $c_i x_i \in N$ und

$$x_i^{-1} g^{-t_i} x_i = x_i^{-1} c_i^{-1} g^{-t_i} c_i x_i = g^{-t_i} [g^{t_i}, (c_i x_i)^{-1}]. \tag{7.1}$$

Es folgt $V_H(g) \in g^{-|G:H|}[H, N]$ und $g^{|G:H|} \in V_H(H)[H, N]$. Wegen $\mathrm{ggT}(|H|, |G : H|) = 1$ ist sogar $H = V_H(H)[H, N]$.

Offenbar ist $[H,N] = \langle [h,x] : h \in H, x \in N\rangle \leq \mathrm{Foc}_G(H) \leq H \cap G' \leq H \cap \mathrm{Ker}(V_H)$ (beachte: $G/\mathrm{Ker}(V_H) \cong V_H(G) \leq H$ ist abelsch). Daher ist auch $H = V_H(H)(H \cap \mathrm{Ker}(V_H))$. Wegen $[H,N] \leq \mathrm{Ker}(V_H)$ folgt $V_H(V_H(g)) = V_H(g)^{-|G:H|}$ aus (7.1) für $g \in H$. Dies liefert $V_H(H) \cap \mathrm{Ker}(V_H) = 1$ und es folgt

$$H = V_H(H) \oplus (H \cap \mathrm{Ker}(V_H)) = V_H(H) \oplus [H,N].$$

Aus Ordnungsgründen ist dann auch $[H,N] = \mathrm{Foc}_G(H) = H \cap \mathrm{Ker}(V_H)$. Dies zeigt (ii) und einen Teil von (i).

Sei R ein beliebiges Repräsentantensystem für G/H und sei $x \in N$. Wie in Definition 7.6 wählen wir $\overline{g} \in R$ mit $gH = \overline{g}H$ für $g \in G$. Es ist auch Rx ein Repräsentantensystem für G/H, denn aus $rxH = sxH$ folgt $rHx = sHx$ und $rH = sH$ für $r,s \in R$. Für $g \in G$ sei $\widetilde{g} \in Rx$ mit $gH = \widetilde{g}H$. Es gilt dann $\overline{gr}xH = \overline{gr}Hx = grHx = grxH = \widetilde{grx}H$ und $\overline{gr}x = \widetilde{grx}$ für $r \in R$. Dies zeigt

$$x^{-1}V_H(g)x = \prod_{r\in R} x^{-1}(gr)^{-1}\overline{gr}x = \prod_{r\in R}(grx)^{-1}\widetilde{grx} = \prod_{s\in Rx}(gs)^{-1}\widetilde{gs} = V_H(g).$$

Also ist $V_H(H) \leq H \cap \mathrm{Z}(N)$. Für $g \in H \cap \mathrm{Z}(N)$ gilt umgekehrt $V_H(g) = g^{-|G:H|}$ nach (7.1). Dies impliziert $V_H(H) = H \cap \mathrm{Z}(N)$ und wir sind fertig. □

Bemerkung 7.27. In der Situation von Satz 7.26 gilt $G/\mathrm{Ker}(V_{H/F}) \cong H/F \cong H \cap \mathrm{Z}(N)$ mit $F := \mathrm{Foc}_G(H)$ nach Satz 7.12. Auf diese Weise kann man häufig Normalteiler konstruieren.

Satz 7.28. *Jede auflösbare Untergruppe $H \leq G$ mit $H \cap gHg^{-1} = 1$ für alle $g \in G \setminus H$ besitzt ein normales Komplement in G (vgl. Aufgabe 21).*

Beweis. Induktion nach $|H|$: Wir können $H \neq 1$ annehmen. Dann ist $H' < H$. Sei $h \in H$ und $V_{H/H'}(h) = \prod_{i=1}^n x_i^{-1}h^{-t_i}x_iH'$ wie in Bemerkung 7.8. Dabei können wir $x_1 = 1$ annehmen. Wegen $hx_1H = H = x_1H$ ist dann $t_1 = 1$ und $x_1^{-1}h^{-t_1}x_1 = h^{-1}$. Für $i > 1$ ist $x_i \notin H$ und $x_i^{-1}h^{-t_i}x_i \in H \cap x_i^{-1}Hx_i = 1$. Dies zeigt $V_{H/H'}(h) = h^{-1}H'$ für alle $h \in H$. Insbesondere ist $V_{H/H'}(H) = H/H'$ und $\mathrm{Ker}(V_{H/H'}) \cap H = H'$. Sei $N := \mathrm{Ker}(V_{H/H'})$. Für $g \in G$ existiert ein $h \in H$ mit $V_{H/H'}(g) = V_{H/H'}(h)$ und $g = hh^{-1}g \in HN$. Also ist $G = HN$. Für $g \in N \setminus H' = N \setminus H$ ist $gH'g^{-1} \cap H' \subseteq gHg^{-1} \cap H = 1$. Nach Induktion besitzt H' ein normales Komplement K in N. Nach Aufgabe 21 sind H' und K Hallgruppen von N. Insbesondere ist K charakteristisch in N und damit normal in G. Es gilt $H \cap K = H \cap N \cap K = H' \cap K = 1$ und $G = HN = HH'K = HK$. Die Behauptung folgt. □

Bemerkung 7.29. Frobenius hat gezeigt, dass die Auflösbarkeitsbedingung in Satz 7.28 überflüssig ist. Man kennt dafür jedoch keinen Beweis, der ohne Charaktertheorie auskommt.

Satz 7.30 (Frobenius' Verlagerungssatz)**.** *Sei $P \in \mathrm{Syl}_p(G)$, sodass $\mathrm{N}_G(Q)/\mathrm{C}_G(Q)$ für alle $Q \leq P$ eine p-Gruppe ist. Dann ist G p-nilpotent.*

Beweis. Nach Sylow gilt die Voraussetzung für alle $P \in \mathrm{Syl}_p(G)$. Sei Γ die Menge der Paare (P,Q) mit $P,Q \in \mathrm{Syl}_p(G)$, sodass ein $c \in \mathrm{C}_G(P \cap Q)$ mit $P = cQc^{-1}$ existiert. Wir wollen zeigen, dass Γ alle Paare von Sylowgruppen enthält. Sei $P, P_1 \in \mathrm{Syl}_p(G)$ mit $(P,P_1) \notin \Gamma$, sodass $|P \cap P_1|$ maximal ist. Offenbar ist dann $D := P \cap P_1 < P$ (anderenfalls könnte man $c = 1$ wählen). Sei $N := \mathrm{N}_G(D)$ und $P \cap N \subseteq S \in \mathrm{Syl}_p(N)$ sowie $P_1 \cap N \subseteq T \in \mathrm{Syl}_p(N)$. Schließlich sei $S \subseteq R \in \mathrm{Syl}_p(G)$. Da $S\,\mathrm{C}_G(D)/\mathrm{C}_G(D)$ eine p-Sylowgruppe von $N/\mathrm{C}_G(D)$ ist, impliziert die Voraussetzung $N = S\,\mathrm{C}_G(D)$.

Nach Sylow existiert ein $n \in N$ mit $T = nSn^{-1}$. Wegen $N = S\,\mathrm{C}_G(D) = \mathrm{C}_G(D)S$ können wir $n \in \mathrm{C}_G(D)$ annehmen. Nach Satz 4.8 ist

$$D < \mathrm{N}_P(D) = N \cap P \subseteq S \cap P \subseteq R \cap P.$$

Nach Wahl von (P, P_1) existiert ein $x \in \mathrm{C}_G(P \cap R) \subseteq \mathrm{C}_G(D)$ mit $P = xRx^{-1}$. Analog ist auch

$$D < \mathrm{N}_{P_1}(D) = N \cap P_1 \subseteq T \cap P_1 = nSn^{-1} \cap P_1 \subseteq nRn^{-1} \cap P_1$$

und es existiert ein $y \in \mathrm{C}_G(nRn^{-1} \cap P_1) \subseteq \mathrm{C}_G(D)$ mit $nRn^{-1} = yP_1y^{-1}$. Insgesamt ist also $P = xRx^{-1} = xn^{-1}yP_1y^{-1}nx^{-1}$ mit $xn^{-1}y \in \mathrm{C}_G(D) = \mathrm{C}_G(P \cap P_1)$. Dieser Widerspruch zeigt, dass Γ alle Paare (P, Q) mit $P, Q \in \mathrm{Syl}_p(G)$ enthält.

Seien nun $x, y \in P$ und $g \in G$ mit $y = gxg^{-1}$. Dann ist $y \in P \cap gPg^{-1}$. Nach dem eben Gezeigten existiert ein $c \in \mathrm{C}_G(P \cap gPg^{-1}) \subseteq \mathrm{C}_G(y)$ mit $cPc^{-1} = gPg^{-1}$. Da $P\,\mathrm{C}_G(P)/\,\mathrm{C}_G(P)$ eine p-Sylowgruppe von $\mathrm{N}_G(P)/\,\mathrm{C}_G(P)$ ist, folgt $\mathrm{N}_G(P) = P\,\mathrm{C}_G(P)$ nach Voraussetzung. Also ist $c^{-1}g = ab$ mit $a \in P$ und $b \in \mathrm{C}_G(P) \subseteq \mathrm{C}_G(x)$. Dann ist $y = c^{-1}yc = c^{-1}gxg^{-1}c = abxb^{-1}a^{-1} = axa^{-1}$. Die Behauptung folgt nun aus Folgerung 7.19. □

Satz 7.31. *Sei G eine nichtabelsche einfache Gruppe und $P \in \mathrm{Syl}_p(G)$ mit $|P| = p^n > 1$. Dann gilt eine der beiden folgenden Aussagen:*

(i) $\mathrm{ggT}\big(|\mathrm{N}_G(P) : P|, (p^n - 1)(p^{n-1} - 1) \dots (p - 1)\big) \neq 1$.

(ii) $n \geq 3$ *und* $\mathrm{ggT}\big(|G : \mathrm{N}_G(P)|, (p^{n-1} - 1)(p^{n-2} - 1) \dots (p^2 - 1)\big) \neq 1$.

Beweis. Nehmen wir zuerst an, dass P abelsch ist. Nach Satz 7.21 ist dann $P \leq \mathrm{C}_G(P) < \mathrm{N}_G(P)$. Sei $g \in \mathrm{N}_G(P) \setminus \mathrm{C}_G(P)$ mit Ordnung q^s für eine Primzahl $q \neq p$. Nach Bemerkung 4.19 operiert $\langle g \rangle$ nicht-trivial auf $P/\Phi(P)$. Da $P/\Phi(P)$ elementarabelsch ist, ist $\mathrm{Aut}(P/\Phi(P)) \leq \mathrm{GL}(n, p)$ und $q \,\big|\, |\mathrm{GL}(n, p)| = (p^n - 1)(p^n - p) \dots (p^n - p^{n-1})$. Wegen $q \neq p$ ist dann auch

$$q \mid \mathrm{ggT}\big(|\mathrm{N}_G(P) : P|, (p^n - 1)(p^{n-1} - 1) \dots (p - 1)\big) \neq 1.$$

Sei nun P nichtabelsch. Insbesondere ist dann $n \geq 3$ und $\Phi(P) \neq 1$. Nach Satz 7.30 existiert eine Untergruppe $Q \leq P$, sodass $\mathrm{N}_G(Q)/\,\mathrm{C}_G(Q)$ keine p-Gruppe ist. Wir wählen wieder einen Primteiler $q \neq p$ von $|\mathrm{N}_G(Q)/\,\mathrm{C}_G(Q)|$. Wegen $|Q : \Phi(Q)| \leq p^{n-1}$ erhält man dann wie eben $q \mid (p^{n-1} - 1)(p^{n-2} - 1) \dots (p^2 - 1)(p - 1)$. Wegen $p^2 - 1 = (p + 1)(p - 1)$ kann man dabei den Faktor $p - 1$ weglassen. Außerdem ist $q \,\big|\, |G : P|$, da $q \neq p$. Im Fall $q \,\big|\, |\mathrm{N}_G(P) : P|$ gilt Aussage (i). Also können wir $q \,\big|\, |G : \mathrm{N}_G(P)|$ annehmen. Somit gilt (ii). □

Beispiel 7.32. Sei G eine einfache Gruppe der Ordnung $pqrs$ mit Primzahlen $p \leq q \leq r \leq s$. Nach Satz 7.22 ist $p = q$ und nach Satz 4.21 ist $q < r$. Außerdem ist $1 \neq \mathrm{ggT}(rs, (p^2 - 1)(p - 1)) = \mathrm{ggT}(rs, p + 1)$ nach Satz 7.31. Dies zeigt $p = q = 2$ und $r = 3$. Nehmen wir $s = 3$ an. Nach Sylow gilt dann $\mathrm{N}_G(S) = S$ für $S \in \mathrm{Syl}_3(G)$. Dies widerspricht aber Satz 7.21. Also ist $s \geq 5$. Sei $S \in \mathrm{Syl}_s(G)$. Dann ist $|G : \mathrm{N}_G(S)| \,\big|\, 12$ und $|G : \mathrm{N}_G(S)| \equiv 1 \pmod{s}$ nach Sylow. Es folgt $6 \leq 1 + s \leq |G : \mathrm{N}_G(S)| \in \{6, 12\}$. Der Fall $|G : \mathrm{N}_G(S)| = 12$ widerspricht wie eben Satz 7.21. Also ist $s = 5$ und $G \cong A_5$ nach Satz 6.32.

8 Erzeuger und Relationen

Wir lassen in diesem Kapitel wieder zu, dass G eine unendliche Gruppe ist.

Definition 8.1. Sei A eine nichtleere Menge, die wir *Alphabet* nennen. Ein *Wort* w ist eine Folge von *Buchstaben* $w = a_1^{\epsilon_1} \dots a_n^{\epsilon_n}$ mit $a_1, \dots, a_n \in A$ und $\epsilon_1, \dots, \epsilon_n \in \{\pm 1\}$. Dabei ist auch das *leere Wort* mit $n = 0$ zugelassen. Gilt $a_i \neq a_{i+1}$ oder $\epsilon_i = \epsilon_{i+1}$ für $i = 1, \dots, n-1$, so heißt w *reduziert*. Offenbar kann man jedes Wort w in ein (eindeutig bestimmtes) reduziertes Wort $\overline{w}$ überführen, indem man Teile der Form aa^{-1} oder $a^{-1}a$ sukzessiv streicht. Auf der Menge W aller Wörter definiert $w \sim v :\Longleftrightarrow \overline{w} = \overline{v}$ eine Äquivalenzrelation. Die Menge der Äquivalenzklassen $F_A := \{[w] : w \in W\}$ bildet dann eine Gruppe bzgl. Konkatenation, d. h.

$$[w][v] := [wv] \qquad [w], [v] \in F_A.$$

Das neutrale Element ist die Äquivalenzklasse des leeren Worts []. Das Inverse von $[a_1^{\epsilon_1} \dots a_n^{\epsilon_n}]$ ist $[a_n^{-\epsilon_n} \dots a_1^{-\epsilon_1}]$. Man nennt F_A die *freie Gruppe über dem Alphabet* A.

Bemerkung 8.2.

(i) Mittels der Injektion $A \to F_A$, $a \mapsto [a]$ können wir A als Teilmenge von F_A auffassen. Es gilt dann $F_A = \langle A \rangle$.

(ii) Im Fall $|A| = 1$ ist offenbar $F_A \cong \mathbb{Z}$. Für $|A| \geq 2$ ist F_A nichtabelsch, denn $\overline{aba^{-1}b^{-1}} = aba^{-1}b^{-1}$ für $a, b \in W$, $a \neq b$.

(iii) F_A ist torsionsfrei.

Satz 8.3 (Universelle Eigenschaft freier Gruppen)**.** *Jede Abbildung $A \to G$ lässt sich zu genau einem Homomorphismus $F_A \to G$ fortsetzen.*

Beweis. Sei $f : A \to G$ gegeben. Für $w = a_1^{\epsilon_1} \dots a_n^{\epsilon_n} \in W$ definieren wir $\widehat{f}(w) := f(a_1)^{\epsilon_1} \dots f(a_n)^{\epsilon_n} \in G$. Offenbar ist $\widehat{f}(\overline{w}) = \widehat{f}(w)$. Somit induziert $\widehat{f}$ eine wohldefinierte Abbildung $F_A \to G$, die wir ebenfalls mit $\widehat{f}$ bezeichnen. Wegen $\widehat{f}(wv) = \widehat{f}(w)\widehat{f}(v)$ für $w, v \in W$ ist $\widehat{f}$ ein Homomorphismus. Wegen $F_A = \langle A \rangle$ ist $\widehat{f}$ eindeutig durch f bestimmt. □

Satz 8.4. *Für endliche Alphabete A und B sind F_A und F_B genau dann isomorph, wenn $|A| = |B|$ gilt.*

Beweis. Sei zunächst $f : A \to B$ eine Bijektion. Wegen $B \subseteq F_B$ existiert eine homomorphe Fortsetzung $\widehat{f} : F_A \to F_B$ von f nach Satz 8.3. Analog hat auch f^{-1} eine homomorphe Fortsetzung $\widehat{f^{-1}} : F_B \to F_A$. Wegen $F_A = \langle A \rangle$ und $F_B = \langle B \rangle$ ist $\widehat{f} \circ \widehat{f^{-1}} = 1$ und $\widehat{f^{-1}} \circ \widehat{f} = 1$. Also sind F_A und F_B isomorph (die Endlichkeit von A und B wird für diese Richtung nicht benutzt).

Nehmen wir nun umgekehrt an, dass F_A und F_B isomorph sind. Da es genau $2^{|A|}$ Abbildungen der Form $A \to C_2$ gibt, existieren nach Satz 8.3 genau so viele Homomorphismen $F_A \to C_2$. Wegen $F_A \cong F_B$ existieren genau $2^{|A|}$ Homomorphismen der Form $F_B \to C_2$. Dies zeigt $|A| = |B|$. □

Definition 8.5. In der Situation von Satz 8.4 nennt man $\operatorname{rk} F_A := |A|$ den *Rang* von F_A. Eine freie Gruppe vom Rang $k \in \mathbb{N}$ wird mit F_k bezeichnet.

Satz 8.6. *Sei X ein Erzeugendensystem von G mit der Eigenschaft, dass jede Abbildung von X in eine Gruppe H eine homomorphe Fortsetzung $G \to H$ besitzt. Dann ist $G \cong F_X$.*

Beweis. Nach Voraussetzung existiert ein Homomorphismus $f : G \to F_X$ mit $f(x) = x$ für $x \in X$. Nach Satz 8.3 existiert auch ein Homomorphismus $g : F_X \to G$ mit $g(x) = x$ für $x \in X$. Offenbar ist dann $f \circ g = \mathrm{id}_{F_X}$ und $g \circ f = \mathrm{id}_G$. Dies zeigt, dass f ein Isomorphismus ist. □

Satz 8.7. *Jede Gruppe G ist zu einer Faktorgruppe einer freien Gruppe F isomorph. Lässt sich G durch n Elemente erzeugen, so kann man $\operatorname{rk} F = n$ wählen.*

Beweis. Sei X ein Erzeugendensystem von G. Nach Satz 8.3 existiert ein Homomorphismus $f : F_X \to G$ mit $f(x) = x$. Offenbar ist f surjektiv und die Behauptung folgt aus dem Homomorphiesatz. □

Bemerkung 8.8.

