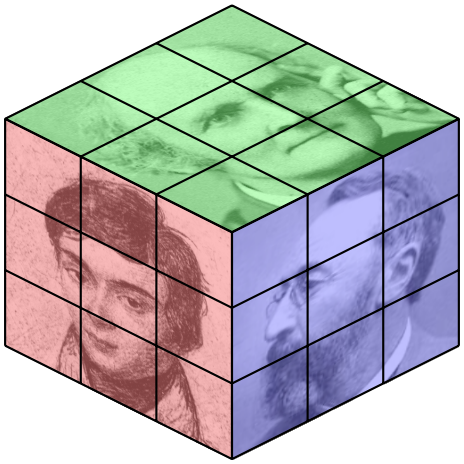
Gruppentheorie

Vorlesung im Sommersemester 2024

Benjamin Sambale
Leibniz Universität Hannover

Version: 28. Juli 2024



Inhaltsverzeichnis

Vorwort

Dieses Skript ist die Grundlage meiner Vorlesung im Sommersemester 2024 an der Leibniz Universität Hannover. Es handelt sich um eine „halbierte“ Version meines Skripts aus früheren Veranstaltungen (Homepage).

Literatur:

- H. Kurzweil, B. Stellmacher, *Theorie der endlichen Gruppen*, Springer, Berlin, 1998[1]
- G. Stroth, *Endliche Gruppen*, De Gruyter, Berlin, 2013[2]
- B. Huppert, *Endliche Gruppen I*, Springer, Berlin, 1967[3]
- I. M. Isaacs, *Finite group theory*, Amer. Math. Soc., R.I., 2008[4]
- J. J. Rotman, *An introduction to the theory of groups*, 4th edition, Springer, New York, 1995
- D. Gorenstein, *Finite groups*, 2nd edition, Chelsea, New York, 1980

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

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:

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

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 $xe = x(yx) = (xy)x = ex = x$. Daher ist e auch rechtsneutral und linksinverse Elemente sind rechtsinvers. 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

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

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*. In diesem Fall ist G auch abelsch. Elemente der Ordnung 2 nennt man *Involutionen*.

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. Falls $|K| = q < \infty$, so schreiben wir $\mathrm{GL}(n, q) := \mathrm{GL}(n, K)$ (dies ist wohldefiniert, da es bis auf Isomorphie nur einen Körper mit q Elementen gibt).

(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* $\bigtimes_{i \in I} G_i$ eine Gruppe mit $(g_i)_{i \in I}(h_i)_{i \in I} := (g_i h_i)_{i \in I}$ für $(g_i)_{i \in I}, (h_i)_{i \in I} \in \bigtimes_{i \in I} G_i$. 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 alle $x, y \in H$ 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

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

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 $x_1, \ldots, x_n \in U$ (dies entspricht den Linearkombinationen in der linearen Algebra). 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) Jede endliche Untergruppe der multiplikativen Gruppe eines Körpers K ist zyklisch (Algebra). Für $n \in \mathbb{N}$ besitzt $K^\times$ höchstens eine Untergruppe der Ordnung n; diese besteht aus den n-ten Einheitswurzeln.

(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) $\boxed{|UV||U \cap V| = |U||V|}$ (*Produktformel*).

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

(v) $|G : U \cap V| \leq |G : U||G : V|$ (POINCARÉ).

Beweis. Aufgabe 3. □

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 2).

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

$$NM = \bigcup_{x \in N} xM = \bigcup_{x \in N} Mx = MN = \langle N, M \rangle \trianglelefteq G$$

nach Lemma 1.9.

(iv) $S_2 \not\trianglelefteq S_3$, denn $(1,3)(1,2)(1,3)^{-1} = (2,3) \notin S_2$.

Definition 1.13. Eine Abbildung $f \colon G \to H$ 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.

Beispiel 1.14.

(i) Der *triviale* Homomorphismus $G \to H$, $g \mapsto 1$ und der *triviale* Automorphismus id_G.

(ii) Für $H \leq G$ ist die Inklusionsabbildung $H \to G$, $h \mapsto h$ ein Monomorphismus.

(iii) Ist $f\colon G \to H$ ein Homomorphismus und $U \leq G$, so ist auch die Einschränkung $f_{|U}\colon K \to H$ ein Homomorphismus.

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

Bemerkung 1.15.

(i) Für einen Homomorphismus $f\colon G \to H$ gilt offenbar $f(1_G) = 1_H$ und $f(x^{-1}) = f(x)^{-1}$ für $x \in G$. Ist $g\colon H \to K$ ein weiterer Homomorphismus, so ist auch $g \circ f\colon G \to K$ ein Homomorphismus. Für $U \leq G$ und $V \leq H$ ist $f(U) \leq H$ und $f^{-1}(V) := \{x \in G : f(x) \in V\} \leq G$. Für $U \trianglelefteq G$ ist $f(U) \trianglelefteq f(G)$, aber nicht unbedingt $f(U) \trianglelefteq H$! Für $V \trianglelefteq H$ ist hingegen stets $f^{-1}(V) \trianglelefteq G$ (in der Analysis sind Urbilder offener Mengen unter stetigen Abbildungen wieder offen, aber Bilder nicht unbedingt). Insbesondere ist $f(G) \leq H$ und $\mathrm{Ker}(f) = f^{-1}(1) \trianglelefteq G$ (*Kern* von f). Genau dann ist f injektiv, wenn $\mathrm{Ker}(f) = 1$ gilt.

(ii) Ist $f\colon G \to H$ ein Isomorphismus, so auch $f^{-1}\colon H \to G$. 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 $f_x\colon G \to G$, $g \mapsto xgx^{-1}$ ein *innerer* Automorphismus von G. Wegen $f_x \circ f_y = f_{xy}$ für $x, y \in G$ ist $f\colon G \to \mathrm{Aut}(G)$, $x \mapsto f_x$ ein Homomorphismus mit Bild $\mathrm{Inn}(G) := f(G)$. Für $\alpha \in \mathrm{Aut}(G)$ und $g, x \in G$ gilt

$$(\alpha \circ f_x \circ \alpha^{-1})(g) = \alpha(x\alpha^{-1}(g)x^{-1}) = \alpha(x)g\alpha(x)^{-1} = f_{\alpha(x)}(g).$$

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.

Satz 1.16.

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

(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

$$\boxed{HN/N \cong H/(H \cap N).}$$

(iv) (2. Isomorphiesatz) Für $N \trianglelefteq G$ und $N \leq H \leq G$ ist $H \trianglelefteq G$ genau dann, wenn $H/N \trianglelefteq G/N$. Gegebenenfalls ist $\boxed{G/H \cong (G/N)/(H/N).}$

Beweis. Algebra. □

Definition 1.17. 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 1.18.

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

Sei nun umgekehrt ein Homomorphismus $f \colon G \to \mathrm{Sym}(\Omega)$, $x \mapsto f_x$ 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 $\mathrm{Ker}(f) = 1$ (bzw. $\mathrm{Ker}(f) = G$) 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 1.19.

(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. Wegen $gH = (gHg^{-1})g$ ist jede Linksnebenklasse auch eine Rechtsnebenklasse, wenn auch nicht unbedingt zur gleichen Untergruppe.

(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 $\mathrm{Inn}(G)$. Nach dem Homomorphiesatz ist

$$G/\mathrm{Z}(G) \cong \mathrm{Inn}(G) \leq \mathrm{Aut}(G) \leq \mathrm{Sym}(G).$$

(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 $\mathrm{N}_G(H)$ durch Konjugation auf H mit Kern $\mathrm{C}_G(H) := \bigcap_{h\in H} \mathrm{C}_G(h)$. Insbesondere ist $\mathrm{N}_G(H)/\mathrm{C}_G(H)$ zu einer Untergruppe von $\mathrm{Aut}(H)$ isomorph.

Satz 1.20. *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* $\boxed{|G/G_\omega| = |{}^G\omega|.}$ *Ist $|G| < \infty$, so ist also jede Bahnenlänge ein Teiler von $|G|$. Ist G zusätzlich transitiv, so ist $|\Omega|$ ein Teiler von $|G|$.*

Beweis. Wohldefiniertheit und Injektivität:

$$xG_\omega = yG_\omega \iff y^{-1}x \in G_\omega \iff {}^{y^{-1}x}\omega = \omega \iff {}^x\omega = {}^y({}^{y^{-1}x}\omega) = {}^y\omega.$$

Die Surjektivität ist offensichtlich. Die letzten beiden Aussagen folgen nach Lagrange. □

Bemerkung 1.21. Sind $(\omega_i)_{i\in I}$ Repräsentanten für die Bahnen von G auf Ω, so gilt die *Bahnengleichung*

$$\boxed{|\Omega| = \sum_{i\in I} |{}^G\omega_i| = \sum_{i\in I} |G : G_{\omega_i}|.}$$

Im Spezialfall der Konjugationsoperation erhält man die *Klassengleichung*

$$\boxed{|G| = \sum_{i\in I} |G : \mathrm{C}_G(x_i)|,}$$

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

$$|G| = |\mathrm{Z}(G)| + \sum_{j\in J} |G : \mathrm{C}_G(x_j)|. \tag{1.1}$$

Satz 1.22 (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 1.23. 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 zusätzlich 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. Tatsächlich gibt es unendliche Gruppen, in denen sogar jede echte Untergruppe Ordnung p hat für sehr große Primzahlen p (*Tarski-Monster*). Andererseits weiß man nicht, ob jede Gruppe mit zwei Erzeugern und Exponent 5 endlich ist. Gelöst ist hingegen das *beschränkte Burnside-Problem*: Für $d, e \in \mathbb{N}$ gibt es nur endlich viele endliche Gruppen mit d Erzeugern und Exponent e. Zelmanov bekam dafür die *Fields-Medaille*.

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 $n \mid ks$. Nun ist l ein Teiler von $\frac{k}{\mathrm{ggT}(n,k)}s$, aber teilerfremd zu $\frac{k}{\mathrm{ggT}(n,k)}$. Dies zeigt $l \mid s$ und $l = s$. Es folgt

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

Sei nun $y \in \mathrm{C}_G(x)$ wie angegeben. Wegen $xy = yx$ ist $(xy)^{mn} = (x^n)^m(y^m)^n = 1$ also $s := |\langle xy\rangle| \leq mn$. Nach dem euklidischen Algorithmus existieren $a, b \in \mathbb{Z}$ mit $an + bm = 1$. Es gilt dann

$$x = x^{an+bm} = x^{an}x^{bm} = x^{bm} = x^{bm}y^{bm} = (xy)^{bm} \in \langle xy\rangle.$$

Lagrange zeigt $n = |\langle x\rangle| \mid s$ und analog $m = |\langle y\rangle| \mid s$. Wegen $\mathrm{ggT}(n,m) = 1$ ist auch $nm \mid s$ und $s = mn$. □

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. *Sei $n \in \mathbb{N}$.*

(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 $\varphi(n)$ (eulersche φ-Funktion).*

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 $d = |H| \,\big|\, n$. Nach Lagrange gilt $x^{n/d}H = (xH)^{|\langle x\rangle/H|} = H$ und $x^{n/d} \in H$. Dies zeigt $H = \langle x^{n/d}\rangle$. 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 $\Phi\colon \mathrm{Aut}(\langle x \rangle) \to (\mathbb{Z}/n\mathbb{Z})^\times$, $\alpha \mapsto i + n\mathbb{Z}$. 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 $G = N_1 \oplus \ldots \oplus N_k$. Lässt sich $G \neq 1$ nicht als direkte Summe von echten Untergruppen schreiben, so nennt man G *unzerlegbar*.

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

Beweis. Wir zeigen, dass die Abbildung

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

ein Isomorphismus ist. Für $i > j$ gilt nach Voraussetzung $N_i \cap N_j \subseteq N_i \cap N_1 \ldots N_{i-1} = 1$. 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. Sei $(x_1, \ldots, x_k) \in \mathrm{Ker}(F)$. Angenommen es existiert $1 \leq l \leq k$ mit $x_l \neq 1$. Sei l maximal mit dieser Eigenschaft. Dann wäre $x_l^{-1} = x_1 \ldots x_{l-1} \in N_l \cap N_1 \ldots N_{l-1} = 1$. Also ist $\mathrm{Ker}(F) = 1$ und F ist auch injektiv. □

Bemerkung 2.8.

(i) 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.

(ii) Die Summanden einer direkten Summe sind in der Regel nicht eindeutig bestimmt. Zum Beispiel ist

$$\langle (1,2)\rangle \oplus \langle (3,4)\rangle = \langle (1,2)\rangle \oplus \langle (1,2)(3,4)\rangle \leq S_4.$$

Außerdem kann in Definition 2.6 die zweite Bedingung nicht durch $N_i \cap N_j = 1$ für $i \neq j$ ersetzt werden kann (sonst wäre $\langle (1,2)\rangle \oplus \langle (3,4)\rangle \oplus \langle (1,2)(3,4)\rangle$). Der folgende Satz zeigt, dass die unzerlegbaren Summanden einer endlichen Gruppe bis auf Reihenfolge und Isomorphie eindeutig bestimmt sind.

Satz 2.9 (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 existiert für jedes i ein j mit

$$G = G_1 \oplus \ldots \oplus G_{i-1} \oplus H_j \oplus G_{i+1} \oplus \ldots \oplus G_s.$$

Insbesondere ist $s = t$ und bei geeigneter Nummerierung gilt $G_i \cong H_i$ für $i = 1, \ldots, s$.

Beweis (Kurosch). Induktion nach $|G|$. O. B. d. A. sei $i = 1$. Sei $\pi_i \colon G \to H_i$ die i-te Projektion der zweiten Zerlegung und $H_{i1} := \pi_i(G_1) \leq H_i$ für $i = 1, \ldots, t$.

Fall 1: Es existiert ein i mit $H_{i1} < H_i$.
Sei $H := H_{11} \oplus \ldots \oplus H_{t1} < G$. Wegen $g = \pi_1(g) \ldots \pi_t(g)$ für alle $g \in G_1$ gilt $G_1 \leq H$. Nach Dedekind ist $H = G_1 \oplus (G_2 \ldots G_s \cap H)$. Wir zerlegen die H_{j1} in unzerlegbare Faktoren. Nach Induktion existiert ein unzerlegbarer Summand K von H_{j1}, den man für G_1 einsetzen kann, d. h. $H = K \oplus (G_2 \ldots G_s \cap H)$ und $K \cap G_2 \ldots G_s = 1$. Jedes Element in K hat die Form $\pi_j(g_1)$ für ein $g_1 \in G_1$. Für $g \in G_2 \ldots G_s$ gilt

$$g\pi_j(g_1) = \pi_1(g) \ldots \pi_j(gg_1) \ldots \pi_t(g) = \pi_1(g) \ldots \pi_j(g_1 g) \ldots \pi_t(g) = \pi_j(g_1)g.$$

Es folgt $K \leq \mathrm{C}_G(G_2 \ldots G_s)$. Aus $|G_1| = |K|$ ergibt sich $G = K \oplus G_2 \oplus \ldots \oplus G_s$. Wieder nach Dedekind ist $H_j = K \oplus (G_2 \ldots G_s \cap H_j)$. Da H_j unzerlegbar ist, muss $K = H_{j1} = H_j$ gelten.

Fall 2: Es gilt $G = H_{11} \oplus \ldots \oplus H_{t1}$.
Dann ist $|G_1| \geq |\pi_i(G_1)| = |H_{i1}| = |H_i|$ für $i = 1, \ldots, t$. Betrachten wir die umgekehrte Projektion $\rho_1 \colon G \to G_1$. Angenommen es gilt $\rho_1(H_i) = G_1$ für ein i. Dann ist $G = H_i G_2 \ldots G_s$ und wegen $|H_i| \leq |G_1|$ muss die Summe direkt sein. Wir können also $\rho_1(H_i) < G_1$ für $i = 1, \ldots, t$ voraussetzen. Man kann nun wie im Fall 1 (nur mit umgekehrten Rollen) nacheinander die H_i jeweils durch ein G_j ersetzen (die Voraussetzung $\rho_1(H_i) < G_1$ bleibt erhalten). Die dabei benutzten G_j müssen paarweise verschieden sein, damit die Summe direkt bleibt. Damit am Ende die rechte Seite der Gleichung die richtige Größe hat, muss irgendwann auch G_1 benutzt werden. Sagen wir H_i wird durch G_1 ersetzt. Verfolgt man die Argumentation von Fall 1 bis zur Gleichung $K = H_{j1} = H_j$, so erkennt man dies nur im Fall $\rho_1(H_i) = G_1$ gelten kann. Widerspruch.

Damit ist die erste Aussage bewiesen. Für die zweite Behauptung beobachtet man, dass

$$G_i \cong G/G_1 \ldots G_{i-1} G_{i+1} \ldots G_s \cong H_j$$

gilt. Man kann nun der Reihe nach jedes G_i durch ein H_j ersetzen. Wie in Fall 2 erklärt muss man dafür paarweise verschiedene H_j benutzen. Am Ende müssen alle H_j verbraucht sein, damit die Ordnung korrekt ist. Dies zeigt $s = t$. □

Bemerkung 2.10. Unendliche Gruppen lassen sich nicht unbedingt als direkte Summen von unzerlegbaren Faktoren schreiben. Für endlich erzeugte abelsche Gruppen existiert nach (ii) des folgenden Satzes eine solche Zerlegung und der Satz von Krull-Schmidt bleibt richtig.

Satz 2.11 (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 $1 < d_1 \mid \ldots \mid d_t$ mit

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

(ii) Es existieren eindeutig bestimmte Primzahlpotenzen $1 < p_1^{a_1} \leq \ldots \leq p_t^{a_t}$ 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.
Sei $x_1, \ldots, x_r$ ein minimales Erzeugendensystem, 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 ist $\mathbb{Z}^r \to G$, $(n_1, \ldots, n_r) \mapsto x_1^{n_1} x_2^{n_2} \ldots x_r^{n_r}$ ein Isomorphismus.