(i) Sei X ein Erzeugendensystem für G und $f : F_X \to G$ mit $f(x) = x$ wie in Satz 8.7. Die Elemente in $\operatorname{Ker}(f)$ nennt man *Relatoren* für G bzgl. X. Für $x_1^{\epsilon_1} \dots x_n^{\epsilon_n} \in \operatorname{Ker}(f)$ gilt also $x_1^{\epsilon_1} \dots x_n^{\epsilon_n} = 1$ in G. Eine Gleichung dieser Form heißt *Relation* für G bzgl. X.

(ii) Sei umgekehrt F_A eine freie Gruppe und $X \subseteq F_A$. Sei $N := \langle gXg^{-1} : g \in F_A \rangle \trianglelefteq F_A$ der normale Abschluss von X in F_A. Wir setzen

$$\langle A \mid X \rangle = \langle A \mid \{x = 1 : x \in X\} \rangle := F_A/N.$$

Man identifiziert Buchstaben $a \in A$ oft mit ihren Nebenklassen $aN \in \langle A \mid X \rangle$ (im Allgemeinen nicht injektiv!). Ist $|A| + |X| < \infty$, so nennt man $\langle A \mid X \rangle$ *endlich präsentiert*. Auf diese Weise lässt sich jede Gruppe beschreiben, aber im Allgemeinen ist es schwierig die Eigenschaften von $\langle A \mid X \rangle$ zu bestimmen. Zum Beispiel kann man nicht entscheiden, wann eine endlich präsentierte Gruppe trivial ist (vgl. Aufgabe 37)!

Beispiel 8.9.

(i) $\langle A \mid \varnothing \rangle \cong F_A$.

(ii) $\langle x \mid x^n \rangle = \langle x \mid x^n = 1 \rangle \cong \mathbb{Z}/n\mathbb{Z} \cong C_n$.

Satz 8.10 (von Dyck). *Seien $G = \langle x_i : i \in I \rangle$ und $H = \langle y_i : i \in I \rangle$ Gruppen, sodass für jede Relation $x_{i_1}^{\epsilon_1} \dots x_{i_n}^{\epsilon_n} = 1$ in G auch die Relation $y_{i_1}^{\epsilon_1} \dots y_{i_n}^{\epsilon_n} = 1$ in H gilt. Dann existiert ein Epimorphismus $G \to H$ mit $f(x_i) = y_i$ für $i \in I$.*

Beweis. Nach Satz 8.3 existieren Epimorphismen $f_G : F_I \to G$ und $f_H : F_I \to H$ mit $f_G(i) = x_i$ und $f_H(i) = y_i$ für $i \in I$. Nach Voraussetzung gilt $\operatorname{Ker}(f_G) \leq \operatorname{Ker}(f_H)$. Also ist

$$G \cong F_I/\operatorname{Ker}(f_G) \to (F_I/\operatorname{Ker}(f_G))/(\operatorname{Ker}(f_H)/\operatorname{Ker}(f_G)) \cong F_I/\operatorname{Ker}(f_H) \cong H$$

der gesuchte Epimorphismus. □

Beispiel 8.11.

(i) Sei $G := \langle x_1, \ldots, x_n \mid [x_i, x_j] = 1 \ \forall i, j \rangle$. Offenbar ist G abelsch und jedes Element in G hat die Form $x_1^{a_1} \ldots x_n^{a_n}$ mit $a_1, \ldots, a_n \in \mathbb{Z}$. Sei nun $H := \langle y_1 \rangle \oplus \ldots \oplus \langle y_n \rangle \cong C_\infty^n$. Nach Satz 8.10 existiert ein Epimorphismus $f : G \to H$ mit $f(x_i) = y_i$ für $i = 1, \ldots, n$. Offenbar ist f auch injektiv und $G \cong H \cong C_\infty^n$. Dies erklärt den Begriff *freie abelsche Gruppe*. Im Allgemeinen ist jede abelsche Gruppe offenbar zu einer Faktorgruppe von $\langle (x_i)_{i \in I} : [x_i, x_j] = 1 \ \forall i, j \in I \rangle$ isomorph.

(ii) Sei $G := \langle x, y \mid x^n = y^2 = (xy)^2 = 1 \rangle$ für $n \geq 2$. Wegen $xyxy = 1$ und $y^2 = 1$ ist $xy = y^{-1}x^{-1} = yx^{-1}$. Auf diese Weise kann man jedes Element in G in der Form $x^i y^j$ mit $i, j \in \mathbb{Z}$ schreiben. Wegen $x^n = y^2 = 1$ kann man $i \in \{0, \ldots, n-1\}$ und $j \in \{0, 1\}$ annehmen. Insbesondere gilt $|G| \leq 2n$. Sei nun $H \cong D_{2n}$. Dann existieren Elemente $\widetilde{x}, \widetilde{y} \in H$ mit $H = \langle \widetilde{x} \rangle \rtimes \langle \widetilde{y} \rangle$. Insbesondere ist $\widetilde{x}^n = \widetilde{y}^2 = 1$. Außerdem gilt $\widetilde{y}\widetilde{x}\widetilde{y}^{-1} = \widetilde{x}^{-1}$, also $(\widetilde{x}\widetilde{y})^2 = 1$. Nach Satz 8.10 gibt es ein Epimorphismus $G \to H$. Wegen $|H| = 2n \geq |G|$ ist daher $G \cong H \cong D_{2n}$.

Satz 8.12 (Gauss)**.** *Für jede Primzahl p und $n \geq 1$ gilt*

$$\mathrm{Aut}(C_{p^n}) \cong \begin{cases} C_2 \times C_{2^{n-2}} & \text{falls } p = 2 \leq n, \\ C_{p^{n-1}(p-1)} & \text{sonst.} \end{cases}$$

Beweis. Nach Satz 2.4 ist $\mathrm{Aut}(C_{p^n}) \cong (\mathbb{Z}/p^n\mathbb{Z})^\times =: G$.

Sei zunächst $p > 2$. Wir müssen zeigen, dass G zyklisch ist. Im Fall $n = 1$ ist $G = \mathbb{F}_p^\times$ und die Behauptung gilt (Algebra). Sei nun $n \geq 2$. Dann ist $|G| = \varphi(p^n) = p^{n-1}(p-1)$. Die kanonische Abbildung $\Psi : G \to (\mathbb{Z}/p\mathbb{Z})^\times$, $a + p^n\mathbb{Z} \mapsto a + p\mathbb{Z}$ ist offenbar ein Epimorphismus. Insbesondere ist $P := \mathrm{Ker}(\Psi) \in \mathrm{Syl}_p(G)$ und $G/P \cong C_{p-1}$. Nach Satz 2.10 genügt es zu zeigen, dass P zyklisch ist. Wir zeigen genauer, dass P von $1 + p + p^n\mathbb{Z} \in P$ erzeugt wird. Dafür berechnet man

$$(1+p)^{p^{n-2}} = \sum_{k=0}^{p^{n-2}} \binom{p^{n-2}}{k} p^k \equiv 1 + p^{n-1} \not\equiv 1 \pmod{p^n}.$$

Sei nun $p = 2$ und o. B. d. A. $n \geq 2$. Dann ist $|G| = 2^{n-1}$. Wegen $(-1 + 2^n\mathbb{Z})^2 = 1 + 2^n\mathbb{Z}$ genügt es

$$G = \langle -1 + 2^n\mathbb{Z} \rangle \oplus \langle 5 + 2^n\mathbb{Z} \rangle$$

zu zeigen. Der Fall $n = 2$ ist klar. Sei also $n \geq 3$. Man berechnet

$$5^{2^{n-3}} = (1+4)^{2^{n-3}} = \sum_{k=0}^{2^{n-3}} \binom{2^{n-3}}{k} 2^{2k} \equiv 1 + 2^{n-1} \pmod{2^n}.$$

und

$$5^{2^{n-2}} = (1 + 2^{n-1})^2 \equiv 1 \pmod{2^n}.$$

Also ist $|\langle 5 + 2^n\mathbb{Z} \rangle| = 2^{n-2}$. Wegen $-1 \not\equiv 1 + 2^{n-1} \pmod{2^n}$ ist auch $\langle -1 + 2^n\mathbb{Z} \rangle \cap \langle 5 + 2^n\mathbb{Z} \rangle = 1$. □

Satz 8.13. *Sei P eine p-Gruppe der Ordnung p^n mit einer zyklischen Untergruppe der Ordnung p^{n-1}. Dann gilt eine der folgenden Aussagen:*

(i) $P \cong C_{p^n}$ oder $P \cong C_{p^{n-1}} \times C_p$.

(ii) $n \geq 3$ und $P \cong M_{p^n} := \langle x, y \mid x^{p^{n-1}} = y^p = 1, \ yxy^{-1} = x^{1+p^{n-2}} \rangle$.

(iii) $p = 2$, $n \geq 3$ *und* $P \cong Q_{2^n} := \langle x, y \mid x^{2^{n-1}} = 1,\ y^2 = x^{2^{n-2}},\ yxy^{-1} = x^{-1} \rangle$ *(*(verallgemeinerte*)* Quaternionengruppe*).*

(iv) $p = 2$, $n \geq 4$ *und* $P \cong D_{2^n}$.

(v) $p = 2$, $n \geq 4$ *und* $P \cong SD_{2^n} := \langle x, y \mid x^{2^{n-1}} = y^2 = 1,\ yxy^{-1} = x^{-1+2^{n-2}} \rangle$ *(*Semidiedergruppe*).*

Beweis. Ist P abelsch, so gilt offenbar (i) nach Satz 2.10. Sei nun P nichtabelsch. Dann ist $n \geq 3$. Sei $x \in P$ mit $|\langle x \rangle| = p^{n-1}$. Dann ist $\langle x \rangle \trianglelefteq P$ nach Satz 4.8. Nehmen wir zunächst an, dass $\langle x \rangle$ ein Komplement in P besitzt, d. h. es gilt $P = \langle x \rangle \rtimes \langle y \rangle$ für ein $y \in P$ mit $y^p = 1$. Ist $p > 2$, so ist $\mathrm{Aut}(\langle x \rangle)$ zyklisch nach Satz 8.12. Es muss dann $yxy^{-1} = x^{1+p^{n-2}}$ gelten, denn $(1 + p^{n-2})^p \equiv 1 \pmod{p^{n-1}}$. Nach Satz 8.10 existiert ein Epimorphismus $M_{p^n} \to P$. Offenbar gilt $|M_{p^n}| \leq p^n$ und es folgt $P \cong M_{p^n}$. Sei nun $p = 2$. Im Fall $n = 3$ ist $\mathrm{Aut}(\langle x \rangle)$ immer noch zyklisch und man erhält wieder $P \cong M_8 \cong D_8$. Sei also $n \geq 4$. Nach Satz 8.12 besitzt $\mathrm{Aut}(\langle x \rangle)$ genau drei Involutionen (=Elemente der Ordnung 2): $x \mapsto x^{-1}$, $x \mapsto x^{1+2^{n-2}}$ und $x \mapsto x^{-1+2^{n-2}}$. Der erste Fall führt zu $P \cong D_{2^n}$, der zweite zu $P \cong M_{2^n}$ und der dritte zu $P \cong SD_{2^n}$.

Im Folgenden können wir annehmen, dass $\langle x \rangle$ kein Komplement in P besitzt. Sei $y \in P \setminus \langle x \rangle$. Dann ist $y^p \in \langle x \rangle = \mathrm{C}_P(x)$. Die Operation von $\langle y \rangle$ auf $\langle x \rangle$ induziert also nach wie vor einen Automorphismus der Ordnung p. Im Fall $y^p \notin \langle x^p \rangle$ wäre $P = \langle y \rangle$ abelsch. Sei also $i \in \mathbb{Z}$ mit

$$x^{pi} = \begin{cases} y^{-2}x^{2^{n-2}} & \text{falls } p = 2, \\ y^{-p} & \text{falls } p > 2. \end{cases}$$

Im Fall $yxy^{-1} = x^{1+p^{n-2}}$ ist $[y, x] = x^{1+p^{n-2}}x^{-1} = x^{p^{n-2}} \in \mathrm{Z}(P)$ und Aufgabe 11(b) liefert

$$(x^i y)^p = x^{ip} y^p [y, x]^{\binom{p}{2}} = 1.$$

Dann wäre aber $\langle x^i y \rangle$ ein Komplement von $\langle x \rangle$. Also ist $p = 2$ und $yxy^{-1} \in \{x^{-1}, x^{-1+2^{n-2}}\}$, wobei im zweiten Fall $n \geq 4$ gilt. In beiden Fällen ist $y^2 = yy^2y^{-1} = yx^{2k}y^{-1} = x^{-2k} = y^{-2}$ und $y^4 = 1$. Dies zeigt $y^2 = x^{2^{n-2}}$. Gilt nun $yxy^{-1} = x^{-1+2^{n-2}} = x^{-1}y^2$, so ist $(xy)^2 = x(yxy^{-1})y^2 = y^4 = 1$. Dann wäre $\langle xy \rangle$ ein Komplement von $\langle x \rangle$. Also ist $xyx^{-1} = y^{-1}$ und es gibt einen Epimorphismus $Q_{2^n} \to P$. Es ist leicht zu sehen, dass $|Q_{2^n}| \leq 2^n$ gilt. Somit ist $P \cong Q_{2^n}$. □

Satz 8.14. *Die Gruppen M_{p^n}, D_{2^n}, Q_{2^n} und SD_{2^n} haben die Ordnung p^n (bzw. 2^n) und sind paarweise nicht isomorph.*

Beweis. Es ist klar, dass man semidirekte Produkte $C_{p^{n-1}} \rtimes C_p$ mit geeigneten Operationen konstruieren kann. Somit zeigt Satz 8.13, dass M_{p^n}, D_{2^n} und SD_{2^n} die „richtige“ Ordnung haben. Sei nun $Q = \langle x, y \rangle \leq \mathrm{GL}(2, \mathbb{C})$ mit

$$x := \begin{pmatrix} e^{\frac{2\pi i}{2^{n-1}}} & 0 \\ 0 & e^{-\frac{2\pi i}{2^{n-1}}} \end{pmatrix}, \qquad y := \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

Offenbar gilt $x^{2^{n-1}} = 1$, $y^2 = x^{2^{n-2}}$ und $yxy^{-1} = x^{-1}$. Also hat jedes Element in Q die Form $x^i y^j$ mit $i \in \{0, \ldots, 2^{n-1} - 1\}$ und $j \in \{0, 1\}$. Wegen $y \notin \langle x \rangle$ ist $|Q| = 2^n$. Nach Satz 8.13 gilt $Q \cong Q_{2^n}$.

Es verbleibt zu zeigen, dass die Gruppen M_{2^n}, D_{2^n}, Q_{2^n} und SD_{2^n} paarweise nicht isomorph sind (mit der Ausnahme $M_8 \cong D_8$). Die semidirekten Produkt M_{2^n}, D_{2^n} und SD_{2^n} besitzen mindestens zwei Involutionen. In Q_{2^n} ist andererseits $(x^i y)^2 = x^i y x^i y^{-1} y^2 = y^2 \neq 1$ für $i \in \mathbb{Z}$. Daher besitzt Q_{2^n} nur eine Involution und es gilt $Q_{2^n} \ncong M_{2^n}$, $Q_{2^n} \ncong D_{2^n}$ und $Q_{2^n} \ncong SD_{2^n}$. Wir können nun $n \geq 4$ annehmen. In der Gruppe M_{2^n} gilt $\langle [x, y] \rangle = \langle x(yx^{-1}y^{-1}) \rangle = \langle x^{2^{n-2}} \rangle \trianglelefteq M_{2^n}$. Da $M_{2^n}/\langle [x, y] \rangle$

abelsch ist, gilt $M'_{2^n} = \langle [x,y] \rangle \cong C_2$. In D_{2^n} gilt andererseits $[x,y] = x^2$ und damit $|D'_{2^n}| \geq 2^{n-2}$. In SD_{2^n} ist analog $[x,y] = x^{2+2^{n-2}}$ und $|SD'_{2^n}| \geq 2^{n-2}$. Dies zeigt $M_{2^n} \ncong D_{2^n}$ und $M_{2^n} \ncong SD_{2^n}$. Schließlich müssen wir noch D_{2^n} von SD_{2^n} unterscheiden. Nach Burnsides Basissatz ist $|D_{2^n} : \Phi(D_{2^n})| = 4 = |SD_{2^n} : \Phi(SD_{2^n})|$. Die maximalen Untergruppen von D_{2^n} sind daher $\langle x \rangle$, $\langle x^2, y \rangle \cong D_{2^{n-1}}$ und $\langle x^2, xy \rangle \cong D_{2^{n-1}}$. Die maximalen Untergruppen von SD_{2^n} sind andererseits $\langle x \rangle$, $\langle x^2, y \rangle \cong D_{2^{n-1}}$ und $\langle x^2, xy \rangle \cong Q_{2^{n-1}} \ncong D_{2^{n-1}}$. Also ist $D_{2^n} \ncong SD_{2^n}$. $\square$

9 Zentralprodukte und extraspezielle Gruppen

Bemerkung 9.1. Sei P eine nichtabelsche p-Gruppe der Ordnung p^n. Da P nicht zyklisch ist, gilt $|P : P'| \geq |P : \Phi(P)| \geq p^2$. Dies zeigt, dass die Nilpotenzklasse von P höchstens $n-1$ beträgt (Satz 3.9). Gilt Gleichheit, so sagt man: P hat *maximale Klasse*. In diesem Fall ist $|P^i|p^i = |P|$ für $i \geq 2$.

Lemma 9.2. *Sei P eine p-Gruppe der Ordnung p^n mit maximaler Klasse. Sei $N \trianglelefteq P$ mit $|N| = p^i \leq p^{n-2}$. Dann ist $N = \mathrm{Z}_i(P) = P^{n-i}$.*

Beweis. Induktion nach n: Für $n = 3$ folgt die Behauptung aus Beispiel 4.20. Sei also $n \geq 4$ und $N \neq 1$. Da auch $P/\mathrm{Z}(P)$ maximale Klasse hat, gilt $|\mathrm{Z}(P)| = p$. Nach Satz 3.14 ist $\mathrm{Z}(P) \leq N$. Induktion impliziert daher $N/\mathrm{Z}(P) = \mathrm{Z}_{i-1}(P/\mathrm{Z}(P)) = \mathrm{Z}_i(P)/\mathrm{Z}(P)$ und $N = \mathrm{Z}_i(P)$. Nach Bemerkung 9.1 ist auch P^{n-i} ein Normalteiler der Ordnung p^i. Also ist $P^{n-i} = \mathrm{Z}_i(P) = N$. □

Satz 9.3 (Taussky)**.** *Für eine nichtabelsche 2-Gruppe P sind folgende Aussagen äquivalent:*

(i) *P hat maximale Klasse.*

(ii) *$|P : P'| = 4$.*

(iii) *P ist eine Diedergruppe, eine Quaternionengruppe oder eine Semidiedergruppe.*

Beweis. Die Implikation (i)$\Longrightarrow$(ii) folgt aus Bemerkung 9.1. Sei nun $|P : P'| = 4$. Sei $2^n := |P|$ minimal, sodass (iii) nicht erfüllt ist. Wir haben in Satz 8.14 bereits gesehen, dass $|M_{2^n}'| = 2$ gilt. Nach Satz 8.13 ist daher $\exp(P) \leq 2^{n-2}$. Sei $Z \leq \mathrm{Z}(P) \cap P'$ mit $|Z| = 2$ (Satz 3.14). Dann ist $|P/Z : (P/Z)'| = |P/P'| = 4$. Nach Wahl von P ist $P/Z \in \{D_{2^{n-1}}, Q_{2^{n-1}}, SD_{2^{n-1}}\}$. Sei also $x \in P$ mit $|P : \langle x\rangle Z| = 2$. Wegen $Z \leq \mathrm{Z}(P)$ und $\exp(P) \leq 2^{n-2}$ ist $\langle x\rangle Z \cong C_{2^{n-2}} \times C_2$. Aus Aufgabe 12 folgt $\mathrm{Z}(P) = Z$. Für $y \in P \setminus \langle x\rangle Z$ gilt $yxy^{-1} \in x^{-1}Z \cup x^{-1+2^{n-3}}Z$ und $yx^2y^{-1} = x^{-2}$. Dies liefert den Widerspruch $x^{2^{n-3}} \in \mathrm{Z}(P) = Z$. Also muss (iii) gelten.

Sei nun $P \in \{D_{2^n}, Q_{2^n}, SD_{2^n}\}$. Wir zeigen (i) durch Induktion nach n (vgl. Aufgabe 19). Im Fall $n = 3$ sind D_8 und Q_8 nichtabelsch und daher von maximaler Klasse. Sei nun $n \geq 4$. Dann ist $[x, y] \in \{x^2, x^{2+2^{n-2}}\}$ und $P' = \langle x^2\rangle$. Aus Aufgabe 12 folgt $\mathrm{Z}(P) = \langle x^{2^{n-2}}\rangle$. Nach Induktion hat $P/\mathrm{Z}(P) \cong D_{2^{n-1}}$ maximale Klasse und daher auch P. □

Bemerkung 9.4. Für $p > 2$ gibt es nichtabelsche p-Gruppen P mit $|P : P'| = p^2$, die nicht maximale Klasse haben. Blackburn hat alle 3-Gruppen mit maximaler Klasse klassifiziert. Andererseits kennt man die p-Gruppen maximaler Klasse für $p > 3$ nicht.

Satz 9.5. *Sei P eine nicht-zyklische p-Gruppe, in der jeder abelsche Normalteiler zyklisch ist. Dann ist $p = 2$ und P hat maximale Klasse.*

Beweis. Sei $A \trianglelefteq P$ ein maximal abelscher Normalteiler (d. h. es gibt keinen abelschen Normalteiler von P, der A echt enthält). Nach Voraussetzung ist A zyklisch und daher $A < P$. Außerdem ist $A \leq \mathrm{C}_P(A) \trianglelefteq P$. Nehmen wir $A < \mathrm{C}_P(A)$ an. Da die Hauptfaktoren von P alle Ordnung p haben (Beispiel 3.8), existiert ein Normalteiler $N \trianglelefteq P$ mit $A < N \leq \mathrm{C}_P(A)$ und $|N : A| = p$. Dann ist $A \leq \mathrm{Z}(\mathrm{C}_P(A)) \cap N \leq \mathrm{Z}(N)$ und $N/\mathrm{Z}(N)$ ist zyklisch. Also ist N abelsch im Widerspruch zur Wahl von A. Dies zeigt $\mathrm{C}_P(A) = A$ und $P/A \leq \mathrm{Aut}(A)$. Im Fall $|A| = p$ wäre $p \nmid |\mathrm{Aut}(A)|$. Also ist $|A| \geq p^2$. Sei $B \leq A$ mit $|B| = p^2$. Da A zyklisch ist, gilt $B \trianglelefteq P$. Für $C := \mathrm{C}_P(B) \trianglelefteq P$ ist $P/C \leq \mathrm{Aut}(B) \cong C_{p(p-1)}$ und daher $|P : C| \leq p$.

Nehmen wir $A < C$ an. Wie üblich existiert ein $N \trianglelefteq P$ mit $A < N \leq C$ und $|N : A| = p$. Nach Wahl von A ist N nichtabelsch und wir können Satz 8.13 anwenden. Wegen $B \leq \mathrm{Z}(N)$ kommt nach Taussky nur $N \cong M_{p^n}$ in Frage. Es gilt $M'_{p^n} = \langle x^{p^{n-2}} \rangle \cong C_p$ und $M_{p^n}/M'_{p^n} \cong C_{p^{n-2}} \times C_p$. Jedes Element der Ordnung p in M_{p^n} liegt also in $\langle x^{p^{n-3}}, y \rangle$. Da $x^{p^{n-3}}$ Ordnung p^2 hat, bilden die Elemente der Ordnung p in M_{p^n} die charakteristische Untergruppe $E := \langle x^{p^{n-2}}, y \rangle \cong C_p \times C_p$. Dann ist E aber ein nicht-zyklischer, abelscher Normalteiler von P. Dieser Widerspruch zeigt $A = C$.

Also ist $|P : A| = p$. Wieder lässt sich Satz 8.13 anwenden. Der Fall $P \cong M_{p^n}$ ist wie eben ausgeschlossen. Dies zeigt die Behauptung. □

Satz 9.6. *Für jede p-Gruppe P sind folgende Aussagen äquivalent:*

(i) *P besitzt nur eine Untergruppe der Ordnung p.*

(ii) *Jede abelsche Untergruppe von P ist zyklisch.*

(iii) *P ist zyklisch oder eine Quaternionengruppe.*

Beweis. Die Implikation (i)$\Longrightarrow$(ii) folgt aus Satz 2.10. Gilt (ii), so ist P zyklisch oder eine Diedergruppe, eine Quaternionengruppe oder eine Semidiedergruppe nach Satz 9.5. In (Semi)diedergruppen ist die abelsche Untergruppe $\langle x^{2^{n-2}}, y \rangle$ nicht zyklisch. Dies zeigt (iii). Nehmen wir nun (iii) an. Ist P zyklisch, so folgt (i) aus Satz 2.4. Für Quaternionengruppen hatten wir in Satz 8.14 bereits gesehen, dass nur eine Involution existiert. □

Satz 9.7. *Für eine Primzahl p gibt es bis auf Isomorphie genau fünf Gruppen der Ordnung p^3. Diese sind gegeben durch:*

(i) *C_{p^3}.*

(ii) *$C_{p^2} \times C_p$.*

(iii) *C_p^3.*

(iv) *M_{p^3}.*

(v) *Q_8 für $p = 2$.*

(vi) *$p_+^{1+2} := \langle x, y \mid x^p = y^p = [x,y]^p = [x,x,y] = [y,x,y] = 1 \rangle$ für $p > 2$.*

Beweis. Sei $|P| = p^3$. Wir können sicher annehmen, dass P nichtabelsch ist. Nach Satz 8.13 dürfen wir auch $\exp(P) = p$ voraussetzen. Dann ist $p > 2$, denn anderenfalls wäre $xy = (xy)^{-1} = y^{-1}x^{-1} = yx$ für $x, y \in P$. Wegen $|P : \Phi(P)| = p^2$ lässt sich P durch zwei Elemente x, y erzeugen. Sicher ist dann $x^p = y^p = [x,y]^p = 1$ und $[x,x,y], [y,x,y] \in P^3 = 1$. Nach Satz 8.10 gibt es einen Epimorphismus $p_+^{1+2} \to P$. Wir müssen nun zeigen, dass $|p_+^{1+2}| \leq p^3$ gilt. Sei dafür $z := [x,y]$. Wegen $xy = [x,y]yx = zyx = yxz$ lässt sich jedes Element in p_+^{1+2} in der Form $x^i y^j z^k$ mit $i, j, k \in \{0, \ldots, p-1\}$ schreiben. Dies zeigt $P \cong p_+^{1+2}$.

Es verbleibt zu zeigen, dass der letzte Fall tatsächlich auftritt. Dafür betrachten wir die Gruppe $P \leq \mathrm{GL}(3,p)$ der oberen Dreiecksmatrizen mit Einsen auf der Hauptdiagonale. Dann ist $|P| = p^3$. Wegen

$$\begin{pmatrix} 1 & 1 & . \\ . & 1 & . \\ . & . & 1 \end{pmatrix} \begin{pmatrix} 1 & . & . \\ . & 1 & 1 \\ . & . & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 \\ . & 1 & 1 \\ . & . & 1 \end{pmatrix} \neq \begin{pmatrix} 1 & 1 & . \\ . & 1 & 1 \\ . & . & 1 \end{pmatrix} = \begin{pmatrix} 1 & . & . \\ . & 1 & 1 \\ . & . & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 & . \\ . & 1 & . \\ . & . & 1 \end{pmatrix}$$

ist P nichtabelsch. Nach dem binomischen Satz ist $x^p - 1 = (x-1)^p = (x-1)^3(x-1)^{p-3} = 0$ für alle $x \in P$, denn

$$\begin{pmatrix} . & * & * \\ . & . & * \\ . & . & . \end{pmatrix}^3 = \begin{pmatrix} . & * & * \\ . & . & * \\ . & . & . \end{pmatrix} \begin{pmatrix} . & . & * \\ . & . & . \\ . & . & . \end{pmatrix} = 0.$$

Dies zeigt schließlich $\exp(P) = p$. □

Definition 9.8. Eine p-Gruppe P heißt *extraspeziell*, falls $P' = \Phi(P) = \mathrm{Z}(P) \cong C_p$ gilt.

Beispiel 9.9. Nach Beispiel 4.20 ist jede nichtabelsche Gruppe der Ordnung p^3 extraspeziell.

Lemma 9.10. *Sei P extraspeziell und $\alpha \in \mathrm{Aut}(P)$ mit $\alpha(x)\,\mathrm{Z}(P) = x\,\mathrm{Z}(P)$ für alle $x \in P$. Dann ist $\alpha \in \mathrm{Inn}(P)$.*

Beweis. Sei $|P/\mathrm{Z}(P)| = p^n$. Dann gibt es ein Erzeugendensystem $x_1, \ldots, x_n \in P$ von P. Es gilt $\alpha(x_i) \in x_i\,\mathrm{Z}(P)$ für $i = 1, \ldots, n$ und α ist durch diese Bilder eindeutig bestimmt. Somit gibt es höchstens p^n viele Automorphismen mit der angegebenen Eigenschaft. Andererseits erfüllt jeder innere Automorphismus die Bedingung. Wegen $|\mathrm{Inn}(P)| = |P/\mathrm{Z}(P)| = p^n$ folgt die Behauptung. □

Lemma 9.11. *Sei P eine extraspezielle Untergruppe einer Gruppe G mit $[G,P] \leq \mathrm{Z}(P)$. Dann ist $G = P\,\mathrm{C}_G(P)$.*

Beweis. Wegen $[G,P] \leq \mathrm{Z}(P) \leq P$ ist $P \trianglelefteq G$. Für $g \in G$ definiert $\alpha(x) := gxg^{-1}$ $(x \in P)$ einen Automorphismus auf P. Dabei gilt $\alpha(x)\,\mathrm{Z}(P) = gxg^{-1}x^{-1}x\,\mathrm{Z}(P) = [g,x]x\,\mathrm{Z}(P) = x\,\mathrm{Z}(P)$. Nach Lemma 9.10 ist α ein innerer Automorphismus auf P. Daher existiert ein $x \in P$ mit $gyg^{-1} = \alpha(y) = xyx^{-1}$ für alle $y \in P$. Es folgt $g = xx^{-1}g \in P\,\mathrm{C}_G(P)$. □

Definition 9.12. Eine Gruppe G heißt *Zentralprodukt* von Untergruppen $N_1, \ldots, N_k \leq G$, falls:

- $G = \langle N_1, \ldots, N_k \rangle$.
- $[N_i, N_j] = 1$ für $i \neq j$.

Wir schreiben $G = N_1 * \ldots * N_k$.

Bemerkung 9.13. Wegen $[N_i, N_j] = 1$ ist $N_i \trianglelefteq G = N_1 * \ldots * N_k$ für $i = 1, \ldots, k$. Somit ist die direkte Summe $N_1 \oplus \ldots \oplus N_k$ auch ein Zentralprodukt. Wie bei der direkten Summe gilt $N * M = M * N$ und $(N_1 * N_2) * N_3 = N_1 * (N_2 * N_3)$ (vgl. Bemerkung 2.9).

Beispiel 9.14. Es gilt $C_2 \cong C_2 * C_2$, aber auch $C_2^2 \cong C_2 * C_2$. Die Schreibweise $N_1 * \ldots * N_k$ ist also in der Regel nicht eindeutig.

Satz 9.15. *Sei $G = N_1 * \ldots * N_k$ mit $k \geq 2$. Dann ist $\bigcap_{i=1}^k N_i \leq \mathrm{Z}(G)$ und $G/\mathrm{Z}(G) \cong N_1/\mathrm{Z}(N_1) \times \ldots \times N_k/\mathrm{Z}(N_k)$.*

Beweis. Wegen $[N_i, N_j] = 1$ ist $\bigcap_{i=1}^k N_i \leq \mathrm{Z}(\langle N_1, \ldots, N_k\rangle) = \mathrm{Z}(G)$ und $N_i\,\mathrm{Z}(G)/\mathrm{Z}(G) \cong N_i/N_i \cap \mathrm{Z}(G) = N_i/\mathrm{Z}(N_i)$. Es genügt also $G/\mathrm{Z}(G) = N_1\,\mathrm{Z}(G)/\mathrm{Z}(G) \oplus \ldots \oplus N_k\,\mathrm{Z}(G)/\mathrm{Z}(G)$ zu zeigen. Es gilt $N_i\,\mathrm{Z}(G) \cap \prod_{j\neq i} N_j\,\mathrm{Z}(G) = \mathrm{Z}(G)$. Die Behauptung folgt. □

Bemerkung 9.16. Analog zum direkten Produkt (vs. direkte Summe) konstruieren wir nun ein „äußeres“ Zentralprodukt.

Satz 9.17. *Seien $G_1, \ldots, G_k$ Gruppen mit $Z_i \leq \mathrm{Z}(G_i)$ und $Z_1 \cong \ldots \cong Z_k$ mit $k \geq 2$. Dann existiert ein Zentralprodukt der Form $G = N_1 * \ldots * N_k$ mit $N_i \cong G_i$ $(i = 1, \ldots, k)$ und $\bigcap_{i=1}^k N_i \cong Z_1$.*

Beweis. Wir wählen Isomorphismen $\varphi_i : Z_1 \to Z_i$ für $i = 2, \ldots, k$. Dann ist

$$Z := \langle z^{-1}\varphi_i(z) : z \in Z_1,\ i = 2, \ldots, k\rangle \leq Z_1 \times \ldots \times Z_k \leq \mathrm{Z}(G_1 \times \ldots \times G_k).$$

Sei $G := (G_1 \times \ldots \times G_k)/Z$. Dann wird G von den Normalteilern $N_i := G_iZ/Z \cong G_i/G_i \cap Z \cong G_i$ erzeugt. Dabei gilt $[N_i, N_j] = [G_iZ/Z, G_jZ/Z] = [G_i, G_j]Z/Z = 1$ für $i \neq j$. Also ist $G = N_1 * \ldots * N_k$. Für $z_1 \in Z_1$ und $i \in \{1, \ldots, k\}$ ist $z_1Z = z_1z_1^{-1}\varphi_i(z_1)Z = \varphi_i(z_1)Z$. Dies zeigt $Z_1 \cong Z_1Z/Z = Z_iZ/Z \leq \bigcap_{i=1}^k N_i$. Sei nun $g_1Z = \ldots = g_kZ \in \bigcap_{i=1}^k N_i$ mit $g_i \in G_i$. Dann ist $g_1^{-1}g_i \in Z \leq Z_1 \times \ldots \times Z_k$ und es folgt $g_i \in Z_i$ für $i = 1, \ldots, k$. Also ist $\bigcap_{i=1}^k N_i = Z_1Z/Z \cong Z_1$. □

Satz 9.18. *Jede extraspezielle p-Gruppe P hat die Form $P = E_1 * \ldots * E_k$ mit $E_i \in \{D_8, Q_8\}$ (falls $p = 2$) bzw. $E_i \in \{M_{p^3}, p_+^{1+2}\}$ (falls $p > 2$) für $i = 1, \ldots, k$. Dabei ist $\bigcap_{i=1}^k E_i \neq 1$. Insbesondere ist $|P| = p^{2k+1}$.*

Beweis. Sei P extraspeziell der Ordnung p^n. Wir argumentieren durch Induktion nach n. Seien $x_1, y_1 \in P$ mit $[x_1, y_1] \neq 1$. Dann ist $P' = \langle [x_1, y_1]\rangle \leq \langle x_1, y_1\rangle =: E_1 \trianglelefteq P$. Nach Lemma 4.12 ist $\Phi(E_1) \leq \Phi(P) = P'$. Aus Burnsides Basissatz folgt daher $|E_1| = p^3$ und $E_1 \in \{D_8, Q_8\}$ (bzw. $E_1 \in \{M_{p^3}, p_+^{1+2}\}$). Im Fall $P = E_1$ sind wir fertig. Sei also $E_1 < P$.

Nach Lemma 9.11 ist $P = E_1Q$ mit $Q := \mathrm{C}_P(E_1)$. Es gilt $\mathrm{Z}(Q) \leq \mathrm{C}_P(E_1Q) = \mathrm{Z}(P) \leq E_1$. Insbesondere ist Q nichtabelsch und daher $1 \neq \Phi(Q) \leq Q' \leq P'$ und $\Phi(Q) = Q' = \mathrm{Z}(Q) = P' \cong C_p$. Dies zeigt, dass Q extraspeziell ist. Nach Induktion hat $Q = E_2 * \ldots * E_k$ die gewünschte Form. Also ist auch $P = E_1 * Q = E_1 * \ldots * E_k$. □

Bemerkung 9.19. Wir beschäftigen uns nun mit der Eindeutigkeit in Satz 9.18.