Nehmen wir nun an, dass auch nicht-triviale Relationen existieren. Wir wählen $x_1, \ldots, x_r$ unter allen minimalen Erzeugendensystemen so, dass eine Relation mit minimalem Exponenten $d_1 > 0$ gilt.O. B. d. A. sei $x_1^{d_1} x_2^{n_2} \ldots x_r^{n_r} = 1$. Im Fall $r = 1$ ist $G \cong C_{d_1}$. Sei also $r > 1$. Wir zeigen $d_1 \mid n_2$. Division mit Rest ergibt $n_2 = qd_1 + u$ mit $0 \leq u < d_1$. Die Relation wird zu

$$1 = x_1^{d_1} x_2^{qd_1+u} \ldots x_r^{n_r} = (x_1 x_2^q)^{d_1} x_2^u x_3^{n_3} \ldots x_r^{n_r}. \tag{2.1}$$

Da man jedes Element $x_1^{l_1} \ldots x_r^{l_r}$ auch in der Form $(x_1 x_2^q)^{l_1} x_2^{l_2 - q l_1} x_3^{l_3} \ldots x_r^{l_r}$ schreiben kann, ist $x_1 x_2^q, x_2, \ldots, x_r$ ebenfalls ein minimales Erzeugendensystem. Aus der Wahl von d_1 sowie (2.1) folgt $u = 0$ und damit $d_1 \mid n_2$. Analog zeigt man $d_1 \mid n_3, \ldots, d_1 \mid n_r$. Wir schreiben $n_i = q_i d_1$ für $i = 3, \ldots, r$. Setzt man $z := x_1 x_2^q x_3^{q_3} \ldots x_r^{q_r}$, so ist $z, x_2, \ldots, x_r$ wieder ein minimales Erzeugendensystem und die Relation wird zu $1 = z^{d_1}$. Damit hat z die Ordnung d_1, denn $1 = z^l = z^l x_2^0 \ldots x_r^0$ mit $0 < l < d_1$ wäre ein Widerspruch zur Wahl vom d_1. Mit $H := \langle z \rangle$ und $G_1 := \langle x_2, \ldots, x_r \rangle$ gilt $G = HG_1$. 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 $0 < l_1 < d_1$. Dann wäre aber $z^{l_1} x_2^{-l_2} \ldots x_r^{-l_r} = 1$ ein Widerspruch zur Wahl von d_1. Folglich ist $H \cap G_1 = 1$ und $G = H \oplus G_1 \cong C_{d_1} \times G_1$.

Nun kann man den Prozess mit G_1 wiederholen. Dann ist $G_1 \cong C_\infty^{r-1}$ oder $G_1 \cong C_{d_2} \times G_2$. Im ersten Fall ist $G \cong C_\infty^{r-1} \times C_{d_1}$ und wir sind fertig. Im zweiten Fall ist $G \cong C_{d_1} \times C_{d_2} \times G_2$, wobei d_2 als Exponent einer Relation $y_2^{d_2} y_3^{n_3'} \ldots y_r^{n_r'} = 1$ mit einem minimalen Erzeugendensystem $y_2, \ldots, y_r$ von G_1 auftritt. Jetzt ist $z, y_2, \ldots, y_r$ ein minimales Erzeugendensystem von G und es gilt die Relation $z^{d_1} y_2^{d_2} y_3^{n_3'} \ldots y_r^{n_r'} = 1$. Wie oben zeigt man $d_1 \mid d_2$. Man iteriert nun den Prozess mit G_2. Am Ende hat G die gewünschte Form.

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 schließlich

$$\overline{G} := G/H \cong C_\infty^s \cong C_\infty^{s'}.$$

Für $\overline{G}_2 := \{x^2 : x \in \overline{G}\} \leq \overline{G}$ ist $2^s = |\overline{G}/\overline{G}_2| = 2^{s'}$ und $s = s'$.

(ii) Ist $d = p_1^{a_1} \ldots p_k^{a_k}$ die Primfaktorzerlegung von d, so gilt $C_d \cong C_{p_1^{a_1}} \times \ldots \times C_{p_k^{a_k}}$ nach Bemerkung 2.3. Aus (i) erhält man also die Zerlegung in (ii). Zyklische Gruppen von Primzahlpotenzordnung sind unzerlegbar, da sie nur eine Untergruppe mit Primzahlordnung enthalten. Die Eindeutigkeit der Zerlegung folgt daher aus Krull-Schmidt. □

Beispiel 2.12. 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 2.13.

(i) In der Situation von Satz 2.11 bilden die Elemente endlicher Ordnung von G eine zu $C_{d_1} \times \ldots \times C_{d_t}$ isomorphe Untergruppe, die man den *Torsionsteil* von G nennt. 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 2.14. Nach Satz 2.11 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 2.15.

- Eine Gruppe $G \neq 1$ heißt *einfach*, falls 1 und G die einzigen Normalteiler von G sind (vgl. Primzahl).
- Eine *Subnormalreihe* σ von G ist eine Folge von Untergruppe $1 = G_0 \trianglelefteq G_1 \trianglelefteq \ldots \trianglelefteq G_k = G$ (wir verlangen nicht $G_i \trianglelefteq G$). 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*.
- Man nennt G *auflösbar*, falls eine Subnormalreihe mit abelschen Faktoren existiert.

Bemerkung 2.16. Jede endliche Gruppe G besitzt eine Kompositionsreihe, denn man kann die Subnormalreihe $1 \leq G$ stets zu einer Kompositionsreihe verfeinern.

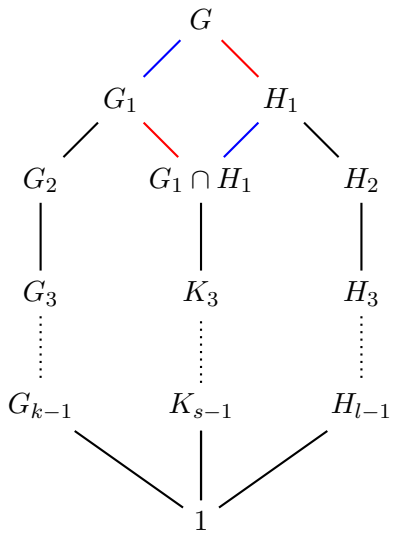
Satz 2.17 (Jordan-Hölder). *Seien* $1 = G_k \trianglelefteq \ldots \trianglelefteq G_0 = G$ *und* $1 = H_l \trianglelefteq \ldots \trianglelefteq H_0 = G$ *Kompositionsreihen einer endlichen Gruppe* G*. Dann ist* $k = l$ *und es existiert ein* $\pi \in S_k$ *mit* $G_{i-1}/G_i \cong H_{\pi(i)-1}/H_{\pi(i)}$ *für* $i = 1, \ldots, k$*. Man nennt* $G_0/G_1, \ldots, G_{k-1}/G_k$ *die* Kompositionsfaktoren *von* G*.*

Beweis. Induktion nach $|G|$: O. B. d. A. sei $G \neq 1$. 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, gilt $G = G_1 H_1$. 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 2.18.

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

(ii) Sei G auflösbar und einfach. Dann ist $1 \leq G$ die einzige Subnormalreihe und $G \cong G/1$ ist abelsch. Für $x \in G \setminus \{1\}$ ist $\langle x \rangle \trianglelefteq G$, also $G = \langle x \rangle$, d. h. G ist zyklisch. Für jeden Teiler d von $|G|$ existiert nach Satz 2.4 ein Normalteiler der Ordnung d. Dies zeigt, dass $|G|$ eine Primzahl ist. Umgekehrt ist C_p für jede Primzahl p einfach.

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

(iv) C_∞ besitzt keine Kompositionsreihe, denn nach (ii) wären die Kompositionsfaktoren endlich.

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

Bemerkung 2.19.

(i) Nach Jordan-Hölder sind die einfachen Gruppen die „Primzahlen“ der endlichen Gruppentheorie. Jede endliche einfache Gruppe gehört zu einer der folgenden Familien:[5]

- C_p (p Primzahl),
- A_n für $n \geq 5$ (Satz 6.33),
- Gruppen vom „Lie-Typ“ ($\mathrm{PSL}(n,q)$, $\mathrm{PSU}(n,q)$, $\ldots, E_8(q)$),
- 26 sporadische Gruppen, deren größte die *Monstergruppe* ist mit ca. 10^{54} Elementen.

Der Beweis dieser Klassifikation 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.[6]

(ii) 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 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 gibt es 49.487.367.289 Gruppen der Ordnung 2^{10} mit den gleichen Kompositionsfaktoren (C_2 mit Vielfachheit 10). Das Erweiterungsproblem ist im Allgemeinen noch ungelöst.[7]

Definition 2.20. 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*. Nach Aufgabe 10 sind die Faktoren einer Hauptreihe bis auf Isomorphie und Reihenfolge eindeutig bestimmt sind. Dies sind die *Hauptfaktoren* von G.

Beispiel 2.21. Die Normalreihe $1 \triangleleft V_4 \triangleleft A_4$ ist eine Hauptreihe von A_4, aber keine Kompositionsreihe, da $V_4 \cong C_2^2$ nicht einfach ist.

Lemma 2.22. *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

$$(G_i \cap H)/(G_{i-1} \cap H) = (G_i \cap H)/((G_i \cap H) \cap G_{i-1}) \cong (G_i \cap H)G_{i-1}/G_{i-1} \leq G_i/G_{i-1}.$$

Also ist H auflösbar. Insbesondere ist auch N auflösbar. Außerdem gilt $1 = G_0N/N \trianglelefteq \ldots \trianglelefteq G_kN/N = G/N$ mit

$$\begin{aligned}(G_iN/N)/(G_{i-1}N/N) &\cong G_iN/G_{i-1}N = G_i(G_{i-1}N)/G_{i-1}N \cong G_i/(G_i \cap G_{i-1}N) \\ &\cong (G_i/G_{i-1})/((G_i \cap G_{i-1}N)/G_{i-1}).\end{aligned}$$

Somit ist auch G/N auflösbar.

[5] Die nichtabelschen einfachen Gruppen der Ordnung $\leq 10^6$ sind Tabelle 2 gelistet.

[6] Aktueller Stand: [Solomon, *The Classification of Finite Simple Groups: A Progress Report*, Notices of the AMS 65 (2018), 646–651, `https://www.ams.org/journals/notices/201806/rnoti-p646.pdf`]

[7] Ein „Periodensystem“ der einfachen Gruppen findet man hier.

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 2.23.

(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 2.24. 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 2.25.

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

(ii) Nach Aufgabe 12 ist $\mathrm{Z}(G)$ charakteristisch in G.

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

(iv) Nach Bemerkung 2.14 ist $\langle (1,2) \rangle$ normal aber nicht charakteristisch in $\langle (1,2), (3,4) \rangle \cong C_2^2$.

Lemma 2.26. *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 2.27. *Eine endliche Gruppe G ist genau dann charakteristisch einfach, wenn G eine 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 $\alpha(N) \cap \widetilde{N} \trianglelefteq G$ 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 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 $\alpha(N) \leq \mathrm{C}_G(N) \subseteq \mathrm{N}_G(M)$ 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 nach Bemerkung 2.14. 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 $1 \neq x_1 \dots x_k \in H$ mit $x_i \in N_i$ für $i = 1, \dots, k$. 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

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

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 $i = 1, \dots, k$. Dies zeigt $N_i \leq H$ für $i = 1, \dots, k$, d. h. $H = G$. Somit ist G charakteristisch einfach. □

Satz 2.28. *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 N/M. Nach Lemma 2.26 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 2.22. Die zweite Behauptung folgt nun aus Satz 2.27. Da man jeden minimalen Normalteiler zu einer Hauptreihe fortsetzen kann, ist auch die dritte Behauptung klar. □

Bemerkung 2.29.

(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 Satz 2.28 haben die Hauptfaktoren von G dann Primzahlordnung, falls $|G| < \infty$. Jede überauflösbare Gruppe ist offenbar auflösbar, aber die Umkehrung ist falsch (Beispiel: A_4). Nach Satz 2.11 sind endlich erzeugte abelsche Gruppen überauflösbar.

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 $[x_1, \dots, x_n] := [x_1, [x_2, \dots, x_n]]$ für $x_1, \dots, x_n \in G$. Für $X, Y \subseteq G$ sei analog

$$[X, Y] := \langle [x, y] : x \in X, y \in Y \rangle,$$
$$[X_1, \dots, X_n] := [X_1, [X_2, \dots, X_n]].$$

Insbesondere ist $G' := G^{(1)} := [G, G]$ die *Kommutatorgruppe* von G. Wir setzen $G'' := (G')'$ und allgemeiner $G^{(k)} := (G^{(k-1)})'$ für $k \geq 2$. Außerdem sei $G^{[1]} := G$ und $G^{[k]} := [G^{[k-1]}, G]$ für $k \geq 2$.[8]

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

[8] Diese Bezeichnung ist in der Literatur nicht einheitlich. Man benutzt auch G^k (Verwechselung mit direktem Produkt), $K_k(G)$ oder $\gamma_k(G)$.

(ii) Für einen Homomorphismus $f\colon G \to H$ 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.

(i) Für $X, Y \leq G$ gilt $[X,Y] \trianglelefteq \langle X, Y\rangle$.

(ii) Für $k \geq 2$ gilt $G^{[k]} = \langle [g_1, \ldots, g_k] : g_1, \ldots, g_k \in G\rangle$.

Beweis.

(i) 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 $Y \leq \mathrm{N}_G([Y,X]) = \mathrm{N}_G([X,Y])$.

(ii) Wir zeigen durch Induktion nach k, dass jedes Element aus $G^{[k]}$ ein Produkt von Kommutatoren der Form $[g_1, \ldots, g_k]$ ist (d. h. man braucht keine Inversen). Der Fall $k = 2$ ist klar wegen $[x,y]^{-1} = [y,x]$. Sei $k \geq 3$, $x \in G^{[k-1]}$ und $y \in G$. Nach Induktion ist x ein Produkt von Kommutatoren $[g_1, \ldots, g_{k-1}]$. Für $x = x_1x_2$ gilt $[x_1x_2, y] = {}^{x_1}[x_2,y][x_1,y] = [{}^{x_1}x_2, {}^{x_1}y][x_1,y]$. Daraus folgt leicht die Behauptung. □

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 $G' \subseteq G_{k-1}$. Nach Induktion existiert ein $l \in \mathbb{N}$ mit $G^{(l+1)} = (G')^{(l)} \subseteq G_{k-1}^{(l)} = 1$.

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.

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

(ii) Für $X, Y, Z \leq G$ gilt $[X,Y,Z] = [X,Z,Y]$, aber nicht unbedingt $[X,Y,Z] = [Y,X,Z]$. Das nächste Lemma gibt eine Beziehung zwischen den Kommutatoren dreier Untergruppen.

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. Es genügt, $[z,x,y]=1$ für $z\in Z$, $x\in X$ und $y\in Y$ zu zeigen. Dafür verifizieren wir die *Hall-Witt-Identität*[9]

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

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 $\mathrm{Z}_i(G)/\mathrm{Z}_{i-1}(G):=\mathrm{Z}(G/\mathrm{Z}_{i-1}(G))$ 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. ist $1=\mathrm{Z}_0(G)<\ldots<\mathrm{Z}_k(G)=G$ 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, falls G endlich ist. Endliche nilpotente Gruppen sind daher sogar überauflösbar. Merke:

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 $l\geq 1$ 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 (wie im obigen Beweis ist $G^{[i+1]}\subseteq \mathrm{Z}_{k-i}(G)$). Die untere und obere Zentralreihe 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 $N=A_3$.

[9] vgl. Jacobi-Identität für Lie-Algebren

Satz 3.11. *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 $N_{i+1} := [G, N_i] \leq N$ 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 letzte Aussage wählen wir $l \geq 1$ maximal mit $N_l \neq 1$. Dann ist $[G, N_l] = N_{l+1} = 1$ und $N_l \subseteq N \cap \mathrm{Z}(G)$. □

Satz 3.12 (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 tritt M mindestens $m + 1$ Mal auf). 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 3.13. Die *Fittinggruppe* $\mathrm{F}(G)$ einer endlichen Gruppe G ist das Produkt aller nilpotenten Normalteiler von G. Nach Satz 3.12 ist $\mathrm{F}(G)$ der größte nilpotente Normalteiler von G (dies entspricht dem auflösbaren Radikal).

Bemerkung 3.14. Offenbar ist $\mathrm{F}(G)$ charakteristisch in G.

Beispiel 3.15. Sei N ein minimaler Normalteiler einer endlichen auflösbaren Gruppe G. Nach Satz 2.28 ist N (elementar)abelsch und daher nilpotent. Dies zeigt $\mathrm{F}(G) \neq 1$. Beispielsweise ist $\mathrm{F}(S_3) = A_3$.

Satz 3.16. *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 $N/\mathrm{Z}(N) \cong \mathrm{F}(\overline{C})/(\mathrm{Z}(N)/\mathrm{Z}(\mathrm{F}(G)))$ 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 2.26. 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 3.17. Für endliche, auflösbare Gruppen G gilt $G/\mathrm{Z}(\mathrm{F}(G)) = \mathrm{N}_G(\mathrm{F}(G))/\mathrm{C}_G(\mathrm{F}(G)) \leq \mathrm{Aut}(\mathrm{F}(G))$ und $G/\mathrm{F}(G) \leq \mathrm{Out}(\mathrm{F}(G))$ nach Satz 3.16.

4 p-Gruppen und die Frattinigruppe

Bemerkung 4.1. Ab jetzt sei G stets eine endliche Gruppe. Bekanntlich existiert nicht zu jedem Teiler d von $|G|$ eine Untergruppe der Ordnung d (A_4 hat keine Untergruppe der Ordnung 6). Ist d jedoch eine Primzahlpotenz, so gibt es Untergruppen der Ordnung d. Diese Tatsache ist von fundamentaler Bedeutung für die Gruppentheorie.

Definition 4.2. 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 4.3 (Sylow)**.** *Sei $|G| = p^a m$ für eine Primzahl $p \nmid m$. Dann gilt:*

(i) G besitzt eine Untergruppe P der Ordnung p^a. Man nennt P eine p-Sylowgruppe *von G. Die Menge der p-Sylowgruppen sei* $\mathrm{Syl}_p(G)$.

(ii) Jede Untergruppe der Ordnung p^b von G ist in einer p-Sylowgruppe enthalten.

(iii) Je zwei p-Sylowgruppen von G sind konjugiert.

(iv) Für $P \in \mathrm{Syl}_p(G)$ gilt $\boxed{|\mathrm{Syl}_p(G)| = |G : \mathrm{N}_G(P)| \equiv 1 \pmod p.}$

Beweis.

(i) Induktion nach $|G|$: Für $G = 1$ ist $P = 1$ eine p-Sylowgruppe (mit $a = 0$). Sei also $G \neq 1$. Nehmen wir zunächst an, dass $|\mathrm{Z}(G)|$ durch p teilbar ist. Nach dem Hauptsatz über endlich erzeugte abelsche Gruppen existiert eine Untergruppe $Z \leq \mathrm{Z}(G)$ mit $|Z| = p^b \neq 1$. Nach Induktion besitzt G/Z eine p-Sylowgruppe P/Z. Wegen $|P| = |P/Z||Z| = p^{a-b+b} = p^a$ ist $P \in \mathrm{Syl}_p(G)$.