Lemma 9.20. *Sei P nichtabelsch der Ordnung p^3 und $a, b \in P' \setminus \{1\}$. Dann existiert ein $\alpha \in \mathrm{Aut}(P)$ mit $\alpha(a) = b$.*

Beweis. Im Fall $p = 2$ ist $a = b$ und es gibt nichts zu tun. Sei daher $p > 2$. Sei zunächst $P = \langle x, y\rangle \cong M_{p^3}$. Dann ist $P' = \langle x^p\rangle$ und es existieren $i, j \in \mathbb{Z}$ mit $a = x^{ip}$ und $b = x^{jp}$. Es gilt $(x^i)^{p^2} = 1 = y^p$ und $y(x^i)y^{-1} = x^{i(1+p)} = (x^i)^{1+p}$. Also erfüllen die Erzeuger x^i und y von P die gleichen Relationen wie x und y. Analog erfüllen auch x^j und y diese Relationen. Nach Satz 8.10 gibt es ein $\alpha \in \mathrm{Aut}(P)$ mit $\alpha(x^i) = x^j$. Sicher ist dann $\alpha(a) = b$.

Sei nun $P = \langle x, y\rangle \cong p_+^{1+2}$. Dann ist $a = [x,y]^i$ und $b = [x,y]^j$ für $i, j \in \mathbb{Z}$. Wie eben existiert ein $\alpha \in \mathrm{Aut}(P)$ mit $\alpha(x^i) = x^j$ und $\alpha(y) = y$. Nach Bemerkung 3.2 gilt $\alpha(a) = \alpha([x,y]^i) = \alpha([x^i, y]) = [x^j, y] = [x,y]^j = b$. □

Satz 9.21. *Für $k \geq 1$ gibt es bis auf Isomorphie genau zwei extraspezielle Gruppen der Ordnung p^{2k+1}, nämlich:*

(i) $p_-^{1+2k} := M_{p^3} * \ldots * M_{p^3}$ *und* $p_+^{1+2k} := p_+^{1+2} * \ldots * p_+^{1+2}$, *falls* $p > 2$.

(ii) $2_-^{1+2k} := D_8 * D_8 * \ldots * D_8$ *und* $2_+^{1+2k} := Q_8 * D_8 * \ldots * D_8$, *falls* $p = 2$.

Beweis. Sei $P = E_1 * \ldots * E_k$ extraspeziell wie in Satz 9.18. Wir müssen zunächst zeigen, dass der Isomorphietyp von P durch die E_i eindeutig bestimmt ist. Sei also $Q = F_1 * \ldots * F_k$ mit $E_i \cong F_i$ für $i = 1, \ldots, k$. Sei außerdem $\bigcap_{i=1}^k E_i \neq 1 \neq \bigcap_{i=1}^k F_i$ und damit $|P| = |Q|$ nach Satz 9.15. Wir wählen Isomorphismen $\varphi_i : E_i \to F_i$. Nach Lemma 9.20 können wir $\varphi_i(z) = \varphi_1(z)$ für $i = 2, \ldots, k$ und $z \in \mathrm{Z}(E_i) = \mathrm{Z}(P)$ annehmen. Jedes Element in P hat die Form $x_1 \ldots x_k$ mit $x_i \in E_i$ für $i = 1, \ldots, k$. Im Fall $x_1 \ldots x_k = 1$ gilt $x_i = (x_1 \ldots x_{i-1} x_{i+1} \ldots x_k)^{-1} \in \mathrm{Z}(E_i)$. Also ist

$$\begin{aligned} x_1 \ldots x_k = y_1 \ldots y_k &\iff x_1 y_1^{-1} \ldots x_k y_k^{-1} = 1 \iff \varphi_1(x_1 y_1^{-1} \ldots x_k y_k^{-1}) = 1 \\ &\iff \varphi_1(x_1 y_1^{-1}) \ldots \varphi_k(x_k y_k^{-1}) = 1 \iff \varphi_1(x_1) \ldots \varphi_k(x_k) = \varphi_1(y_1) \ldots \varphi_k(y_k). \end{aligned}$$

Somit ist die Abbildung $\Psi : P \to Q$, $x_1 \ldots x_k \mapsto \varphi_1(x_1) \ldots \varphi_k(x_k)$ wohldefiniert und injektiv. Wegen $|P| = |Q|$ ist Ψ auch bijektiv. Offenbar ist Ψ auch ein Isomorphismus.

Wir zeigen nun $P := M_{p^3} * M_{p^3} \cong M_{p^3} * p_+^{1+2}$ für $p > 2$. Sei $P = \langle x, y, a, b\rangle$ mit $\langle x, y\rangle \cong \langle a, b\rangle \cong M_{p^3}$ und $[y,x] = x^p = a^p = [b,a]$. Wir definieren $P_1 := \langle x, yb\rangle \cong M_{p^3}$ und $P_2 := \langle xa^{-1}, b\rangle$. Wegen $(xa^{-1})^p = x^p a^{-p} = 1$, $[xa^{-1}, b]^p = [a^{-1}, b]^p = 1$ und $[xa^{-1}, xa^{-1}, b] = [b, xa^{-1}, b] = 1$ ist $P_2 \cong p_+^{1+2}$. Schließlich ist $[x, xa^{-1}] = 1 = [x,b]$ und

$$[yb, xa^{-1}] = ybxa^{-1}b^{-1}y^{-1}ax^{-1} = [b, a^{-1}][y,x] = a^{-p}x^p = 1$$

und $[xb, b] = 1$. Also ist $P = P_1 * P_2 \cong M_{p^3} * p_+^{1+2}$. Im Fall $p > 2$ kann es somit höchstens zwei extraspezielle Gruppen der Ordnung p^{2k+1} geben. Wegen $\exp(p_+^{1+2k}) = \exp(p_+^{1+2}) = p$ und $\exp(p_-^{1+2k}) = \exp(M_{p^3}) = p^2$ gibt es genau zwei Isomorphieklassen.

Im Folgenden können wir $p = 2$ annehmen. Sei $P := D_8 * D_8 = \langle x, y\rangle * \langle a, b\rangle$ mit $x^2 = a^2$. Dann ist $P_1 := \langle x, ya\rangle \cong Q_8$ und $P_2 := \langle a, bx\rangle \cong Q_8$. Wegen $[ya, bx] = [y,x][a,b] = x^2a^2 = 1$ ist $P \cong P_1 * P_2 \cong Q_8 * Q_8$. Es gibt also auch hier höchstens zwei extraspezielle Gruppen der Ordnung 2^{2k+1}. Nach Aufgabe 45 sind 2_-^{1+2k} und 2_+^{1+2k} nicht isomorph. □

10 Verallgemeinerte Fittinggruppe

Definition 10.1.

(i) $G \neq 1$ heißt *quasieinfach*, falls $G' = G$ und $G/\operatorname{Z}(G)$ einfach ist.

(ii) Eine Untergruppe $H \leq G$ heißt *subnormal*, falls eine Folge $H = H_0 \trianglelefteq H_1 \trianglelefteq \ldots \trianglelefteq H_k = G$ existiert. Wir schreiben $H \trianglelefteq\trianglelefteq G$. Subnormalität ist also der transitive Abschluss der Normalteilerrelation.

(iii) Eine *Komponente* von G ist eine subnormale quasieinfache Untergruppe von G.

Beispiel 10.2. Jede nichtabelsche einfache Gruppe ist quasieinfach.

Bemerkung 10.3. Für $H \trianglelefteq\trianglelefteq G$ muss die Folge $H \trianglelefteq \operatorname{N}_G(H) \trianglelefteq \operatorname{N}_G(\operatorname{N}_G(H)) \trianglelefteq \ldots$ nicht unbedingt bei G enden! Zum Beispiel ist $\langle (1,2)(3,4)\rangle \trianglelefteq \langle (1,3,2,4),(1,2)\rangle =: P \in \operatorname{Syl}_2(S_4)$, aber $P = \operatorname{N}_{S_4}(P)$. Andererseits ist $\langle (1,2)(3,4)\rangle \trianglelefteq V_4 \trianglelefteq S_4$.

Lemma 10.4. *Sei K eine Komponente von G. Dann gilt:*

(i) Ist $K \leq H \leq G$, so ist K eine Komponente von H.

(ii) Ist $N \triangleleft K$, so ist $N \leq \operatorname{Z}(K)$.

(iii) Ist $K \not\subseteq N \trianglelefteq G$, so ist KN/N eine Komponente von G/N.

Beweis. Nach Definition existiert eine Folge $K = K_0 \trianglelefteq \ldots \trianglelefteq K_n = G$. Dann ist $K = K_0 \cap H \trianglelefteq \ldots \trianglelefteq K_n \cap H = H$. Dies zeigt (i).

Sei nun $N \triangleleft K$. Dann ist $N \operatorname{Z}(K)/\operatorname{Z}(K) \trianglelefteq K/\operatorname{Z}(K)$. Da $K/\operatorname{Z}(K)$ einfach ist, gilt $N \leq \operatorname{Z}(K)$ oder $K = N\operatorname{Z}(K)$. Im zweiten Fall wäre $K = K' = (N\operatorname{Z}(K))' = N' \leq N$. Also folgt (ii).

Sei schließlich $K \not\subseteq N \trianglelefteq G$. Dann ist $N \cap K \triangleleft K$ und $N \cap K \leq \operatorname{Z}(K)$ nach (ii). Dies zeigt $(K/K \cap N)/(\operatorname{Z}(K)/K \cap N) \cong K/\operatorname{Z}(K)$. Wegen $\operatorname{Z}(K)/K \cap N \leq \operatorname{Z}(K/K \cap N) \trianglelefteq K/K \cap N$ folgt $\operatorname{Z}(K/K \cap N) = \operatorname{Z}(K)/K \cap N$. Insbesondere ist $(K/K \cap N)/\operatorname{Z}(K/K \cap N)$ einfach. Außerdem ist $(KN/N)' = K'N/N = KN/N$. Somit ist $KN/N \cong K/K \cap N$ quasieinfach. Schließlich ist $KN/N = K_0N/N \trianglelefteq \ldots \trianglelefteq K_nN/N = G/N$. Dies zeigt (iii). □

Lemma 10.5. *Sei K eine Komponente von G und $H \trianglelefteq\trianglelefteq G$. Dann ist $K \leq H$ oder $[K,H] = 1$.*

Beweis. Wir können $H < G$ annehmen. Sei also $H \leq N \triangleleft G$. Im Fall $G = K$ erhält man $H \leq N \leq \operatorname{Z}(G)$ aus Lemma 10.4. Dann gilt also $[K,H] = 1$. Wir können daher $K < G$ annehmen. Sei also $K \leq M \triangleleft G$. Dann ist $H_1 := [H,K] \leq [N,M] \leq N \cap M$ und $K \leq \operatorname{N}_M(H_1) =: G_1 < G$ nach Lemma 3.3. Nach Lemma 10.4 ist K eine Komponente von G_1 und $H_1 \trianglelefteq\trianglelefteq G_1$. Durch Induktion nach $|G|$ können wir $[K,H_1] = 1$ oder $K \leq H_1$ annehmen. Im ersten Fall ist $1 = [K,H,K] = [K,K,H]$. Aus Lemma 3.6 folgt $[H,K] = [H,K'] = [H,K,K] = 1$. Sei also $K \leq H_1 \leq N$. Dann ist K eine Komponente von N und $H \trianglelefteq\trianglelefteq N$. Per Induktion gilt die Behauptung für N und wir sind fertig. □

Satz 10.6. *Seien $K_1, \ldots, K_n$ die Komponenten von G. Dann ist*

$$\mathrm{E}(G) := \langle K_1, \ldots, K_n \rangle = K_1 * \ldots * K_n$$

und $[\mathrm{E}(G), \mathrm{F}(G)] = 1$.

Beweis. Aus Lemma 10.5 folgt $[K_i, K_j] = 1$ für $i \neq j$. Dies zeigt $\mathrm{E}(G) = K_1 * \ldots * K_n$. Da $\mathrm{F}(G)$ nilpotent ist, kann $\mathrm{F}(G)$ keine Komponente von G enthalten. Lemma 10.5 liefert also $[\mathrm{F}(G), K_i] = 1$ und $[\mathrm{F}(G), \mathrm{E}(G)] = 1$. □

Definition 10.7. Man nennt

$$\mathrm{F}^*(G) := \mathrm{F}(G)\,\mathrm{E}(G) = \mathrm{F}(G) * \mathrm{E}(G) \trianglelefteq G$$

die *verallgemeinerte Fittinggruppe* von G.

Bemerkung 10.8. Der nächste Satz verallgemeinert Satz 3.19.

Satz 10.9. *Es gilt* $\mathrm{C}_G(\mathrm{F}^*(G)) \leq \mathrm{F}^*(G)$.

Beweis. Sei $G \neq 1$. Wir zeigen zunächst $\mathrm{F}^*(G) \neq 1$. Sei dafür N ein minimaler Normalteiler von G. Ist N abelsch, so gilt $1 \neq N \leq \mathrm{F}(G) \leq \mathrm{F}^*(G)$. Sei nun N nichtabelsch. Nach Satz 2.26 ist $N = T_1 \oplus \ldots \oplus T_n$ mit einfachen Gruppen $T_1 \cong \ldots \cong T_n$. Da T_1 nichtabelsch ist, ist T_1 eine Komponente von G. Es folgt $1 \neq T_1 \leq \mathrm{E}(G) \leq \mathrm{F}^*(G)$.

Sei nun $C := \mathrm{C}_G(\mathrm{F}^*(G)) \trianglelefteq G$. Es genügt zu zeigen, dass C abelsch ist, denn dann hat man $C \leq \mathrm{F}(G) \leq \mathrm{F}^*(G)$. Nach dem eben Gezeigtem reicht es also $\mathrm{F}^*(C/\mathrm{Z}(C)) = 1$ zu beweisen. Sei $\mathrm{F}(C/\mathrm{Z}(C)) = N/\mathrm{Z}(C)$. Wegen $\mathrm{Z}(C) \leq \mathrm{Z}(N)$ ist dann $N \trianglelefteq C$ nilpotent und daher $N \leq \mathrm{F}(C)$. Nun ist $\mathrm{F}(C)$ charakteristisch in $C \trianglelefteq G$ und daher $\mathrm{F}(C) \trianglelefteq G$. Dies zeigt $N \leq \mathrm{F}(G) \cap C \leq \mathrm{Z}(C)$. Also ist $\mathrm{F}(C/\mathrm{Z}(C)) = 1$.

Sei schließlich $K/\mathrm{Z}(C)$ eine Komponente von $C/\mathrm{Z}(C)$. Dann ist

$$K/\mathrm{Z}(C) = (K/\mathrm{Z}(C))'' = K''\,\mathrm{Z}(C)/\mathrm{Z}(C)$$

und $K = K''\,\mathrm{Z}(C)$. Insbesondere ist $K/K'' \cong \mathrm{Z}(C)/\mathrm{Z}(C) \cap K''$ abelsch und $K' = K''$. Aus $K \trianglelefteq \trianglelefteq C$ folgt $K' \trianglelefteq \trianglelefteq C$. Um zu zeigen, dass $K'/\mathrm{Z}(K')$ einfach ist, nehmen wir $\mathrm{Z}(K') < N \trianglelefteq K'$ an. Dann ist $N\,\mathrm{Z}(C)/\mathrm{Z}(C) \trianglelefteq \trianglelefteq C/\mathrm{Z}(C)$ und Lemma 10.5 zeigt $K \leq N\,\mathrm{Z}(C)$ oder $[K, N] \leq \mathrm{Z}(C)$. Im ersten Fall ist $K' \leq (N\,\mathrm{Z}(C))' \leq N' \leq N \leq K'$. Im zweiten Fall ist $[K, K, N] = [K, N, K] = 1$ und Lemma 3.6 liefert den Widerspruch $[N, K'] = [N, K, K] = 1$. Also ist $K'/\mathrm{Z}(K')$ einfach und K' ist eine Komponente von $C \trianglelefteq G$. Dann ist K' auch eine Komponente von G und wir erhalten den Widerspruch $K' \leq \mathrm{F}^*(G) \cap C \leq \mathrm{Z}(C)$. Somit besitzt $C/\mathrm{Z}(C)$ keine Komponenten und $\mathrm{F}^*(C/\mathrm{Z}(C)) = 1$. □

11 Die Einfachheit von $\mathrm{PSL}(n,q)$

Bemerkung 11.1.

(i) Im Folgenden sei $n \in \mathbb{N}$ und q eine Primzahlpotenz.

(ii) Für $i,j \in \{1,\dots,n\}$ sei $e_{ij} = (m_{rs})_{r,s=1}^{n} \in \mathbb{F}_q^{n\times n}$ mit $m_{rs} = \delta_{ir}\delta_{js}$. Dann gilt $e_{ij}e_{kl} = \delta_{jk}e_{il}$.

Lemma 11.2. *Es gilt* $\mathrm{Z}(\mathrm{GL}(n,q)) = K^\times 1_n$ *und* $\mathrm{Z}(\mathrm{SL}(n,q)) = \mathrm{Z}(\mathrm{GL}(n,q)) \cap \mathrm{SL}(n,q)$.