Sei nun $|\mathrm{Z}(G)| \not\equiv 0 \pmod p$. Die (verfeinerte) Klassengleichung (1.1) liefert ein $x \in G \setminus \mathrm{Z}(G)$ mit $p \nmid |G : \mathrm{C}_G(x)|$. Wegen $x \notin \mathrm{Z}(G)$ ist $\mathrm{C}_G(x) < G$ und nach Induktion existiert $P \in \mathrm{Syl}_p(\mathrm{C}_G(x))$. Offenbar ist dann auch $P \in \mathrm{Syl}_p(G)$.

(ii) Sei $U \leq G$ mit $|U| = p^b$. Die Bahnenlängen der Operation von U auf G/P durch Linksmultiplikation (siehe Aufgabe 6) sind dann Teiler von p^b, also p-Potenzen. Wegen $p \nmid m = |G : P|$ existiert ein Fixpunkt $xP \in G/P$ von U, d. h. $Ux \subseteq UxP = xP$ und $U \subseteq xPx^{-1}$. Als Bild von P unter einem inneren Automorphismus ist $xPx^{-1} \in \mathrm{Syl}_p(G)$.

(iii) Dies folgt aus dem Beweis von (ii).

(iv) Nach (iii) operiert G transitiv auf $\mathrm{Syl}_p(G)$ durch Konjugation. Der Stabilisator von P ist $\mathrm{N}_G(P)$. Also folgt $|\mathrm{Syl}_p(G)| = |G : \mathrm{N}_G(P)|$ aus Satz 1.20. Für die Kongruenz betrachten wir die Operation von P auf $\mathrm{Syl}_p(G)$ durch Konjugation. Sei $Q \in \mathrm{Syl}_p(G)$ ein Fixpunkt, d. h. $P \leq \mathrm{N}_G(Q)$. Wegen $P, Q \in \mathrm{Syl}_p(\mathrm{N}_G(Q))$ existiert nach (iii) ein $x \in \mathrm{N}_G(Q)$ mit $P = xQx^{-1} = Q$. Also besitzt P genau einen Fixpunkt auf $\mathrm{Syl}_p(G)$ und die Bahnengleichung zeigt $|\mathrm{Syl}_p(G)| \equiv 1 \pmod p$. □

Folgerung 4.4 (Cauchy)**.** *Für jeden Primteiler p von $|G|$ besitzt ein Element der Ordnung p.*

Beweis. Man wähle $1 \neq x \in P \in \mathrm{Syl}_p(G)$. Nach Lagrange ist $|\langle x\rangle| = p^n$ mit $n \geq 1$. Nach Lemma 2.1 hat $y := x^{p^{n-1}} \in G$ Ordnung p. □

Beispiel 4.5.

(i) Seien $p < q$ Primzahlen mit $q \not\equiv 1 \pmod{p}$ (zum Beispiel $pq = 15$). Sei G eine Gruppe der Ordnung pq. Nach Sylow ist $|\mathrm{Syl}_p(G)|$ ein Teiler von pq und gleichzeitig kongruent zu 1 modulo p. Dies zeigt $|\mathrm{Syl}_p(G)| = 1$ und analog $|\mathrm{Syl}_q(G)| = 1$. Sei $P \in \mathrm{Syl}_p(G)$ und $Q \in \mathrm{Syl}_q(G)$. Dann sind $P, Q \trianglelefteq G$ (sogar charakteristisch) und $P \cap Q = 1$ nach Lagrange. Wegen $|PQ| = |P||Q| = pq = |G|$ ist $G = P \oplus Q \cong C_p \times C_q \cong C_{pq}$ (alternatives Argument: Wegen $|P \cup Q| = p + q - 1 < pq$ muss G Elemente der Ordnung pq besitzen).

(ii) In der Algebra zeigt man, dass alle Gruppen der Ordnung < 60 auflösbar sind. Ein „schwieriger" Fall ist $|G| = 30 = 2 \cdot 3 \cdot 5$. Man kann hier induktiv annehmen, dass G einfach ist. Nach Sylow gilt dann $\mathrm{Syl}_5(G) = \{P_1, \ldots, P_6\}$. Wegen $|P_1 \cup \ldots \cup P_6| = 1 + 6 \cdot 4 = 25$ ist nur noch Platz für höchstens zwei 3-Sylowgruppen. Nach Sylow folgt $|\mathrm{Syl}_3(G)| = 1$ im Widerspruch zur Einfachheit von G.

Bemerkung 4.6.

(i) Nach Lagrange und Cauchy ist G genau dann eine π-Gruppe, falls jeder Primteiler von $|G|$ in π liegt. Insbesondere ist die Ordnung einer p-Gruppe eine Potenz von p. Allerdings lässt sich diese Charakterisierung von π-Gruppen nicht auf unendliche Gruppe ausdehnen.

(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 $\mathrm{O}_p(G)$. Für $H \leq G$ ist $H \cap \mathrm{O}_\pi(G)$ ein π-Normalteiler von H und es folgt $H \cap \mathrm{O}_\pi(G) \leq \mathrm{O}_\pi(H)$.

(iii) 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 $PN/N \in \mathrm{Syl}_p(G/N)$.

(iv) 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 4.7. *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 4.8. Aus statistischer Sicht sind fast alle Gruppen p-Gruppen. Unter den Gruppen der Ordnung ≤ 2000 haben beispielsweise über 99% die Ordnung 2^{10} (siehe Tabelle 1). Die Anzahl der Gruppen der Ordnung 2^{11} ist unbekannt (siehe Bemerkung 2.19).

Satz 4.9. *Die folgenden Aussagen sind äquivalent:*

(1) G ist nilpotent.

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

(3) Jede maximale Untergruppe von G ist normal.

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

(5) G ist die direkte Summe seiner Sylowgruppen.

Beweis.

(1)⇒(2): Satz 3.11.

(2)⇒(3): Trivial.

(3)⇒(4): 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 (3) ist $H \trianglelefteq G$. Aus Bemerkung 4.6 folgt nun der Widerspruch $G = H\mathrm{N}_G(P) = H$.

(4)⇒(5): 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 $G = P_1 \oplus \ldots \oplus P_n$.

(5)⇒(1): Nach Satz 4.7 ist jede Sylowgruppe nilpotent und daher auch G (Satz 3.12). □

Satz 4.10. *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 4.9 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 2.26 ist also $Q_i \trianglelefteq G$ und somit $Q_i \leq \mathrm{O}_{p_i}(G)$. □

Definition 4.11. Die *Frattinigruppe* $\Phi(G)$ ist der Durchschnitt aller maximalen Untergruppen von G.[10] Für $G = 1$ setzt man $\Phi(G) = 1$.

Bemerkung 4.12. Für $G \neq 1$ ist sicher $\Phi(G) < G$. Außerdem ist $\Phi(G)$ charakteristisch in G.

Lemma 4.13. *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 $N \not\subseteq \Phi(G)$ existiert eine maximale Untergruppe $M < G$ mit $N \not\subseteq M$ 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. □

[10] vgl. Jacobson-Radikal in der Ringtheorie

Satz 4.14 (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 4.6 ist $G = \Phi(G)\mathrm{N}_G(P)$ und Lemma 4.13 zeigt $G = \mathrm{N}_G(P)$, d. h. $P \trianglelefteq G$. Dann ist auch $P \trianglelefteq \Phi(G)$ und die Behauptung folgt aus Satz 4.9.

(ii) Für $P \in \mathrm{Syl}_p(G)$ ist $P\Phi(G)/\Phi(G) \in \mathrm{Syl}_p(G/\Phi(G))$. Nach Satz 4.9 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 4.6. Lemma 4.13 zeigt nun $G = \mathrm{N}_G(P)$ und $P \trianglelefteq G$. Die Behauptung folgt mit Satz 4.9.

(iii) Ist $D := G' \cap \mathrm{Z}(G) \nsubseteq \Phi(G)$, so existiert eine maximale Untergruppe $M < G$ mit $D \nsubseteq M$, 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 4.15 (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 4.9). 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 4.14. □

Satz 4.16. *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 4.17 (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. □

Satz 4.18. *Sei* $\alpha \in \mathrm{Aut}(G)$ *mit* $\mathrm{ggT}(|\langle\alpha\rangle|, |\Phi(G)|) = 1$ *und* $\alpha(x) \equiv x \pmod{\Phi(G)}$ *für alle* $x \in G$. *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 4.17. Dies zeigt $P' = \Phi(P)$. Nach Satz 3.11 ist $P' \leq \mathrm{Z}(P)$ und nach Aufgabe 7 ist $P/\mathrm{Z}(P)$ nicht zyklisch. Also gilt $P' = \Phi(P) = \mathrm{Z}(P)$. 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

$$|\mathrm{GL}(2,p)| = (p^2 - 1)(p^2 - p) = (p-1)^2 p(p+1)$$

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* $p^n q$ *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 (Lemma 2.22). 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 $N := \mathrm{N}_G(D)$. 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 4.9. 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 $G = PT$. 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 $K := D^G = \langle gDg^{-1} : g \in G \rangle \leq P$ und $K \trianglelefteq G$. Nach Wahl von G sind K und G/K auflösbar. Also ist auch G auflösbar. □

5 Komplemente und Hallgruppen

Bemerkung 5.1. Als Verallgemeinerung von Sylow zeigen wir, dass in auflösbaren Gruppen G stets eine Untergruppe der Ordnung d existiert, sofern d und $|G|/d$ teilerfremd sind. Für überauflösbare Gruppen existiert sogar für jeden Teiler d von $|G|$ eine Untergruppe der Ordnung d.

Definition 5.2. Sei $N \leq G$. Eine Untergruppe $H \leq G$ mit $G = NH$ und $H \cap N = 1$ nennt man *Komplement* von N in G.

Bemerkung 5.3.

(i) In diesem Kapitel interessieren wir uns nur für den Fall $N \trianglelefteq G$.

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

(iii) 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 $(x')^{-1}x = h'h^{-1} \in N \cap H = 1$.

Beispiel 5.4.

(i) Sei K ein Komplement von $N \trianglelefteq G$ und $N \leq H \leq G$. Dann ist $H \cap K$ ein Komplement von N in H, denn $(H \cap K)N = H \cap KN = H$. Ist $M \trianglelefteq G$ mit $M \leq N$, so ist KM/M ein Komplement von N/M, denn $N \cap KM = (N \cap K)M = M$ nach Dedekind.

(ii) In einer direkten Summe $N \oplus M$ ist N ein Komplement von M und umgekehrt. Nach Bemerkung 2.8 sind Komplemente also im Allgemeinen nicht eindeutig bestimmt.

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

(iv) Nach Satz 4.9 hat jede Sylowgruppe einer nilpotenten Gruppe ein Komplement.

(v) Nach Aufgabe 22 hat jeder vollständige Normalteiler ein Komplement.

(vi) S_2 ist ein Komplement von A_3 in S_3.

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

Bemerkung 5.5. Im Folgenden betrachten wir Homomorphismen der Form $G \to \mathrm{Aut}(H)$, wobei G und H Gruppen sind. Wegen $\mathrm{Aut}(H) \leq \mathrm{Sym}(H)$ operiert dann G auf H. Für $g \in G$ und $x, y \in H$ gilt dabei ${}^g(xy) = ({}^gx)({}^gy)$.

Lemma 5.6. *Sei $\varphi\colon H \to \mathrm{Aut}(N)$ 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

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

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

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

Definition 5.7. Man nennt G das *semidirekte Produkt* von N mit H und schreibt $G = N \rtimes_\varphi H$.

Bemerkung 5.8.

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

(ii) 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 $\varphi\colon H \hookrightarrow \mathrm{Aut}(N)$.

(iii) Ist φ trivial, so ist offensichtlich $N \rtimes_\varphi H \cong N \times H$. Sei nun φ nicht-trivial. Dann existieren $h \in H$ und $x \in N$ mit ${}^h x \neq x$. Es folgt $(x,1)*(1,h) = (x,h) \neq ({}^h x, h) = (1,h)*(x,1)$. Ist besondere ist G nichtabelsch.

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

Lemma 5.9. *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 $\varphi\colon H \to \mathrm{Aut}(N)$ die Konjugationsabbildung. Wir zeigen, dass die Abbildung

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

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

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

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

Sei nun $G := N \rtimes_\varphi H$. Dann ist die Projektion $G \to H$, $(x,h) \mapsto h$ ein Epimorphismus mit Kern $\widetilde{N} := \{(x,1) : x \in N\} \trianglelefteq G$. Außerdem ist $N \to \tilde{N}$, $x \mapsto (x,1)$ ein Isomorphismus. Analog ist $H \to G$, $h \mapsto (1,h)$ ein Monomorphismus mit Bild $\widetilde{H} := \{(1,h) : h \in H\} \leq G$. Offenbar gilt $\widetilde{N} \cap \widetilde{H} = 1$ und $G = \widetilde{N}\widetilde{H}$. $\square$

Beispiel 5.10.

(i) Nach Aufgabe 4 besitzt jede abelsche Gruppe A den Automorphismus $x \mapsto x^{-1}$ $(x \in A)$. Ist $\varphi\colon C_2 \to \mathrm{Aut}(A)$ 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 $2n$ (vgl. Aufgabe 9). Offenbar ist dann φ nicht-trivial und D_{2n} ist nichtabelsch. Andererseits ist $D'_{2n} \leq C_n$ und D_{2n} ist metabelsch.

(ii) Nach Aufgabe 22 gibt es einen Isomorphismus $\varphi\colon S_3 \to \mathrm{Aut}(S_3)$ mit $S_3 \rtimes_\varphi S_3 \cong S_3 \times S_3$. Semidirekte Produkte lassen sich also nicht ohne Weiteres durch die entsprechenden Homomorphismen klassifizieren.

Satz 5.11. *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* $G \cong C_q \rtimes C_p$ *ist nichtabelsch.*

Beweis. Im Fall $p = q$ ist G abelsch zum Beispiel nach Satz 4.17. Dann folgt die Behauptung aus Satz 2.11. Sei nun also G nichtabelsch und $p < q$. Nach Beispiel 4.5 ist $q \equiv 1 \pmod{p}$ und G besitzt eine normale q-Sylowgruppe Q. Offenbar ist $P \in \mathrm{Syl}_p(G)$ ein Komplement von Q, d. h. $G = Q \rtimes P$. Wegen $\mathrm{Aut}(Q) \cong C_{q-1}$ existiert ein nicht-trivialer Homomorphismus $\varphi\colon P \to \mathrm{Aut}(Q)$. Daher existiert eine solche Gruppe auch. Nach Aufgabe 23 ist der Isomorphietyp dieser Gruppe durch p und q eindeutig bestimmt. □

Beispiel 5.12. Bis auf Isomorphie sind C_{21} und $C_7 \rtimes C_3$ die einzigen Gruppen der Ordnung 21.

Bemerkung 5.13. Im Folgenden untersuchen wir, wann ein fest gewählter Normalteiler ein Komplement besitzt. Jedes Komplement von $H \leq G$ ist offenbar ein Repräsentantensystem für G/H. Wir werden umgekehrt Komplemente konstruieren, indem wir beliebige Repräsentantensysteme „glätten“.

Definition 5.14. Sei $N \trianglelefteq G$ abelsch und $\mathcal{R}$ die Menge der Repräsentantensysteme für G/N. Für $R, S \in \mathcal{R}$ definieren wir

$$(R|S) := \prod_{\substack{(r,s)\in R\times S,\\ rN=sN}} rs^{-1}K \in N$$

(da N abelsch ist, spielt die Reihenfolge der Faktoren keine Rolle).

Lemma 5.15. *Für $R, S, T \in \mathcal{R}$, $g \in G$ und $x \in N$ gilt:*

(i) $(R|R) = 1$ *und* $(R|S)^{-1} = (S|R)$.

(ii) $(R|S)(S|T) = (R|T)$.

(iii) $gR, gS \in \mathcal{R}$ *und* $(gR|gS) = g(R|S)g^{-1}$.

(iv) $(xR|S) = x^{|G/N|}(R|S)$.

Beweis.

(i) Die Gleichung $(R|R) = 1$ ist trivial. Außerdem ist

$$(R|S)^{-1} = \prod_{\substack{(r,s)\in R\times S,\\ rN=sN}} sr^{-1} = \prod_{\substack{(s,r)\in S\times R,\\ sN=rN}} sr^{-1}K = (S|R).$$

(ii) Es gilt

$$(R|S)(S|T) = \prod_{\substack{(r,s)\in R\times S\\ rN=sN}} rs^{-1} \prod_{\substack{(s,t)\in S\times T\\ sN=tN}} st^{-1} = \prod_{\substack{(r,t)\in R\times T\\ rN=tN}} rt^{-1} = (R|T).$$

(iii) Wegen $|gR| = |R|$ und $(gR)N = gRN = gG = G$ gilt $gR \in \mathcal{R}$ und analog $gS \in \mathcal{R}$. Außerdem ist

$$(gR|gS) = \prod_{\substack{(gr,gs)\in gR\times gS\\ grN=gsN}} grs^{-1}g^{-1} = g(R|S)g^{-1}.$$

(iv) Da N abelsch ist, gilt

$$(xR|S) = \prod_{\substack{(r,s)\in R\times S,\\ rN=xrN=sN}} xrs^{-1} = x^{|G/N|} \prod_{\substack{(r,s)\in R\times S,\\ rN=sN}} xrs^{-1} = x^{|G/N|}(R|S). \qquad \square$$

Satz 5.16 (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 4.6 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 4.7 und Lemma 2.26 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.