Beweis. Offenbar ist $K^\times 1_n \subseteq \mathrm{Z}(\mathrm{GL}(n,q))$. Für beide Aussagen genügt es also $\mathrm{C}_{\mathrm{GL}(n,q)}(\mathrm{SL}(n,q)) \subseteq K^\times 1_n$ zu zeigen. Sei $A = (a_{ij}) \in \mathrm{C}_{\mathrm{GL}(n,q)}(\mathrm{SL}(n,q))$ und $i,j \in \{1,\dots,n\}$ mit $i \neq j$. Dann ist $1 + e_{ij} \in \mathrm{SL}(n,q)$ und $A(1+e_{ij}) = (1+e_{ij})A$. Es folgt

$$\begin{pmatrix} 0 & \cdots & 0 & a_{1i} & 0 & \cdot & 0 \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ 0 & \cdots & 0 & a_{ni} & 0 & \cdots & 0 \end{pmatrix} = Ae_{ij} = e_{ij}A = \begin{pmatrix} 0 & \cdots & 0 \\ \vdots & & \vdots \\ 0 & \cdots & 0 \\ a_{j1} & \cdots & a_{jn} \\ 0 & \cdots & 0 \\ \vdots & & \vdots \\ 0 & \cdots & \cdots \end{pmatrix}.$$

Dies zeigt $a_{ij} = 0$ für $i \neq j$ und $a_{ii} = a_{jj}$. □

Definition 11.3. Wie setzen

$$\mathrm{PGL}(n,q) := \mathrm{GL}(n,q)/\,\mathrm{Z}(\mathrm{GL}(n,q)),$$
$$\mathrm{PSL}(n,q) := \mathrm{SL}(n,q)/\,\mathrm{Z}(\mathrm{SL}(n,q)).$$

Satz 11.4.

$$|\mathrm{PGL}(n,q)| = \frac{|\mathrm{GL}(n,q)|}{q-1} = (q^n-1)(q^n-q)\dots(q^n-q^{n-2})q^{n-1},$$
$$|\mathrm{PSL}(n,q)| = \frac{|\mathrm{SL}(n,q)|}{\gcd(n,q-1)} = \frac{(q^n-1)(q^n-q)\dots(q^n-q^{n-2})q^{n-1}}{\gcd(n,q-1)}.$$

Beweis. Sei $A \in \mathrm{GL}(n,q)$. Dann ist die erste Zeile von A nicht der Nullvektor. Es gibt daher q^n-1 Möglichkeiten für die erste Zeile. Die zweite Zeile darf nicht linear abhängig zur ersten Zeile sein. Dies gibt $q^n - q$ Möglichkeiten für die zweite Zeile. Die dritte Zeile liegt nicht im Span der ersten beiden Zeilen. Es gibt also $q^n - q^2$ Möglichkeiten für die dritte Zeile usw. Umgekehrt liefert jede solche Wahl eine Matrix mit linear unabhängigen Zeilen, also eine invertierbare Matrix. Dies zeigt

$$|\mathrm{GL}(n,q)| = (q^n-1)\dots(q^n-q^{n-1}) = (q^n-1)\dots(q^n-q^{n-2})(q-1)q^{n-1}$$

und die erste Behauptung folgt aus Lemma 11.2.

Für die zweite Behauptung beobachten wir, dass der Homomorphismus $\det : \mathrm{GL}(n,q) \to \mathbb{F}_q^\times$ surjektiv ist. Daher ist $|\mathrm{SL}(n,q)| = \frac{|\mathrm{GL}(n,q)|}{q-1}$. Sei nun $\lambda 1_n \in K^\times 1_n \cap \mathrm{SL}(n,q) = \mathrm{Z}(\mathrm{SL}(n,q))$ mit $\lambda \in K^\times$. Dann ist $1 = \det(\lambda 1_n) = \lambda^n$ und $|\langle\lambda\rangle| \mid \mathrm{ggT}(n, q-1)$. Da $K^\times$ zyklisch ist (Algebra), gibt es genau eine Untergruppe $L \leq K^\times$ mit $L = \mathrm{ggT}(n, q-1)$ (Satz 2.4). Es gilt dann $\lambda \in L$. Umgekehrt erfüllt jedes Element $\gamma \in L$ die Bedingung $\gamma^n = 1$. Also ist $|\mathrm{Z}(\mathrm{SL}(n,q))| = |L| = \mathrm{ggT}(n, q-1)$. □

Beispiel 11.5.

(i) Offenbar ist $\mathrm{PGL}(1,q) = 1 = \mathrm{SL}(1,q)$.

(ii) Ist q eine 2-Potenz, so ist $\mathrm{PSL}(2,q) \cong \mathrm{SL}(2,q)$. Ist $q = 2$, so gilt auch $\mathrm{GL}(n,q) = \mathrm{SL}(n,q) \cong \mathrm{PSL}(n,q) \cong \mathrm{PGL}(n,q)$. Insbesondere ist $\mathrm{PSL}(2,2) \cong \mathrm{SL}(2,2) \cong \mathrm{GL}(2,2) \cong S_3$.

Lemma 11.6 („Iwasawas Lemma“)**.** *Sei $G \leq \mathrm{Sym}(\Omega)$ primitiv und perfekt. Existiert ein auflösbarer Normalteiler $A \trianglelefteq G_\omega$ ($\omega \in \Omega$) mit $\langle gAg^{-1} : g \in G\rangle = G$, so ist G einfach.*

Beweis. Sei $1 \neq N \trianglelefteq G$. Nach Satz 6.20 und Satz 1.21 ist $G = G_\omega N \leq \mathrm{N}_G(NA)$, d. h. $NA \trianglelefteq G$. Nach Voraussetzung ist $G = \langle gAg^{-1} : g \in G\rangle \leq NA$ und $G/N \cong A/A \cap N$ ist auflösbar. Im Fall $N < G$ erhält man den Widerspruch $G/N = G'/N = (G/N)' < G/N$. Also ist $N = G$ und G ist einfach. □

Lemma 11.7. *Für $n \geq 2$ operiert $\mathrm{PSL}(n,q)$ treu und primitiv auf der Menge Ω der 1-dimensionalen Untervektorräume von $\mathbb{F}_q^n$.*

Beweis. Offenbar operiert $\mathrm{SL}(n,q)$ auf Ω. Sei $A \in \mathrm{SL}(n,q)$ im Kern dieser Operation. Für den i-ten Einheitsvektor $e_i = (0,\ldots,0,1,0,\ldots,0)$ existiert dann ein $\lambda_i \in \mathbb{F}_q$ mit $Ae_i = \lambda_i e_i$. Also ist A eine Diagonalmatrix mit Diagonale $(\lambda_1,\ldots,\lambda_n)$. Wegen $\lambda_1 e_1 + \lambda_i e_i = A(e_1 + e_i) \in \mathbb{F}_q(e_1 + e_i)$ gilt sogar $\lambda_1 = \ldots = \lambda_n$. Umgekehrt operiert jede Matrix in $\mathrm{Z}(\mathrm{SL}(n,q))$ trivial auf Ω. Wir haben also gezeigt, dass $\mathrm{PSL}(n,q)$ treu auf Ω operiert.

Für die Primitivität genügt es zu zeigen, dass $\mathrm{PSL}(n,q)$ 2-transitiv auf Ω operiert. Seien also $v_1, v_2, w_1, w_2 \in \mathbb{F}_q^n \setminus \{0\}$ mit $\mathbb{F}_q v_1 \neq \mathbb{F}_q v_2$ und $\mathbb{F}_q w_1 \neq \mathbb{F}_q w_2$. Dann existiert ein $A \in \mathrm{GL}(n,q)$ mit $Av_1 = w_1$, $Av_2 = w_2$ und $Ax = x$ für $x \in \mathbb{F}_q^n \setminus \mathbb{F}_q\{v_1, v_2\}$. Sei $\lambda := \det(A)$ und $B \in \mathrm{GL}(n,q)$ mit $Bv_1 = w_1$, $Bv_2 = \lambda^{-1} w_2$ und $Bx = x$ für $x \in \mathbb{F}_q^n \setminus \mathbb{F}_q\{v_1, v_2\}$. Dann ist $B \in \mathrm{SL}(n,q)$ und das entsprechende Element $\overline{B} \in \mathrm{PSL}(n,q)$ bildet $(\mathbb{F}_q v_1, \mathbb{F}_q v_2)$ auf $(\mathbb{F}_q w_1, \mathbb{F}_q w_2)$ ab. □

Lemma 11.8. $\mathrm{SL}(n,q) = \langle 1_n + \lambda e_{ij} : \lambda \in \mathbb{F}_q,\ i \neq j\rangle$.

Beweis. Im Fall $n = 1$ ist $\mathrm{SL}(n,q) = 1$ und die Behauptung ist klar. Sei also $n \geq 2$. Es ist klar, dass die Matrizen $1_n + \lambda e_{ij}$ Determinante 1 haben. Sei umgekehrt $A \in \mathrm{SL}(n,q)$ beliebig. Durch die Multiplikation $A(1_n + \lambda e_{ij})$ wird das λ-fache der i-ten Spalte von A zur j-ten Spalte addiert. Analog bewirkt die Multiplikation $(1_n + \lambda e_{ij})A$ die Addition des λ-fachen der j-ten Zeile zur i-ten Zeile. Dies sind die elementaren Operation im Gauß-Algorithmus. Wegen $\det(A) = 1$ existiert ein $i \in \{1,\ldots,n\}$ mit $a_{1i} \neq 0$. Nach einer Spaltenoperation dürfen wir $i > 1$ annehmen. Ersetzt man A durch $A(1_n + (1 - a_{11})a_{1i}^{-1} e_{i1})$, so ist $a_{11} = 1$. Nach weiteren Spaltenoperationen dürfen wir $a_{1j} = 0$ für $j > 1$ annehmen. Analog erhält man durch Zeilenoperationen $a_{j1} = 0$ für $j > 1$. Im Fall $n = 2$ ist dann bereits $A = 1_2$ wegen $\det(A) = 1$. Sei also $n \geq 3$ und $A' := (a_{ij})_{i,j=2}^n$. Dann gilt $A' \in \mathrm{SL}(n-1,q)$. Durch Induktion nach n kann man also A' mittels Zeilen- und Spaltenoperationen in die Einheitsmatrix umwandeln. Diese Operationen funktionieren auch für A und verändern die erste Zeile und Spalte nicht. Insgesamt hat man also Matrizen $P, Q \in \langle 1_n + \lambda e_{ij} : \lambda \in \mathbb{F}_q,\ i \neq j\rangle$ mit $PAQ = 1_n$. Die Behauptung folgt. □

Lemma 11.9. *Für $n \geq 2$ und $(n,q) \notin \{(2,2),(2,3)\}$ ist $\mathrm{SL}(n,q)$ perfekt.*

Beweis. Nach Lemma 11.8 genügt es zu zeigen, dass die Matrizen $1_n + \lambda e_{ij}$ Kommutatoren sind. Es gilt $(1_n + \lambda e_{ij})(1_n - \lambda e_{ij}) = 1_n + \lambda e_{ij} - \lambda e_{ij} - \lambda^2 e_{ij}^2 = 1_n$ und $(1_n + \lambda e_{ij})^{-1} = (1_n - \lambda e_{ij})$. Sei zunächst $n \geq 3$, $\lambda \in \mathbb{F}_q$ und $i,j,k \in \{1,\dots,n\}$ paarweise verschieden. Dann ist

$$\begin{aligned}[1_n + \lambda e_{ik}, 1_n + e_{kj}] &= (1_n + \lambda e_{ik})(1_n + e_{kj})(1_n - \lambda e_{ik})(1_n - e_{kj}) \\ &= 1_n + \lambda(e_{ik} - e_{ik}) + e_{kj} - e_{kj} + \lambda(e_{ik}e_{kj} + e_{ik}e_{kj} - e_{ik}e_{kj}) = 1_n + \lambda e_{ij}.\end{aligned}$$

Sei nun $n = 2$ und $q > 3$. Sei $\alpha, \beta \in \mathbb{F}_q^\times$ und

$$A := \begin{pmatrix} \alpha & 0 \\ 0 & \alpha^{-1} \end{pmatrix} \in \mathrm{SL}(2,q) \qquad\qquad B := 1_2 + \beta e_{12} \in \mathrm{SL}(2,q).$$

Dann ist

$$\begin{aligned}[A,B] &= \begin{pmatrix} \alpha & 0 \\ 0 & \alpha^{-1} \end{pmatrix} \begin{pmatrix} 1 & \beta \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \alpha^{-1} & 0 \\ 0 & \alpha \end{pmatrix} \begin{pmatrix} 1 & -\beta \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} \alpha & \alpha\beta \\ 0 & \alpha^{-1} \end{pmatrix} \begin{pmatrix} \alpha^{-1} & -\alpha^{-1}\beta \\ 0 & \alpha \end{pmatrix} \\ &= \begin{pmatrix} 1 & \beta(\alpha^2 - 1) \\ 0 & 1 \end{pmatrix} = 1_2 + \beta(\alpha^2 - 1)e_{12}.\end{aligned}$$

Wegen $q > 3$ können wir α so wählen, dass $\alpha^2 \neq 1$ gilt. Mit $\beta := \lambda(\alpha^2 - 1)^{-1}$ ist dann $[A,B] = 1_2 + \lambda e_{12}$ und $[(B^{-1})^{\mathrm{T}}, (A^{-1})^{\mathrm{T}}] = [A,B]^{\mathrm{T}} = 1_2 + \lambda e_{21}$. Dies zeigt die Behauptung. □

Beispiel 11.10. Wegen $|\mathrm{SL}(2,2)| = 6$ und $|\mathrm{SL}(2,3)| = 24$ sind $\mathrm{SL}(2,2)$ und $\mathrm{SL}(2,3)$ nicht perfekt.

Satz 11.11. *Für $n \geq 2$ und $(n,q) \notin \{(2,2),(2,3)\}$ ist $\mathrm{PSL}(n,q)$ einfach.*

Beweis. Wir benutzen Iwasawas Lemma. Sei $G := \mathrm{SL}(n,q)$, $Z := \mathrm{Z}(G)$ und $\overline{H} := HZ/Z$ für $H \leq G$. Nach Lemma 11.7 ist $\overline{G}$ eine primitive Permutationsgruppe. Nach Lemma 11.9 ist $\overline{G}' = \overline{G'} = \overline{G}$, d. h. $\overline{G}$ ist perfekt. Wie üblich operiert G auf $\mathbb{F}_q^n$. Sei $H \leq G$ der Stabilisator von $e_1 := (1,0,\dots,0)$. Dann ist $\overline{H}$ der Stabilisator von $U := \mathbb{F}_q e_1$ in $\overline{G}$. Sei

$$A := \left\{ \begin{pmatrix} 1 & * & \cdots & * \\ 0 & 1 & 0 & 0 \\ & & & \\ 0 & 0 & \ddots & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \right\} = \{1_n + \sum_{i=2}^{n} \lambda_i e_{1i} : \lambda_i \in \mathbb{F}_q\} \subseteq H.$$

Wegen $(1_n + \sum_{i=2}^n \lambda_i e_{1i})(1_n + \sum_{i=2}^n \gamma_i e_{1i}) = 1_n + \sum_{i=2}^n (\lambda_i + \gamma_i) e_{1i} \in A$ ist A eine abelsche Untergruppe von H. Für $v, w \in \mathbb{F}_q^n$ mit $v + U = w + U$ und $h \in H$ gilt $h(v - w) \in hU = U$ und daher $hv + U = hw + U$. Also operiert H auf $\mathbb{F}_q^n / U$. Der Kern dieser Operation ist A. Dies zeigt $A \trianglelefteq H$. Sicher ist dann auch $\overline{A}$ ein abelscher Normalteiler von $\overline{H}$. Es verbleibt zu zeigen, dass $\overline{G} = \langle \overline{gAg^{-1}} : g \in G \rangle$ gilt. Nach Lemma 11.8 genügt es $1_n + \lambda e_{ij} \in \bigcup_{g \in G} gAg^{-1}$ zu zeigen ($\lambda \in \mathbb{F}_q$, $i \neq j$). Nach Definition gilt bereits $1_n + \lambda e_{1j} \in A$. Sei $j \neq i \geq 2$ und sei $g_i = (m_{kl})_{k,l=1}^n \in G$ mit

$$m_{kl} = \begin{cases} -1 & \text{falls } (k,l) = (1,i), \\ 1 & \text{falls } k = l \notin \{1,i\} \text{ oder } (k,l) = (i,1), \\ 0 & \text{sonst.} \end{cases}$$

Dann ist $g_i^{-1} = 2 \cdot 1_n - g_i$ und $g_i(1_n + \lambda e_{1j}) g_i^{-1} = 1_n + \lambda g_i e_{1j} = 1_n + \lambda e_{ij}$. Die Behauptung folgt. □

Bemerkung 11.12.

(i) Nach Satz 11.4 ist $|\mathrm{PSL}(2,4)| = |\mathrm{PSL}(2,5)| = 60$. Aus Satz 6.32 folgt daher $\mathrm{PSL}(2,4) \cong \mathrm{PSL}(2,5) \cong A_5$. Man kann weiter $\mathrm{PSL}(2,7) \cong \mathrm{PSL}(3,2)$, $\mathrm{PSL}(2,9) \cong A_6$ und $\mathrm{PSL}(4,2) \cong A_8$ zeigen.

(ii) Die kleinste einfache Gruppe, die nicht zu C_p, A_n oder $\mathrm{PSL}(n,q)$ isomorph ist, ist $\mathrm{PSU}(3,3)$ der Ordnung 6048.

(iii) Die Gruppen $\mathrm{SL}(n,q)$ mit $n \geq 2$ und $(n,q) \notin \{(2,2),(2,3)\}$ sind quasieinfach.

12 Schur-Multiplikatoren

Definition 12.1. Eine *Schur-Erweiterung* einer endlichen Gruppe G ist eine Gruppe $\widehat{G}$, sodass ein $Z \leq \mathrm{Z}(\widehat{G}) \cap \widehat{G}'$ mit $\widehat{G}/Z \cong G$ existiert.

Beispiel 12.2.

(i) D_8 und Q_8 sind Schur-Erweiterungen von C_2^2.

(ii) Nach Lemma 11.9 und Bemerkung 11.12 ist $\mathrm{SL}(2,5)$ eine Schur-Erweiterung von A_5.

(iii) Sei $\widehat{G}$ eine Schur-Erweiterung einer zyklischen Gruppe $G \cong \widehat{G}/Z$. Dann ist $\widehat{G}/\mathrm{Z}(\widehat{G}) \cong (\widehat{G}/Z)/(\mathrm{Z}(\widehat{G})/Z)$ zyklisch und $\widehat{G}$ ist abelsch (Aufgabe 4(a)). Dies zeigt $Z \leq \widehat{G}' = 1$ und $\widehat{G} \cong G$.

Bemerkung 12.3. Wir studieren in diesem Kapitel Existenz und Eindeutigkeit von Schur-Erweiterungen.