Wir benutzen nun Lemma 5.15. Durch

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

wird eine Äquivalenzrelation auf $\mathcal{R}$ definiert. Sei $\overline{R}$ die Äquivalenzklasse von R und $\overline{\mathcal{R}} := \{\overline{R} : R \in \mathcal{R}\}$. Nach Lemma 5.15 operiert G durch Linksmultiplikation auf $\mathcal{R}$. Wegen $(gR|gS) = g(R|S)g^{-1}$ werden Äquivalenzklassen auf Äquivalenzklassen abgebildet. Daher operiert G auch auf $\overline{\mathcal{R}}$ durch ${}^g\overline{R} := \overline{{}^gR}$. Wir zeigen, dass N transitiv auf $\overline{\mathcal{R}}$ 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 $x := (R, S)^{-n} \in N$. Nach Lemma 5.15 gilt $(xR|S) = x^{|G/N|}(R|S) = (R|S)^{1-n|G/N|} = 1$. Dies zeigt ${}^x\overline{R} = \overline{S}$ und N ist transitiv. Das Frattini-Argument liefert $G = NG_{\overline{R}}$ 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). Da N transitiv auf $\overline{\mathcal{R}}$ operiert existiert ein $x \in N$ mit $xG_{\overline{R}}x^{-1} = G_{x\overline{R}} = G_{\overline{K}}$ (Bemerkung 1.18(iii)). 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 $K = G_{\overline{K}} = xG_{\overline{R}}x^{-1}$. Sei also $1 < N' < N$. 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 2.28 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 5.17. 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 (Gruppen ungerader Ordnung sind auflösbar) ist die Auflösbarkeitsbedingung in Satz 5.16 also eigentlich überflüssig (der Beweis hat 250 Seiten).

Definition 5.18. 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. Ggf. ist $\mathrm{ggT}(|H|, |G : H|) = 1$.

Beispiel 5.19.

(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 4.9).

(iii) A_5 besitzt *keine* $\{3, 5\}$-Hallgruppe, denn eine solche Hallgruppe wäre zyklisch der Ordnung 15 (Beispiel 4.5). Der folgende Satz impliziert daher, dass A_5 nicht auflösbar ist.

Satz 5.20 (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 $|K| = p^n r$ 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. Nach Induktion sind HM/M und KM/M in G/M 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 5.21.

(i) Man kann umgekehrt zeigen, dass G auflösbar ist, falls p'-Hallgruppen für jeden Primteiler p von $|G|$ existieren. Dies verallgemeinert Burnsides p^aq^b-Satz (siehe Charaktertheorie).

(ii) Gross hat im Fall $2 \notin \pi$ bewiesen, dass je zwei π-Hallgruppen einer beliebigen endlichen Gruppe konjugiert sind. Der Beweis benutzt die Klassifikation der endlichen einfachen Gruppen. Allgemeiner lässt sich die Existenz von π-Hallgruppen an den Kompositionsfaktoren ablesen. Sind beispielsweise alle Kompositionsfaktoren π-Gruppen oder π'-Gruppen (man nennt G dann π-*separabel*), so gelten die Aussagen von Hall für π. Der Beweis benötigt allerdings Schur-Zassenhaus ohne Auflösbarkeitsbedingung (vgl. Bemerkung 5.17).

Satz 5.22. *Sei G überauflösbar der Ordnung n. Dann besitzt G für jeden Teiler d von n eine Untergruppe der Ordnung d.*

Beweis. Induktion nach $|G|$. Sei N ein minimaler Normalteiler von G. Man kann N zu einer Hauptreihe von G ergänzen. Nach Voraussetzung ist $p = |N|$ eine Primzahl und G/N ist ebenfalls überauflösbar. Im Fall $p \mid d$ besitzt G/N nach Induktion eine Untergruppe H/N der Ordnung d/p. Dann ist $|H| = d$. Sei nun $p \nmid d$. Dann besitzt G/N eine Untergruppe H/N der Ordnung d. Nach Schur-Zassenhaus (oder Hall) besitzt N ein Komplement der Ordnung d in H. □

Bemerkung 5.23. Unter folgenden Bedingungen existiert eine Untergruppe $H \leq G$:

G	$\lvert H\rvert$	Begründung
beliebig	Primzahlpotenz	Sylow + Satz 5.22
auflösbar	$\mathrm{ggT}(\lvert H\rvert, \lvert G/H\rvert) = 1$	Hall
überauflösbar	$\lvert H\rvert \mid \lvert G\rvert$	Satz 5.22

Satz 5.24 (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. Nach Satz 3.11 ist $1 \neq \mathrm{Z}(M) \cap N \trianglelefteq G$. Da N minimal ist, folgt $N \subseteq \mathrm{Z}(M)$ 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 4.6. Offenbar ist $\mathrm{N}_N(Q) = \mathrm{N}_G(Q) \cap N \trianglelefteq \mathrm{N}_G(Q)$. Da N abelsch ist, gilt auch $\mathrm{N}_N(Q) \trianglelefteq N$. Insgesamt ist also $\mathrm{N}_N(Q) \trianglelefteq G$. Die Minimalität von N zeigt $\mathrm{N}_N(Q) \in \{1, N\}$. 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 $Q \subseteq \mathrm{C}_G(N) = N$ (Lemma 2.5). Widerspruch. Also ist $\mathrm{N}_N(Q) = 1$ 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 $f\colon G \to \mathrm{Sym}(\Omega)$. 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 $f\colon G \to \mathrm{Sym}(\Omega)$ eine beliebige Operation, so wird $G/\mathrm{Ker}(f)$ zu einer Permutationsgruppe.

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

Beweis. Wir betrachten die Operation $f\colon G \to \mathrm{Sym}(G)$ durch Linksmultiplikation. Für $x \in \mathrm{Ker}(f)$ 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*

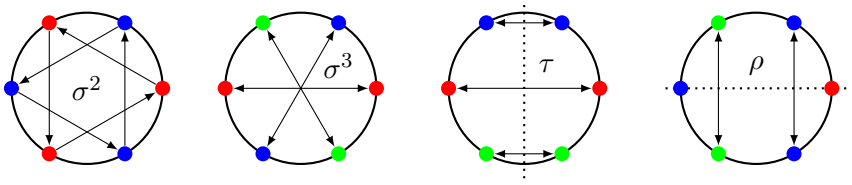
$$s = \frac{1}{|G|} \sum_{g \in G} f(g).$$

Beweis. Im Fall $s = \infty$ ist auch $f(1) = |\Omega| = \infty$ und die Gleichung gilt. Sei also $s < \infty$. Seien $\omega_1, \ldots, \omega_s$ Repräsentanten für die Bahnen von G. 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. Wir wollen Halsketten mit sechs Perlen zählen, wobei Perlen in drei Farben zur Verfügung stehen. Naiverweise gibt es zunächst 3^6 solche Halsketten, von denen jedoch einige identisch sind. Wir ordnen die Halskette so an, dass die Perlen ein regelmäßiges 6-Eck bilden. Rotation um $\pi/3$ wird die Halskette nicht verändern. Ebenso können wir die Halskette im Raum drehen und dadurch eine Spiegelung der 6 Eckpunkte realisieren. Zwei Halsketten sind also genau dann identisch, wenn sie in der gleichen Bahn unter der Diedergruppe $G := D_{12}$ liegen (siehe Aufgabe 9). Wir wenden Burnsides Lemma auf die Menge Ω der 3^6 Halsketten an.

Sicher ist $f(1) = 3^6$. Eine Drehung $\sigma \in G$ um $\pi/3$ lässt nur die drei einfarbigen Halsketten fest, d. h. $f(\sigma) = 3$. Die Drehung σ^2 um $2\pi/3$ lässt die einfarbigen Halsketten und die Halsketten mit alternierenden Farben fest. Davon gibt es $f(\sigma^2) = 3^2$ Stück. Analog zeigt man $f(\sigma^3) = 3^3$. Außerdem ist $f(\sigma^4) = f(\sigma^{-2}) = 3^2$, $f(\sigma^5) = f(\sigma^{-1}) = 3$ sowie $\sigma^6 = 1$. Sei nun τ eine der drei Spiegelungen durch zwei Seitenmittelpunkte. Dann ist $f(\tau) = 3^3$. Ist schließlich ρ eine der drei Spiegelungen durch zwei Eckpunkte, so gilt $f(\rho) = 3^4$.



Nach Burnsides Lemma gibt es

$$\begin{aligned}\frac{1}{12}\big(3^6 + 2\cdot 3 + 2\cdot 3^2 + 3^3 + 3\cdot 3^3 + 3\cdot 3^4\big) &= \frac{1}{4}\big(3^4(3+1) + 3^2(1+3) + 2 + 6\big)\\ &= 81 + 9 + 2 = 92\end{aligned}$$

verschiedene Halsketten.

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*, falls es eine Bijektion $\varphi\colon \Omega \to \Omega'$ mit ${}^g\varphi(\omega) = \varphi({}^g\omega)$ für $g \in G$ und $\omega \in \Omega$ gibt. Ggf. sind Ω und Ω' *isomorphe G-Mengen*.

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 $f\colon G \to \mathrm{Sym}(\Omega)$. 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 1.20 ist die Abbildung $\varphi\colon \Delta \to \Omega$, $gG_{\omega_i} \mapsto {}^g\omega_i$ 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 $f\colon G \to \mathrm{Sym}(\Omega)$ 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 $f\colon G \to \mathrm{Sym}(\Omega)$ 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 $\Delta \subseteq \{1, \ldots, n\}$ 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).

Lemma 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.

(i) 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 (auf einer Bahn von Ω) 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.

(ii) Sei G eine einfache Gruppe und $M < G$ eine maximale Untergruppe. Nach Aufgabe 6 und Lemma 6.16 operiert G treu und primitiv auf G/M (M ist der Stabilisator der trivialen Nebenklasse). Kennt man alle maximalen Untergruppen von einfachen Gruppen, so kann man mit dem Satz von Aschbacher-O'Nan-Scott alle primitiven Permutationsgruppen klassifizieren. Zum Beispiel ist jede primitive Permutationsgruppe vom Grad 34 zu A_{34} oder S_{34} isomorph.[11] Die Bestimmung der maximalen Untergruppe der Monstergruppe (und damit aller sporadischen Gruppen) wurde 2023 abgeschlossen.[12] Im Folgenden beschreiben wir die primitiven auflösbaren Gruppen.