Satz 12.4. *Jede Schur-Erweiterung einer endlichen Gruppe ist endlich.*

Beweis. Sei $\widehat{G}$ eine Schur-Erweiterung der endlichen Gruppe $G \cong \widehat{G}/Z$. Sei $n := |G|$. Wegen $Z \leq \widehat{G}'$ genügt es zu zeigen, dass $\widehat{G}'$ endlich ist. Sei R ein Repräsentantensystem für $\widehat{G}/Z$ und $\Gamma := \{[r,s] : r,s \in R\}$. Dann ist $|\Gamma| \leq |R|^2 = |\widehat{G}/Z|^2 = n^2$. Für $r,s \in R$ und $z \in Z \leq \mathrm{Z}(\widehat{G})$ gilt $[rz,s] = [r,s] = [r,sz]$. Jedes Element $g \in \widehat{G}'$ hat also die Form $g = c_1 \dots c_m$ mit $c_1, \dots, c_m \in \Gamma$. Es genügt zu zeigen, dass man dabei $m \leq n^3$ wählen kann (dann folgt $|\widehat{G}'| \leq n^{2n^3} < \infty$). Sei $g = c_1 \dots c_m$ eine solche Darstellung mit minimalem m. Nehmen wir $m > n^3$ an. Dann existiert ein $\gamma \in \Gamma$ mit $|\{i \in \{1,\dots,m\} : c_i = \gamma\}| > n$. Wegen $c_i c_{i+1} = c_{i+1}(c_{i+1}^{-1} c_i c_{i+1}) = c_{i+1}\delta$ mit $\delta \in \Gamma$ können wir $c_1 = \dots = c_{n+1} = \gamma$ annehmen. Im Widerspruch zur Minimalität von m werden wir zeigen, dass γ^{n+1} ein Produkt von n Kommutatoren ist. Sei dafür $\gamma = [r,s]$ mit $r,s \in R$. Wegen $\gamma^n = \gamma^{|G|} \in Z \leq \mathrm{Z}(\widehat{G})$ ist

$$\gamma^{n+1} = \gamma\gamma^n = \gamma s \gamma^n s^{-1} = \gamma s \gamma s^{-1} (s\gamma s^{-1})^{n-1} = [r,s]s[r,s]s^{-1}[srs^{-1},s]^{n-1} = [r,s^2][srs^{-1},s]^{n-1}. \quad \square$$

Definition 12.5. Sei G eine endliche Gruppe und A eine (möglicherweise unendliche) abelsche Gruppe. Die Menge $C^1(G,A)$ aller Abbildungen der Form $G \to A$ wird durch $(\alpha\beta)(g) := \alpha(g)\beta(g)$ für $\alpha, \beta \in C^1(G,A)$ und $g \in G$ zu einer abelschen Gruppe (es gilt $C^1(G,A) \cong A^{|G|}$). Sei $C^2(G,A) := C^1(G \times G, A)$ und

$$Z^2(G,A) := \{\alpha \in C^2(G,A) : \alpha(x,y)\alpha(xy,z) = \alpha(y,z)\alpha(x,yz)\ \forall x,y,z \in G\}.$$

Offenbar ist dann $Z^2(G,A)$ eine Untergruppe von $C^2(G,A)$. Man nennt die Elemente in $Z^2(G,A)$ *Faktorensysteme* (oder (2-)*Kozyklen*) von G nach A.

Lemma 12.6. *Die Abbildung $\partial : C^1(G,A) \to Z^2(G,A)$ mit $\partial\alpha(x,y) := \alpha(x)\alpha(y)\alpha(xy)^{-1}$ für $\alpha \in C^1(G,A)$ und $x,y \in G$ ist ein Homomorphismus.*

Beweis. Offenbar ist $\partial\alpha \in C^2(G,A)$ für $\alpha \in C^1(G,A)$. Für $x,y,z \in G$ gilt

$$\begin{aligned}\partial\alpha(x,y)\partial\alpha(xy,z) &= \alpha(x)\alpha(y)\alpha(xy)^{-1}\alpha(xy)\alpha(z)\alpha(xyz)^{-1} = \alpha(x)\alpha(y)\alpha(z)\alpha(xyz)^{-1}\\ &= \alpha(y)\alpha(z)\alpha(yz)^{-1}\alpha(x)\alpha(yz)\alpha(xyz)^{-1} = \partial\alpha(y,z)\partial\alpha(x,yz).\end{aligned}$$

Dies zeigt $\partial\alpha \in Z^2(G,A)$. Für $\alpha,\beta \in C^1(G,A)$ und $x,y \in G$ gilt schließlich

$$\partial(\alpha\beta)(x,y) = (\alpha\beta)(x)(\alpha\beta)(y)(\alpha\beta)(xy)^{-1} = \alpha(x)\alpha(y)\alpha(xy)^{-1}\beta(x)\beta(y)\beta(xy)^{-1} = \partial\alpha(x,y)\partial\beta(x,y).$$

Also ist ∂ ein Homomorphismus. □

Definition 12.7. Sei $B^2(G,A) := \partial(C^1(G,A)) \trianglelefteq Z^2(G,A)$ und $H^2(G,A) := Z^2(G,A)/B^2(G,A)$. Man nennt $H^2(G,A)$ die *zweite Kohomologiegruppe* von G nach A.

Lemma 12.8. *Für $\overline{\alpha} \in H^2(G,A)$ existiert ein $\alpha \in Z^2(G,A)$ mit $\alpha B^2(G,A) = \overline{\alpha}$ und $\alpha(1,x) = \alpha(x,1) = 1$ für $x \in G$.*

Beweis. Sei zunächst $\beta \in Z^2(G,A)$ mit $\beta B^2(G,A) = \overline{\alpha}$ beliebig. Nach Definition von $Z^2(G,A)$ ist $\beta(x,1)\beta(x,1) = \beta(1,1)\beta(x,1)$ und $\beta(x,1) = \beta(1,1)$ für $x \in G$. Analog ist $\beta(1,x) = \beta(1,1)$. Sei $\gamma(x) := \beta(1,1)^{-1}$ für $x \in G$ und $\alpha := \beta\partial\gamma \in Z^2(G,A)$. Dann ist $\alpha B^2(G,A) = \overline{\alpha}$ und $\alpha(x,1) = \beta(x,1)\gamma(x)\gamma(1)\gamma(x)^{-1} = 1$ für $x \in G$. Sicher ist auch $\alpha(1,x) = 1$. □

Definition 12.9. Man nennt $M(G) := H^2(G,\mathbb{C}^\times)$ den *Schur-Multiplikator* von G.

Satz 12.10. *$M(G)$ ist eine endliche abelsche Gruppe mit* $\exp(M(G)) \mid |G|$.

Beweis. Sicher ist $M(G)$ abelsch. Sei $n := |G|$ und sei $\beta \in Z^2(G,\mathbb{C}^\times)$ beliebig. Da $\mathbb{C}$ algebraisch abgeschlossen ist, existieren $\gamma(x) \in \mathbb{C}^\times$ mit $\gamma(x)^n = \prod_{y\in G}\beta(y,x)^{-1}$ für $x \in G$. Es gilt dann

$$\gamma(y)^{-n}\gamma(z)^{-n} = \prod_{x\in G}\beta(x,y)\prod_{x\in G}\beta(x,z) = \prod_{x\in G}\beta(x,y)\beta(xy,z) = \prod_{x\in G}\beta(y,z)\beta(x,yz) = \beta(y,z)^n\gamma(yz)^{-n}$$

für $y,z \in G$. Sei $\alpha := \beta\partial\gamma \in Z^2(G,\mathbb{C}^\times)$. Dann ist $\overline{\alpha} := \alpha B^2(G,\mathbb{C}^\times) = \beta B^2(G,\mathbb{C}^\times) \in M(G)$ und

$$\alpha(y,z)^n = \beta(y,z)^n\gamma(y)^n\gamma(z)^n\gamma(yz)^{-n} = 1$$

für alle $y,z \in G$. Insbesondere gibt es nur endlich viele Möglichkeiten für α und es folgt $|M(G)| < \infty$. Außerdem ist $\overline{\alpha}^n = \overline{\alpha^n} = 1$. □

Lemma 12.11. *Für $\alpha \in Z^2(G,A)$ induziert die Abbildung* $\mathrm{Hom}(A,\mathbb{C}^\times) \to C^2(G,\mathbb{C}^\times)$, $\lambda \mapsto \lambda\circ\alpha$ *einen Homomorphismus $\Psi_\alpha : \mathrm{Hom}(A,\mathbb{C}^\times) \to M(G)$.*

Beweis. Für $\lambda \in \mathrm{Hom}(A,\mathbb{C}^\times)$ und $x,y,z \in G$ ist

$$(\lambda\circ\alpha)(x,y)(\lambda\circ\alpha)(xy,z) = \lambda(\alpha(x,y)\alpha(xy,z)) = \lambda(\alpha(y,z)\alpha(x,yz)) = (\lambda\circ\alpha)(y,z)(\lambda\circ\alpha)(x,yz)$$

und $\lambda\circ\alpha \in Z^2(G,\mathbb{C}^\times)$. Für $\lambda,\mu \in \mathrm{Hom}(A,\mathbb{C}^\times)$ ist $(\lambda\mu)\circ\alpha = (\lambda\circ\alpha)(\mu\circ\alpha)$. Also ist Ψ_α tatsächlich ein Homomorphismus. □

Lemma 12.12. *Für eine endliche abelsche Gruppe A ist* $\mathrm{Hom}(A,\mathbb{C}^\times) \cong A$.

Beweis. Sei $A = \langle a_1\rangle \oplus \ldots \oplus \langle a_n\rangle$ und $d_i := |\langle a_i\rangle|$ für $i = 1, \ldots, n$. Sei $\zeta_i \in \mathbb{C}$ eine primitive d_i-te Einheitswurzel. Für jedes $\lambda \in \mathrm{Hom}(A, \mathbb{C}^\times)$ gilt dann $\lambda(a_i) \in \langle \zeta_i\rangle$. Wir definieren $F : A \to \mathrm{Hom}(A, \mathbb{C}^\times)$ mit $F(a_1^{k_1} \ldots a_n^{k_n})(a_i) := \zeta_i^{k_i}$ für $i = 1, \ldots, n$. Man zeigt leicht, dass F ein wohldefinierter Isomorphismus ist. □

Satz 12.13 (Schur). *Sei $\widehat{G}$ eine Schur-Erweiterung von G mit $\widehat{G}/Z \cong G$. Dann ist Z zu einer Untergruppe von $M(G)$ isomorph. Insbesondere besitzt G nur endlich viele Schur-Erweiterungen.*

Beweis. Für $x \in G$ wählen wir ein Urbild $\widehat{x} \in \widehat{G}$ unter dem kanonischen Epimorphismus $\widehat{G} \to \widehat{G}/Z \cong G$. Dabei sei $\widehat{1} = 1$. Sei $\alpha(x, y) := \widehat{x}\widehat{y}\widehat{xy}^{-1} \in Z$ für $x, y \in G$. Für $x, y, z \in G$ gilt dann

$$\alpha(x,y)\alpha(xy,z)\widehat{xyz} = \alpha(x,y)\widehat{xy}\widehat{z} = \widehat{x}\widehat{y}\widehat{z} = \alpha(y,z)\widehat{xyz} = \alpha(y,z)\alpha(x,yz)\widehat{xyz}.$$

Dies zeigt $\alpha \in Z^2(G, Z)$. Nach Satz 12.4 und Lemma 12.12 genügt es zu zeigen, dass die Abbildung Ψ_α aus Lemma 12.11 injektiv ist. Sei also $\lambda \in \mathrm{Hom}(Z, \mathbb{C}^\times)$ mit $\lambda \circ \alpha = \partial\gamma$ für ein $\gamma \in C^1(G, \mathbb{C}^\times)$. Dann ist $1 = \lambda(1) = \lambda(\alpha(1, 1)) = \partial\gamma(1) = \gamma(1)$. Sei $\widehat{\lambda} : \widehat{G} \to \mathbb{C}^\times$ mit $\widehat{\lambda}(\widehat{x}a) := \gamma(x)\lambda(a)$ für $x \in G$ und $a \in Z$. Wegen $\gamma(1) = 1$ ist $\widehat{\lambda}$ eine Fortsetzung von λ. Für $x, y \in G$ und $a, b \in Z$ gilt

$$\begin{aligned}\widehat{\lambda}(\widehat{x}a \cdot \widehat{y}b) &= \widehat{\lambda}(\widehat{xy}\alpha(x,y)ab) = \gamma(xy)\lambda(\alpha(x,y))\lambda(a)\lambda(b) = \gamma(xy)\gamma(x)\gamma(y)\gamma(xy)^{-1}\lambda(a)\lambda(b)\\ &= \gamma(x)\lambda(a)\gamma(y)\lambda(b) = \widehat{\lambda}(\widehat{x}a)\widehat{\lambda}(\widehat{y}b).\end{aligned}$$

Also ist $\widehat{\lambda}$ ein Homomorphismus mit $\widehat{G}/\operatorname{Ker}(\widehat{\lambda}) \leq \mathbb{C}^\times$. Es folgt $Z \leq \widehat{G}' \leq \operatorname{Ker}(\widehat{\lambda})$. Dies zeigt $\lambda = 1$ und wir sind fertig. □

Satz 12.14 (Schur). *Es existiert eine Schur-Erweiterung $\widehat{G}$ mit $M(G) \leq \mathrm{Z}(\widehat{G}) \cap \widehat{G}'$ und $\widehat{G}/M(G) \cong G$.*

Beweis. Nach Satz 12.10 ist $M(G) = \langle\overline{\alpha}_1\rangle \oplus \ldots \oplus \langle\overline{\alpha_n}\rangle$. Sei $d_i := |\langle\overline{\alpha_i}\rangle|$ und $A_i \leq \mathbb{C}^\times$ mit $|A_i| = d_i$ für $i = 1, \ldots, n$. Sei $\alpha_i \in Z^2(G, \mathbb{C}^\times)$ mit $\alpha_i B^2(G, \mathbb{C}^\times) = \overline{\alpha_i}$. Dann ist $\alpha_i^{d_i} = \partial\gamma_i$ für ein $\gamma_i \in C^1(G, \mathbb{C}^\times)$. Sei $\delta_i(x) \in \mathbb{C}^\times$ mit $\delta_i(x)^{d_i} = \gamma_i(x)^{-1}$ für $x \in G$. Nachdem wir α_i durch $\alpha_i\partial\delta_i$ ersetzt haben, gilt $\alpha_i^{d_i} = 1$ für $i = 1, \ldots, n$. Insbesondere ist $\alpha_i \in Z^2(G, A_i)$ für $i = 1, \ldots, n$. Nach Lemma 12.8 dürfen wir auch $\alpha_i(x, 1) = \alpha_i(1, x) = 1$ für $x \in G$ annehmen. Sei $A := A_1 \times \ldots \times A_n \cong M(G)$ und $\alpha \in C^2(G, A)$ mit $\alpha(x, y) = (\alpha_1(x, y), \ldots, \alpha_n(x, y))$ für $x, y \in G$. Offenbar ist dann $\alpha \in Z^2(G, A)$ mit $\alpha(1, x) = \alpha(x, 1) = 1$ für $x \in G$.

Wir definieren eine neue Verknüpfung auf $\widehat{G} := G \times A$ via

$$(x, a) \cdot (y, b) := (xy, \alpha(x, y)ab) \qquad (x, y \in G,\ a, b \in A).$$

Für $x, y, z \in G$ und $a, b, c \in A$ ist dann

$$\begin{aligned}((x,a)\cdot(y,b))\cdot(z,c) &= (xy,\alpha(x,y)ab)\cdot(z,c) = (xyz,\alpha(xy,z)\alpha(x,y)abc) = (xyz,\alpha(x,yz)\alpha(y,z)abc)\\ &= (x,a)\cdot(yz,\alpha(y,z)bc) = (x,a)\cdot((y,b)\cdot(z,c)).\end{aligned}$$

Die Verknüpfung ist also assoziativ. Wegen $(1_G, 1_A) \cdot (x, a) = (x, \alpha(1, x)a) = (x, a)$ ist $(1_G, 1_A)$ ein neutrales Element. Schließlich ist $(x^{-1}, \alpha(x^{-1}, x)^{-1}a^{-1}) \cdot (x, a) = (1_G, 1_A)$. Also ist $\widehat{G}$ eine endliche Gruppe. Wir identifizieren G mit $\{(g, 1_A) : g \in G\}$ und A mit $\{(1_G, a) : a \in A\}$. Offenbar ist dann A eine Untergruppe von $\widehat{G}$. Außerdem ist die Abbildung $\widehat{G} \to G$, $(x, a) \mapsto x$ ein Homomorphismus mit Kern A. Dies zeigt $A \trianglelefteq \widehat{G}$ und $\widehat{G}/A \cong G$. Für $(x, a) \in \widehat{G}$ und $b \in A$ gilt $(x, a) \cdot b = (x, ab) = (x, ba) = b \cdot (x, a)$. Es folgt $A \leq \mathrm{Z}(\widehat{G})$. Es verbleibt $A \leq \widehat{G}'$ zu zeigen.

Sei $\pi_i : A \to A_i \leq \mathbb{C}^\times$ die i-te Projektion. Mit der Abbildung Ψ_α aus Lemma 12.11 gilt dann $\Psi_\alpha(\pi_i) = \overline{\alpha_i}$ für $i = 1, \ldots, n$. Wegen $M(G) = \langle \overline{\alpha_1}, \ldots, \overline{\alpha_n} \rangle$ ist Ψ_α surjektiv. Nach Lemma 12.12 ist $\mathrm{Hom}(A, \mathbb{C}^\times) \cong A \cong M(G)$. Daher ist Ψ_α auch injektiv. Nach Satz 2.10 (angewendet auf $\widehat{G}/\widehat{G}'$) existieren Normalteiler $N_1, \ldots, N_s \trianglelefteq \widehat{G}$ mit $\widehat{G}' = N_1 \cap \ldots \cap N_s$, sodass $\widehat{G}/N_i$ zyklisch ist für $i = 1, \ldots, s$. Nehmen wir $A \not\leq \widehat{G}'$ an. Dann existiert ein i mit $A \not\leq N_i$. Indem man G/N_i in $\mathbb{C}^\times$ einbettet, erhält man einen Homomorphismus $\varphi : \widehat{G} \to \mathbb{C}^\times$ mit $\varphi(A) \neq 1$. Die Einschränkung φ_A ist also ein nicht-triviales Element in $\mathrm{Hom}(A, \mathbb{C}^\times)$. Sei $\Psi_\alpha(\varphi_A) = \beta B^2(G, \mathbb{C}^\times)$. Für $x, y \in G$ gilt dann

$$\beta(x,y) = \varphi(\alpha(x,y)) = \varphi(x \cdot y \cdot (xy)^{-1}) = \varphi(x)\varphi(y)\varphi(xy)^{-1} = \partial\varphi(x,y).$$

Dies liefert den Widerspruch $\Psi_\alpha(\varphi_A) = 1$. Also ist $A \leq \widehat{G}'$ und $\widehat{G}$ ist eine Schur-Erweiterung von G. □

Bemerkung 12.15. Wir verbessern nun die Aussage $\exp(M(G)) \,\big|\, |G|$ aus Satz 12.10.

Satz 12.16. *Für $H \leq G$ existiert ein Homomorphismus $F : M(G) \to M(H)$ mit $\overline{\alpha}^{|G:H|} = 1$ für $\overline{\alpha} \in \mathrm{Ker}(F)$.*

Beweis. Sei $\alpha \in Z^2(G, \mathbb{C}^\times)$. Dann liegt die Einschränkung α_H sicher in $Z^2(H, \mathbb{C}^\times)$. Im Fall $\alpha \in B^2(G, \mathbb{C}^\times)$ ist auch $\alpha_H \in B^2(H, \mathbb{C}^\times)$. Dies induziert einen wohldefinierten Homomorphismus $F : M(G) \to M(H)$. Sei $\alpha B^2(G, \mathbb{C}^\times) \in \mathrm{Ker}(F)$, d. h. $\alpha_H = \partial\gamma$ für ein $\gamma \in C^1(H, \mathbb{C}^\times)$. Sei $\widetilde{\gamma} \in C^1(G, \mathbb{C}^\times)$ eine beliebige Fortsetzung von γ. Indem wir α durch $\alpha\partial\widetilde{\gamma}^{-1}$ ersetzen, können wir $\alpha_H = 1$ annehmen. Sei R ein Repräsentantensystem für G/H. Für $x \in G$ sei $r_x \in R$ und $h_x \in H$ mit $x = r_x h_x$. Sei $\gamma(x) := \alpha(r_x, h_x)$ für $x \in G$ und $\beta := \alpha\partial\gamma$. Für $x \in G$ und $h \in H$ gilt dann

$$\begin{aligned}\beta(x,h) &= \alpha(x,h)\gamma(x)\gamma(h)\gamma(xh)^{-1} = \alpha(x,h)\alpha(r_x,h_x)\alpha(r_x,h_xh)^{-1} \\ &= \alpha(x,h)\alpha(r_x,h_x)\alpha(r_x,h_x)^{-1}\alpha(r_xh_x,h)^{-1}\alpha(h_x,h) = 1.\end{aligned}$$

Sei nun $x, y \in G$. Dann ist $\beta(x,y) = \beta(x, r_y h_y) = \beta(x,r_y)\beta(xr_y, h_y)\beta(r_y,h_y)^{-1} = \beta(x,r_y)$. Sei schließlich $\delta(x) := \prod_{r\in R} \beta(x,r)$ für $x \in G$. Für $x, y \in G$ ist dann

$$\beta(x,y)^{|G:H|}\delta(xy) = \prod_{r\in R} \beta(x,y)\beta(xy,r) = \prod_{r\in R} \beta(y,r)\beta(x,yr) = \delta(y)\prod_{r\in R}\beta(x,r_{yr}) = \delta(x)\delta(y).$$

Dies zeigt $\beta^{|G:H|} = \partial\delta \in B^2(G, \mathbb{C}^\times)$. Somit ist auch $\alpha^{|G:H|} \in B^2(G, \mathbb{C}^\times)$. □

Satz 12.17. *Sind alle Sylowgruppen von G zyklisch, so gilt $M(G) = 1$ (vgl. Satz 7.24).*

Beweis. Sei $P \in \mathrm{Syl}_p(G)$. Nach Beispiel 12.2 besitzt P keine echte Schur-Erweiterung. Nach Satz 12.14 ist daher $M(P) = 1$. Satz 12.16 gilt $\overline{\alpha}^{|G:P|} = 1$ für alle $\overline{\alpha} \in M(G)$. Da p beliebig ist, folgt $M(G) = 1$. □

Satz 12.18. *Sei $\widehat{G}$ eine Schur-Erweiterung einer perfekten Gruppe G mit $|\widehat{G}| = |G||M(G)|$ (existiert nach Satz 12.14). Jede weitere Schur-Erweiterung von G ist dann zu einer Faktorgruppe von $\widehat{G}$ isomorph. Insbesondere ist $\widehat{G}$ bis auf Isomorphie die einzige Schur-Erweiterung von G mit maximaler Ordnung.*

Beweis. Sei X ein Erzeugendensystem von G und sei F die freie Gruppe über dem Alphabet X. Nach Satz 8.7 existiert ein $N \trianglelefteq F$ mit $G \cong F/N$. Wir definieren $\widehat{G} := F'/[F,N]$ und $Z := (F' \cap N)/[F,N] \leq \mathrm{Z}(\widehat{G})$. Wegen $F/N \cong G \cong G' \cong F'N/N$ ist $F = F'N$ und $\widehat{G} = (F'N)'/[F,N] = F''/[F,N] = \widehat{G}'$. Also gilt auch $Z \leq \widehat{G}'$ und $\widehat{G}/Z \cong F'/F' \cap N \cong F'N/N = F/N \cong G$. Somit ist $\widehat{G}$ eine Schur-Erweiterung von G.

Sei nun $\widetilde{G}$ eine weitere Schur-Erweiterung von G mit $\widetilde{G}/W \cong G$. Sei $\widetilde{x} \in \widetilde{G}$ ein Urbild von $x \in X$. Nach Satz 4.13 und Lemma 4.12 gilt

$$\widetilde{G} = \langle \widetilde{x} : x \in X \rangle W = \langle \widetilde{x} : x \in X \rangle (\mathrm{Z}(\widetilde{G}) \cap \widetilde{G}') = \langle \widetilde{x} : x \in X \rangle \Phi(\widetilde{G}) = \langle \widetilde{x} : x \in X \rangle.$$

Ist $x_1^{a_1} \dots x_n^{a_n} = 1$ eine Relation in G mit $x_1, \dots, x_n \in X$, so ist $\widetilde{x_1}^{a_1} \dots \widetilde{x_n}^{a_n} \in W \leq \mathrm{Z}(\widetilde{G})$. Insbesondere ist $[\widetilde{y_1}^{b_1} \dots \widetilde{y_m}^{b_m}, \widetilde{x_1}^{a_1} \dots \widetilde{x_n}^{a_n}] = 1$ eine Relation in $\widetilde{G}$ mit $y_1, \dots, y_m \in X$. Nach Satz 8.10 existiert also ein Epimorphismus $\pi : F/[F,N] \to \widetilde{G}$ mit $\pi(x[F,N]) = \widetilde{x}$. Wegen $\widetilde{G}'/W = (\widetilde{G}/W)' \cong G' = G = \widetilde{G}/W$ ist $\widetilde{G}$ perfekt. Dies zeigt $\pi(\widehat{G}) = \pi((F/[F,N])') = \widetilde{G}' = \widetilde{G}$. Also ist $\widetilde{G}$ zu einer Faktorgruppe von $\widehat{G}$ isomorph. Insbesondere muss $\widehat{G}$ maximale Ordnung haben, d. h. $|\widehat{G}| = |G||M(G)|$. □

Bemerkung 12.19.

(i) Aus dem obigen Beweis folgt die *Hopf-Formel* $M(F/N) \cong (F' \cap N)/[F,N]$, wobei F eine freie Gruppe ist.

(ii) Die in Satz 12.18 konstruierte Gruppe $\widehat{G}$ heißt *universelle Schur-Erweiterung* von G.

Satz 12.20. *Die universelle Schur-Erweiterung einer perfekten Gruppe hat trivialen Schur-Multiplikator.*

Beweis. Sei $\widehat{G}/Z \cong G$ wie in Satz 12.18. Wegen $\widehat{G}'/Z = (\widehat{G}/Z)' \cong G' = G \cong \widehat{G}/Z$ ist auch $\widehat{G}$ perfekt. Sei $\widehat{\widehat{G}}$ eine Schur-Erweiterung von $\widehat{G}$ mit $\widehat{\widehat{G}}/W \cong \widehat{G}$. Dann ist auch $\widehat{\widehat{G}}$ perfekt. Sei $\mathrm{Z}(\widehat{\widehat{G}}/W) = X/W$. Dann ist $[\widehat{\widehat{G}}, X, \widehat{\widehat{G}}] = [\widehat{\widehat{G}}, \widehat{\widehat{G}}, X] \leq [\widehat{\widehat{G}}, W] = 1$. Aus Lemma 3.6 folgt $[X, \widehat{\widehat{G}}] = [X, \widehat{\widehat{G}}, \widehat{\widehat{G}}] = 1$ und $\mathrm{Z}(\widehat{\widehat{G}}/W) = X/W = \mathrm{Z}(\widehat{\widehat{G}})/W$. Wegen $\widehat{\widehat{G}}/W \cong \widehat{G}$ existiert $L/W \leq \mathrm{Z}(\widehat{\widehat{G}}/W)$ mit $\widehat{\widehat{G}}/L \cong (\widehat{\widehat{G}}/W)/(L/W) \cong \widehat{G}/Z \cong G$. Wegen $L \leq \mathrm{Z}(\widehat{\widehat{G}}) \cap \widehat{\widehat{G}}'$ ist also auch $\widehat{\widehat{G}}$ eine Schur-Erweiterung von G. Dies zeigt $\widehat{\widehat{G}} \cong \widehat{G}$ und $M(\widehat{G}) = 1$. □

Definition 12.21. Für endliche Gruppen G, H sei

$$P(G,H) := \{\varphi : G \times H \to \mathbb{C}^\times : \varphi(xy,z) = \varphi(x,z)\varphi(y,z),\ \varphi(x,yz) = \varphi(x,y)\varphi(x,z)\} \leq C^1(G \times H, \mathbb{C}^\times).$$

Die Elemente von $P(G,H)$ heißen *Paarungen*.

Satz 12.22 (Künneth-Formel)**.** *Für endliche Gruppen G und H gilt $M(G \times H) \cong M(G) \times M(H) \times P(G,H)$.*

Beweis. Sei $\alpha \in Z^2(G \times H, \mathbb{C}^\times)$. Wir fassen G und H als Untergruppen von $G \times H$ auf. Wie üblich hat man Einschränkungen $\alpha_G \in Z^2(G, \mathbb{C}^\times)$ und $\alpha_H \in Z^2(H, \mathbb{C}^\times)$. Sei $\varphi(x,y) := \alpha(x,y)\alpha(y,x)^{-1}$ für $x \in G$ und $y \in H$. Für $x, y \in G$ und $z \in H$ ist $xz = zx$, $yz = zy$ und

$$\begin{aligned}\varphi(xy,z) &= \alpha(xy,z)\alpha(z,xy)^{-1} = \alpha(y,z)\alpha(x,yz)\alpha(x,y)^{-1}\alpha(x,y)\alpha(z,x)^{-1}\alpha(zx,y)^{-1} \\ &= \varphi(x,z)\alpha(x,z)^{-1}\varphi(y,z)\alpha(z,y)\alpha(x,zy)\alpha(xz,y)^{-1} = \varphi(x,z)\varphi(y,z).\end{aligned}$$

Analog zeigt man $\varphi(x,yz) = \varphi(x,y)\varphi(x,z)$ für $x \in G$ und $y, z \in H$. Also ist $\varphi \in P(G,H)$. Dies liefert einen Homomorphismus

$$\begin{aligned}F : Z^2(G \times H, \mathbb{C}^\times) &\to Z^2(G, \mathbb{C}^\times) \times Z^2(H, \mathbb{C}^\times) \times P(G,H), \\ \alpha &\mapsto (\alpha_G, \alpha_H, \varphi).\end{aligned}$$

Für $\gamma \in C^1(G \times H, \mathbb{C}^\times)$ ist sicher $(\partial\gamma)_G = \partial\gamma_G \in B^2(G, \mathbb{C}^\times)$ und $(\partial\gamma)_H \in B^2(H, \mathbb{C}^\times)$. Wegen $\partial\gamma(x, y) = \partial\gamma(y, x)$ für $x \in G$ und $y \in H$ ist $F(\partial\gamma) = 1$. Somit induziert F einen Homomorphismus $\overline{F} : M(G \times H) \to M(G) \times M(H) \times P(G, H)$.

Surjektivität von $\overline{F}$: Sei $\alpha_1 \in Z^2(G, \mathbb{C}^\times)$, $\alpha_2 \in Z^2(H, \mathbb{C}^\times)$ und $\varphi \in P(G, H)$. Nach Lemma 12.8 dürfen wir $\alpha_1(1, 1) = \alpha_2(1, 1) = 1$ annehmen. Für $x_1, y_1 \in G$ und $x_2, y_2 \in H$ sei $\alpha(x_1x_2, y_1y_2) := \alpha_1(x_1, y_1)\alpha_2(x_2, y_2)\varphi(x_1, y_2)$. Dann ist

$$\begin{aligned}\alpha(x_1x_2, y_1y_2)\alpha(x_1y_1x_2y_2, z_1z_2) &= \alpha_1(x_1, y_1)\alpha_2(x_2, y_2)\varphi(x_1, y_2)\alpha_1(x_1y_1, z_1)\alpha_2(x_2y_2, z_2)\varphi(x_1y_1, z_2)\\ &= \alpha_1(y_1, z_1)\alpha_1(x_1, y_1z_1)\alpha_2(y_2, z_2)\alpha_2(x_2, y_2z_2)\varphi(x_1, y_2z_2)\varphi(y_1, z_2)\\ &= \alpha(y_1y_2, z_1z_2)\alpha(x_1x_2, y_1y_2z_1z_2)\end{aligned}$$

und $\alpha \in Z^2(G \times H, \mathbb{C}^\times)$. Wegen $\varphi(x, 1) = \varphi(x, 1)\varphi(x, 1) = 1$ für $x \in G$ ist $\alpha_G = \alpha_1$ und analog $\alpha_H = \alpha_2$. Für $x \in G$ und $y \in H$ ist schließlich

$$\alpha(x, y)\alpha(y, x)^{-1} = \alpha_1(x, 1)\alpha_2(1, y)\varphi(x, y)\alpha_1(1, x)^{-1}\alpha_2(y, 1)^{-1}\varphi(1, 1)^{-1} = \varphi(x, y).$$

Dies zeigt $F(\alpha) = (\alpha_1, \alpha_2, \varphi)$.

Injektivität von $\overline{F}$: Sei $F(\alpha) = (\partial\gamma_1, \partial\gamma_2, 1)$ mit $\gamma_1 \in C^1(G, \mathbb{C}^\times)$ und $\gamma_2 \in C^1(H, \mathbb{C}^\times)$. Es gilt dann $\alpha(x, y) = \alpha(y, x)$ für $x \in G$ und $y \in H$. Sei $\delta(xy) := \gamma_1(x)\gamma_2(y)\alpha(x, y)^{-1}$ für $x \in G$ und $h \in H$. Dann ist

$$\begin{aligned}\partial\delta(x_1x_2, y_1y_2) &= \delta(x_1x_2)\delta(y_1y_2)\delta(x_1y_1x_2y_2)^{-1}\\ &= \gamma_1(x_1)\gamma_2(x_2)\alpha(x_1, x_2)^{-1}\gamma_1(y_1)\gamma_2(y_2)\alpha(y_1, y_2)^{-1}\gamma_1(x_1y_1)^{-1}\gamma_2(x_2y_2)^{-1}\alpha(x_1y_1, x_2y_2)\\ &= \alpha(x_1, y_1)\alpha(x_2, y_2)\alpha(x_1, x_2)^{-1}\alpha(y_1, y_2)^{-1}\alpha(x_1y_1, x_2y_2)\\ &= \alpha(y_1, x_2)\alpha(x_1, y_1x_2)\alpha(x_1y_1, x_2)^{-1}\alpha(x_2, y_2)\alpha(x_1, x_2)^{-1}\alpha(y_1, y_2)^{-1}\alpha(x_1y_1, x_2y_2)\\ &= \alpha(x_1x_2, y_1)\alpha(x_1y_1x_2, y_2)\alpha(y_1, y_2)^{-1} = \alpha(x_1x_2, y_1y_2)\end{aligned}$$

für $x_1, y_1 \in G$ und $x_2, y_2 \in H$. Also ist $\alpha \in B^2(G \times H, \mathbb{C}^\times)$ und $\overline{F}$ ist ein Isomorphismus. □

Bemerkung 12.23.

(i) Für $\varphi \in P(G, H)$ und $y \in H$ ist $G \to \mathbb{C}^\times$, $x \mapsto \alpha(x, y)$ ein Homomorphismus. Insbesondere ist $\alpha(x, y) = 1$ für $x \in G'$ und analog $\alpha(x, y) = 1$ für $x \in G$ und $y \in H'$. Es folgt $P(G, H) \cong P(G/G', H/H')$.

(ii) Für Gruppen G, H und K gibt es Isomorphismen $P(G \times H, K) \cong P(G, K) \times P(H, K)$ und $P(G, H \times K) \cong P(G, H) \times P(G, K)$ durch Einschränkung (leicht zu zeigen). Mit dem nächsten Lemma kann man $P(G, H)$ also vollständig bestimmen.

Lemma 12.24. *Für $n, m \in \mathbb{N}$ ist $P(C_n, C_m) \cong C_{\mathrm{ggT}(n,m)}$.*

Beweis. Sei $\langle x\rangle \cong C_n$, $\langle y\rangle \cong C_m$ und $\alpha \in P(\langle x\rangle, \langle y\rangle)$. Dann ist $\alpha^n = 1$ und $\alpha^m = 1$, also auch $\alpha^{\mathrm{ggT}(n,m)} = 1$. Sei $\zeta \in \mathbb{C}$ eine primitive $\mathrm{ggT}(n, m)$-te Einheitswurzel. Dann ist $\varphi(x, y) = \zeta^k$ mit $0 \le k \le \mathrm{ggT}(n, m)$. Außerdem ist φ durch $\varphi(x, y)$ bereits eindeutig bestimmt. Für jedes $\zeta^k \in \langle\zeta\rangle$ kann man umgekehrt ein $\varphi \in P(\langle x\rangle, \langle y\rangle)$ mit $\alpha(x, y) = \zeta^k$ konstruieren. Dies liefert den Isomorphismus $P(C_n, C_m) \cong \langle\zeta\rangle \cong C_{\mathrm{ggT}(n,m)}$. □

Folgerung 12.25. *Sind G und H endliche Gruppen mit* $\mathrm{ggT}(|G/G'|, |H/H'|) = 1$*, so ist* $M(G \times H) \cong M(G) \times M(H)$.

Beweis. Die Behauptung folgt aus Satz 12.22, Bemerkung 12.23 und Lemma 12.24. □

Satz 12.26. *Es gilt*

$$M(C_{n_1} \times \ldots \times C_{n_k}) \cong \bigtimes_{1 \le i < j \le k} C_{\mathrm{ggT}(n_i, n_j)}.$$

Beweis. Nach Satz 12.17, Satz 12.22, Bemerkung 12.23 und Lemma 12.24 ist

$$\begin{aligned} M(C_{n_1} \times \ldots \times C_{n_k}) &= M(C_{n_2} \times \ldots \times C_{n_k}) \times P(C_{n_1}, C_{n_2} \times \ldots \times C_{n_k}) \cong \ldots \\ &\cong \bigtimes_{1 \le i < j \le k} P(C_{n_i}, C_{n_j}) \cong \bigtimes_{1 \le i < j \le k} C_{\mathrm{ggT}(n_i, n_j)}. \end{aligned}$$

□

Beispiel 12.27.

(i) Ist G elementarabelsch vom Rang n, so ist $M(G)$ elementarabelsch von Rang $\binom{n}{2}$. Insbesondere ist $M(C_2^2) \cong C_2$. Die Gruppen D_8 und Q_8 sind also die einzigen echten Schur-Erweiterungen von C_2^2. Die in Satz 12.14 konstruierte Gruppe $\widehat{G}$ ist im Allgemeinen also nicht eindeutig.

(ii) Nach Satz 12.16 ist $M(A_5) \le M(C_2^2) \cong C_2$. Nach Beispiel 12.2 ist daher $M(A_5) \cong C_2$. Da A_5 perfekt ist, gilt $M(A_5 \times G) \cong M(G) \times C_2$ für jede Gruppe G (Bemerkung 12.23).

(iii) Sei $\widehat{G}$ eine Schur-Erweiterung von $G \in \{D_{2^n}, Q_{2^n}, SD_{2^n}\}$ mit $\widehat{G}/Z \cong G$. Dann ist $\widehat{G}$ eine 2-Gruppe und $4 = |G : G'| = |\widehat{G}/Z : \widehat{G}'/Z| = |\widehat{G} : \widehat{G}'|$. Nach Taussky gilt daher $\widehat{G} \in \{D_{2^m}, Q_{2^m}, SD_{2^m}\}$. Es folgt $|Z| \le |\mathrm{Z}(\widehat{G})| = 2$ und im Fall $|Z| = 2$ ist $Z = \mathrm{Z}(\widehat{G})$ und $G \cong \widehat{G}/Z \cong D_{2^{m-1}}$. Wir haben also gezeigt:

$$M(G) \cong \begin{cases} C_2 & \text{falls } G \cong D_{2^n}, \\ 1 & \text{falls } G \in \{Q_{2^n}, SD_{2^n}\}. \end{cases}$$

Benjamin Sambale
Julian Brough

Hand in by: Mo 31. 10. 2016

Group theory
Sheet 1

On this sheet, groups are not necessarily finite!

Aufgabe 1 $(1+1+1+1$ points$)$**.** Let G be a group. Show:

(a) If H is a non-empty finite subset of G such that $xy \in H$ for all $x, y \in H$, then $H \leq G$.

(b) If $H \leq G$ such that $|G : H| = 2$, then $H \trianglelefteq G$.

(c) The map $G \to G$, $x \mapsto x^{-1}$ is an automorphism if and only if G is abelian.

(d) The map $G \to G$, $x \mapsto x^2$ is an endomorphism if and only if G is abelian.

Aufgabe 2 $(2+2+2+2+2+2$ points$)$**.** Let G be a group and $U, V, W \leq G$. Show:

(a) $V \subseteq U \implies |G : V| = |G : U||U : V|$.

(b) $U \cup V \leq G \iff U \cup V \in \{U, V\}$.

(c) $UV \leq G \iff UV = VU$.

(d) $|UV| = |U : U \cap V||V| = |V : U \cap V||U|$.

(e) If $|G : U|$ and $|G : V|$ are finite and coprime, then $|G : U \cap V| = |G : U||G : V|$ and $G = UV$.

(f) $U \subseteq W \implies UV \cap W = U(V \cap W)$ (Dedekind's modular law).

Aufgabe 3 $(2+2$ points$)$**.** Show that the following statements are *false*:

(a) If $d \mid |G| < \infty$, then G contains a subgroup of order d.

(b) If $M \trianglelefteq N \trianglelefteq G$, then $M \trianglelefteq G$.

Benjamin Sambale
Julian Brough

Hand in by: Mo 7. 11. 2016

Group theory
Sheet 2

Aufgabe 4 $(2+2+2$ points$)$**.** Let G be a group. Show:

(a) If $G/\operatorname{Z}(G)$ is cyclic, then G is abelian.

(b) If $|G|<\infty$ and $H<G$, then $\bigcup_{g\in G} gHg^{-1}\neq G$.

(c) If $\operatorname{Z}(G)=1$, then $\operatorname{C}_{\operatorname{Aut}(G)}(\operatorname{Inn}(G))=1$.

Aufgabe 5 $(2+2$ points$)$**.**

(a) How many abelian groups of order 72 exist up to isomorphism?

(b) Determine the isomorphism type of $\operatorname{Aut}(C_{24})$.

Aufgabe 6 $(2+2$ points$)$**.** A group G is called *complete* if $\operatorname{Z}(G)=1$ and $\operatorname{Aut}(G)=\operatorname{Inn}(G)$. Show:

(a) S_3 is complete.

(b) If N is a complete normal subgroup of a group G, then $G=N\oplus \operatorname{C}_G(N)$.

Aufgabe 7 (3 points)**.** Let G be a group and let $H\leq G$ such that $|G:H|<\infty$. Show that there exists a normal subgroup $N\trianglelefteq G$ such that $N\subseteq H$ and $|G:N|<\infty$.
Hint: Consider the action of G on G/H by left multiplication.

Benjamin Sambale
Julian Brough

Hand in by: Mo 14. 11. 2016

Group theory
Sheet 3

Aufgabe 8 $(2+2+2+2+2+2$ points$)$**.** A subgroup H of a group G is called *fully invariant* in G if $\alpha(H) \subseteq H$ for every endomorphism α of G.

(a) Show that every fully invariant subgroup of G is characteristic in G.

(b) Show that every subgroup of a cyclic group is fully invariant.

(c) Compute the normal subgroups of S_4. Which of them are characteristic or fully invariant?
Hint: You may use the structure of the conjugacy classes (1st example class).

(d) Show that $\mathrm{Z}(G)$ is characteristic in G for any group G.

(e) Show that $\mathrm{Z}(G)$ is *not* always fully invariant in G.

(f) Show that $\mathrm{Inn}(G)$ is characteristic in $\mathrm{Aut}(G)$ if G is simple.
Hint: Use Exercise 4(c).

Aufgabe 9 $(2+2$ points$)$**.** Determine the composition factors and chief factors of S_4 and $\mathrm{GL}(2,\mathbb{F}_3)$.
Hint: It helps to consider the action of $\mathrm{GL}(2,\mathbb{F}_3)$ on the set of 1-dimensional subspaces of $\mathbb{F}_3^2$.

Aufgabe 10 (3 points)**.** Show that S_6 is generated by two elements but contains a subgroup which is *not* generated by two elements.

Benjamin Sambale
Julian Brough

Hand in by: Mo 21. 11. 2016

Group theory
Sheet 4

Aufgabe 11 (2 + 2 points)**.** Let G be a group and $x, y \in G$. Show:

(a) If $[x, x, y] = 1$, then $[x^n, y] = [x, y]^n$ for all $n \in \mathbb{Z}$.

(b) If $[x, x, y] = [y, x, y] = 1$, then $(xy)^n = x^n y^n [y, x]^{\binom{n}{2}}$ for $n \in \mathbb{N}$.

Aufgabe 12 (2 + 2 points)**.** Let A be an abelian normal subgroup of a group G such that G/A is cyclic, say $G/A = \langle xA \rangle$ with $x \in G$. Show that the map $A \to G'$, $a \mapsto [a, x]$ is an epimorphism. Conclude that $|A| = |G'||A \cap \mathrm{Z}(G)|$.

Aufgabe 13 (2 points)**.** Show that $\mathrm{F}(N \oplus M) = \mathrm{F}(N) \oplus \mathrm{F}(M)$ for groups N and M.

Aufgabe 14 (3 + 3 points)**.** Let G be a group. Show:

(a) $\exp(\mathrm{Z}_i(G)/\mathrm{Z}_{i-1}(G)) \leq \exp(\mathrm{Z}(G))$ for $i \geq 1$.
Hint: Use induction on i and Exercise 11(a).

(b) $[G^{[i]}, \mathrm{Z}_j(G)] \leq \mathrm{Z}_{j-i}(G)$ for $1 \leq i \leq j$.
Hint: Use induction on $i + j$ and the 3-subgroups lemma.

Benjamin Sambale
Julian Brough

Hand in by: Mo 28. 11. 2016

Group theory
Sheet 5

Aufgabe 15 $(2+2+2+2+2+2$ points$)$**.**

(a) Compute $\Phi(S_4)$.

(b) Show that $\Phi(N \oplus M) = \Phi(N) \oplus \Phi(M)$ for finite groups N, M.

(c) Compute the Frattini subgroup of a finite abelian group.
Hint: Please don't use the definition.

(d) Show that $\Phi(G) \leq \mathrm{F}(G)$ and $\mathrm{F}(G/\Phi(G)) = \mathrm{F}(G)/\Phi(G)$ for every finite group G.

(e) Let P be a finite p-group with $Q \leq P$, $N \trianglelefteq P$. Show that $\Phi(Q) \leq \Phi(P)$ and $\Phi(P/N) = \Phi(P)N/N$.

(f) Show that $\Phi(P) = \langle x^2 : x \in P \rangle$ for every finite 2-group P.

Aufgabe 16 (3 points)**.** Let G_1 and G_2 be groups. Show that there is a bijection between the subgroups of $G_1 \times G_2$ and the set of 5-tuples $(H_1, H_2, K_1, K_2, \varphi)$ where $K_i \trianglelefteq H_i \leq G_i$ $(i = 1, 2)$ and $\varphi : H_1/K_1 \to H_2/K_2$ is an isomorphism.

Aufgabe 17 (3 points)**.** Let G be a finite group such that every two conjugate elements commute (i. e. $[x, gxg^{-1}] = 1$ for all $x, g \in G$). Show that G is nilpotent.

Benjamin Sambale
Julian Brough

Hand in by: Mo 05. 12. 2016

Group theory
Sheet 6

Aufgabe 18 (2 + 2 + 2 points)**.** Let H be a Hall π-subgroup of a finite group G, and let $N \trianglelefteq G$. Show:

(a) $H \cap N$ is a Hall π-subgroup of N and HN/N is a Hall π-subgroup of G/N.

(b) $H \cap U$ is *not* always a Hall π-subgroup of U if $U \leq G$.

(c) $\mathrm{N}_G(\mathrm{N}_G(H)) = \mathrm{N}_G(H)$.

Aufgabe 19 (2 + 2 points)**.** Determine the integers $n \geq 2$ such that the dihedral group D_{2n} is nilpotent. Also compute the nilpotency class of D_{2n} for those values of n.

Aufgabe 20 (2 points)**.** Let G be a finite group such that $|\Phi(G)|$ is divisible by a prime p. Show that p divides $|G/\Phi(G)|$.

Aufgabe 21 (2 points)**.** A finite group G is called *Frobenius group* if there exists a subgroup $1 < H < G$ such that $H \cap gHg^{-1} = 1$ for every $g \in G \setminus H$. Show that in this case H is a Hall subgroup of G.

Aufgabe 22 (3 points)**.** Construct a finite group G with two non-conjugate Hall π-subgroups.
Hint: One can take $G = \mathrm{GL}(3, 2)$.

Benjamin Sambale
Julian Brough

Hand in by: Mo 19. 12. 2016
(no courses next week!)

Group theory
Sheet 7

Aufgabe 23 (2 + 2 points)**.** Determine the transitive permutation groups of degree at most 4. Which of them are primitive or regular?

Aufgabe 24 (3 points)**.** How many ways exist to color the faces of a tetrahedron if we can choose from n colors (distinct faces may have the same color)?

Aufgabe 25 (2 + 2 points)**.**

(a) Let $G \to \mathrm{Sym}(\Omega)$ be a transitive action such that $1 < |\Omega| < \infty$. Show that G contains an element without fixed points on Ω.

(b) Let $\sigma \in S_n$ be chosen uniformly at random. What is the probability that σ has no fixed points?

Aufgabe 26 (3 points)**.** Show that A_5 is a primitive permutation group of degree 5, 6 and 10.

Aufgabe 27 (3 points)**.** Let G be a non-abelian simple group. Show that $\mathrm{Aut}(G)$ is complete (cf. Exercise 6).
Hint: Use Exercise 4(c).

Benjamin Sambale
Julian Brough

Hand in by: Mo 09. 01. 2017

Group theory
Sheet 8

Aufgabe 28 (2 points)**.** Compute the transfer $V_{G/G'}$.

Aufgabe 29 (2 points)**.** Show that $|G' \cap \mathrm{Z}(G)|$ is not divisible by p if G has abelian Sylow p-subgroups (p is a prime).

Aufgabe 30 (2 points)**.** Let G be a transitive permutation group such that every non-trivial element of G has at most one fixed point and at least one non-trivial element has a fixed point. Show that G is a Frobenius group (cf. Exercise 21).

Aufgabe 31 (3 points)**.** Show that $\mathrm{SL}(2, \mathbb{F}_{2^n})$ acts 3-transitively on the set of 1-dimensional subspaces of $\mathbb{F}_{2^n}^2$.

Aufgabe 32 (3 points)**.** How many groups of order 12 exist up to isomorphism?

Aufgabe 33 (3 points)**.** Let $G \neq 1$ be a finite group such that 1 and G are the only fully invariant subgroups of G (cf. Exercise 8). Show that G is characteristically simple.

Benjamin Sambale
Julian Brough

Hand in by: Mo 16. 01. 2017

Group theory
Sheet 9

Aufgabe 34 $(6 + 2 + 2$ points$)$**.**

(a) Show that A_5 is the only non-abelian simple group of order less than 168.

(b) Show that every group of order 264 is solvable.

(c) Show that the infinite group $A_\infty := \bigcup_{n\geq 1} A_n$ is simple.

Aufgabe 35 (2 points)**.** Let G be a finite p-nilpotent group and let $P \in \mathrm{Syl}_p(G)$. Show that $\mathrm{N}_G(Q)/\mathrm{C}_G(Q)$ is a p-group for every $Q \leq P$ (converse of Frobenius transfer theorem).

Aufgabe 36 $(2 + 2$ points$)$**.**

(a) Give a presentation of S_4 in terms of generators and relations.

(b) Determine the structure of $\langle x, y \mid x^2 = y^2 = 1\rangle$.
Hint: It is a semidirect product of familiar groups.

Aufgabe 37 (3 points)**.** Show that

$$\langle x, y, z \mid xyx^{-1} = y^2,\ yzy^{-1} = z^2,\ zxz^{-1} = x^2\rangle = 1.$$

Benjamin Sambale
Julian Brough

Hand in by: Mo 23. 01. 2017

Group theory
Sheet 10

Aufgabe 38 (2 + 2 + 2 + 2 points)**.** Let $n \geq 3$.

(a) Let $\mathbb{H} := \mathbb{R} + \mathbb{R}i + \mathbb{R}j + \mathbb{R}k$ be the Hamiltonian skew field defined by

$$i^2 = j^2 = k^2 = ijk = -1.$$

Show that $\{\pm 1, \pm i, \pm j, \pm k\} \cong Q_8$ with respect to multiplication.

(b) Show that $Q_{2^n} = \langle x, y \mid x^{2^{n-2}} = y^2,\ yxy^{-1} = x^{-1} \rangle$ (note the difference to the definition).

(c) Show that $G/\operatorname{Z}(G) \ncong Q_{2^n}$ for any group G.
Hint: Exercise 4(a) is relevant.

(d) Compute $\operatorname{Aut}(Q_8)$.
Hint: Study the action of $\operatorname{Aut}(Q_8)$ on the set of maximal subgroups of Q_8.

Aufgabe 39 (2 + 2 + 2 points)**.** A finite group is called *Dedekind group* if all of its subgroups are normal.

(a) Show that every Dedekind group is nilpotent.

(b) Show that a Dedekind p-group is abelian if $p > 2$.
Hint: Use Theorem 9.6.

(c) Show that $Q_8 \times C_2^n$ is a Dedekind group for every $n \geq 0$.

Aufgabe 40 (2 + 2 points)**.**

(a) Determine the integers $n \geq 1$ such that $\operatorname{Aut}(C_n)$ is cyclic.
Hint: Use Theorem 8.12.

(b) Show that $\operatorname{Aut}(G) \ncong C_3$ for any finite group G.

Aufgabe 41 (2 points)**.** Let P be a non-abelian p-group with an abelian subgroup A of order p^2 such that $\operatorname{C}_P(A) = A$. Show that P has maximal class.
Hint: Use induction on $|P|$.

Benjamin Sambale
Julian Brough

Hand in by: Mo 30. 01. 2017

Group theory
Sheet 11

Aufgabe 42 $(2+2+2+2$ points$)$**.** Let G be a finite group. Show:

(a) G is nilpotent if and only if all its subgroups are subnormal.

(b) $H \leq \mathrm{F}(G)$ if and only if H is nilpotent and $H \trianglelefteq \trianglelefteq G$.

(c) If $H, K \trianglelefteq \trianglelefteq G$, then $H \cap K \trianglelefteq \trianglelefteq G$.

(d) If $H \trianglelefteq \trianglelefteq G$ and $P \in \mathrm{Syl}_p(G)$, then $H \cap P \in \mathrm{Syl}_p(H)$.

Aufgabe 43 $(2+2+2$ points$)$**.** For a finite group G we denote the smallest cardinality of a generating set by $d(G)$. Let $d(1) := 0$. Show:

(a) $d(A_n) = 2$ for $n \geq 4$.
Hint: Show first that A_n is generated by the 3-cycles.

(b) $|G| \geq 2^{d(G)}$.

(c) $|\mathrm{Aut}(G)| \leq \prod_{i=0}^{d(G)-1}(|G| - 2^i)$ and this is best possible.

Aufgabe 44 $(2+2$ points$)$**.**

(a) Show that a group is finite if and only if it has only finitely many subgroups.

(b) Show that a finitely generated group has only finitely many subgroups of a given index $n \in \mathbb{N}$.

Aufgabe 45 (2 points)**.** Show that $2_+^{1+2n} \ncong 2_-^{1+2n}$ for every $n \geq 1$ (see Theorem 9.21).
Hint: Compare the number of elements of order 4 in both groups.

Benjamin Sambale
Julian Brough

Hand in by: Mo 06. 02. 2017

Group theory
Sheet 12

Aufgabe 46 (2 points)**.** Show that every minimal normal subgroup of a finite group G is contained in $\mathrm{F}^*(G)$.

Aufgabe 47 $(2+3$ points$)$**.** Let $q \neq 1$ be a prime power.

(a) Determine the isomorphism type of a Sylow p-subgroup of $\mathrm{GL}(2,q)$ where $p \mid q$.

(b) Determine the isomorphism type of a Sylow 2-subgroup of $\mathrm{SL}(2,q)$ and of $\mathrm{PSL}(2,q)$.
Hint: Use Theorem 9.6.

Aufgabe 48 $(2+2$ points$)$**.** Let $\widehat{G}$ be a Schur cover of a finite group G with $\widehat{G}/Z \cong G$.

(a) Show that for every $W \leq Z$, also $\widehat{G}/W$ is a Schur cover of G.

(b) Let $\widehat{H}$ be a Schur cover of a finite group H. Show that $\widehat{G} \times \widehat{H}$ is a Schur cover of $G \times H$.

Aufgabe 49 (3 points)**.** Show that $\mathrm{PSL}(3,4)$ and A_8 are non-isomorphic simple groups of the same order.
Hint: Use the Jordan canonical form to show that $\mathrm{PSL}(3,4)$ has no element of order 6.

Stichwortverzeichnis