[11] Siehe Tabelle 3 und OEIS

[12] siehe arXiv:2304.14646; zur Geschichte: Wilson's blog

Lemma 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 $\varphi\colon N \to \Omega$, $x \mapsto {}^x\omega$ eine Bijektion. Für $g \in G_\omega$ und $x \in N$ gilt ${}^g\varphi(x) = {}^{gx}\omega = {}^{(gxg^{-1})g}\omega = {}^{gxg^{-1}}\omega = \varphi({}^g x)$. □

Lemma 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 $A := N^{(k)} > N^{(k+1)} = 1$ (wobei $N^{(0)} := N$). Dann ist A abelsch und charakteristisch in N. Also ist $A \trianglelefteq G$. Nach Lemma 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 dem Frattini-Argument 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, d. h. 1 und A sind die einzigen G_ω-invarianten Unterräume 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 $\varphi\colon G \to \mathrm{Sym}(G/H)$ durch Linksmultiplikation. Für $x \in \mathrm{Ker}(\varphi)$ gilt $H = 1H = xH$ und $x \in H$. Somit ist $\mathrm{Ker}(\varphi) \subseteq H$ (vgl. Aufgabe 6). 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 Lemma 6.16 beweisen, dass H maximal in G ist. Sei also $H < M \leq G$. Dann ist $1 \neq M \cap V \trianglelefteq M$, denn

$$|M : M \cap V| = |MV : V| = |G : V| = |VH : V| = |H|.$$

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.

(i) Sei $V \cong C_p^n$. Nach linearer Algebra operiert $\mathrm{GL}(n,p)$ irreduzibel auf V. Daher ist die *affine Gruppe*

$$\mathrm{AGL}(n,p) := V \rtimes \mathrm{GL}(n,p)$$

primitiv vom Grad p^n. Für $p = n = 2$ erhält man $\mathrm{AGL}(2,2) \cong V_4 \rtimes S_3 \cong S_4$, denn S_4 ist die größte Permutationsgruppe vom Grad 4 und $|\mathrm{AGL}(2,2)| = 24$. 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 $f_\gamma \colon V \to V$, $v \mapsto \gamma v$ sicher linear und bijektiv. Also gibt es einen Monomorphismus $f \colon \mathbb{F}_{p^n}^\times \to \mathrm{Aut}(V) \cong \mathrm{GL}(n,p)$, $\gamma \mapsto f_\gamma$ 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 $V \setminus \{0\}$. Daher ist S irreduzibel und $V \rtimes S$ ist eine primitive Permutationsgruppe. Man nennt S *Singer-Zyklus*. Im Fall $n = 1$ ist sicher $V \rtimes S = \mathrm{AGL}(1,p) \cong C_p \rtimes C_{p-1}$. Für $p = n = 2$ erhält man $V_4 \rtimes C_3 \cong A_4$ (die einzige Untergruppe mit Index 2 in S_4).

(ii) Satz 6.21 zeigt, dass es keine primitive auflösbare Gruppe vom Grad 6 gibt. Insbesondere ist A_6 nicht auflösbar.

Definition 6.24. Seien G, H Gruppen und $\varphi \colon G \to \mathrm{Sym}(\Omega)$ eine Operation. Wie üblich ist $H^\Omega := \{f \colon \Omega \to H\}$ eine Gruppe mit $(ff')(\omega) := f(\omega)f'(\omega)$ für $f, f' \in H^\Omega$ und $\omega \in \Omega$ (es gilt $H^\Omega \cong H^{|\Omega|}$). Offenbar operiert G auf H^Ω durch $({}^g f)(\omega) := f({}^{g^{-1}}\omega)$ (nachrechnen). Wegen

$$({}^g(ff'))(\omega) = (ff')({}^{g^{-1}}\omega) = f({}^{g^{-1}}\omega)f'({}^{g^{-1}}\omega) = ({}^g f)(\omega)({}^g f')(\omega)$$

erhält man einen Homomorphismus $\psi \colon G \to \mathrm{Aut}(H^\Omega)$. Man nennt

$$H \wr_\varphi G := H^\Omega \rtimes_\psi G$$

das *Kranzprodukt* von H und G bzgl. Ω.

Bemerkung 6.25.

(i) Ist $G \leq \mathrm{Sym}(\Omega)$ und $\varphi \colon G \to \mathrm{Sym}(\Omega)$ die Inklusionsabbildung, so schreiben wir $H \wr G := H \wr_\varphi G$. Man spricht dann vom *Standardkranzprodukt*.

(ii) Im Fall $\Omega = \{1, \ldots, n\}$ identifizieren wir H^Ω mit H^n. Für Elemente $(h_1, \ldots, h_n, g), (h'_1, \ldots, h'_n, g') \in H \wr G$ gilt dann

$$(h_1, \ldots, h_n, g) * (h'_1, \ldots, h'_n, g') = (h_1 h'_{{}^{g^{-1}}1}, \ldots, h_n h'_{{}^{g^{-1}}n}, gg').$$

Außerdem ist $|H \wr_\varphi G| = |H|^n |G|$.

Satz 6.26. *Sei G eine imprimitive Permutationsgruppe auf Ω mit Block Δ. Sei $H := \{g \in G : {}^g\Delta = \Delta\}$ und sei $\varphi \colon H \to \mathrm{Sym}(\Delta)$ die Operation auf Δ. Sei $\Gamma := \{{}^g\Delta : g \in G\}$ und sei $\psi \colon G \to \mathrm{Sym}(\Gamma)$ die Operation auf Γ. Dann ist G zu einer Untergruppe von $\varphi(H) \wr \psi(G)$ isomorph.*

Beweis. Sei $\Gamma = \{\Delta = \Delta_1, \ldots, \Delta_n\}$. Wir wählen $g_i \in G$ mit ${}^{g_i}\Delta_i = \Delta$ für $i = 1, \ldots, n$. Für $x \in G$ sei ${}^{x}\Delta_i = \Delta_{x(i)}$. Dann ist

$${}^{g_i x g_{x^{-1}(i)}^{-1}}\Delta = {}^{g_i x}\Delta_{x^{-1}(i)} = {}^{g_i}\Delta_i = \Delta,$$

also $g_i x g_{x^{-1}(i)}^{-1} \in H$. Wir definieren $f_x \in \varphi(H)^\Gamma$ durch $f_x(\Delta_i) := \varphi(g_i x g_{x^{-1}(i)}^{-1})$ und

$$F\colon G \to \varphi(H) \wr \psi(G), \quad x \mapsto (f_x, \psi(x)).$$

Für $x, y \in G$ gilt nun

$$\begin{aligned}(f_x \cdot {}^{x} f_y)(\Delta_i) &= \varphi(g_i x g_{x^{-1}(i)}^{-1}) f_y({}^{x^{-1}}\Delta_i) = \varphi(g_i x g_{x^{-1}(i)}^{-1}) f_y(\Delta_{x^{-1}(i)}) \\ &= \varphi(g_i x g_{x^{-1}(i)}^{-1}) \varphi(g_{x^{-1}(i)} y g_{y^{-1}x^{-1}(i)}^{-1}) = \varphi(g_i x y g_{(xy)^{-1}(i)}^{-1}) = f_{xy}(\Delta_i).\end{aligned}$$

Dies zeigt

$$F(x) * F(y) = (f_x, \psi(x)) * (f_y, \psi(y)) = (f_x \cdot {}^{x} f_y, \psi(x)\psi(y)) = (f_{xy}, \psi(xy)) = F(xy),$$

d. h. F ist ein Homomorphismus. Für $x \in \mathrm{Ker}(F)$ gilt $\psi(x) = 1$, d. h. x operiert trivial auf Γ. Außerdem ist $f_x(\Delta_i) = 1$, d. h. $g_i x g_{x^{-1}(i)}^{-1} = g_i x g_i^{-1}$ operiert trivial auf Δ. Also operiert x trivial auf ${}^{g_i^{-1}}\Delta = \Delta_i$ für $i = 1, \ldots, n$. Insgesamt operiert x trivial auf $\Omega = \Delta_1 \cup \ldots \cup \Delta_n$ und es folgt $x = 1$. Daher ist F injektiv und die Behauptung folgt. □

Beispiel 6.27. Die Diedergruppe $G = D_8$ operiert treu auf der Menge $\Omega := \{1, 2, 3, 4\}$ der vier Ecken eines Quadrats. Zwei diagonal gegenüberliegende Ecken bilden einen Block, sagen wir $\Delta := \{1, 3\}$. Mit den Bezeichnungen aus Satz 6.26 ist $H = \langle (1,3), (2,4) \rangle$ und $\varphi(H) = \langle (1,3) \rangle \cong C_2$. Da G (im Allgemeinen) transitiv auf $\Gamma = \{\Delta, \{2, 4\}\}$ operiert, ist auch $\psi(G) \cong \mathrm{Sym}(\Gamma) \cong C_2$. Satz 6.26 zeigt $D_8 \leq C_2 \wr C_2$. Wegen $|C_2 \wr C_2| = 2^2 \cdot 2 = 8 = |D_8|$ folgt $D_8 \cong C_2 \wr C_2 \cong C_2^2 \rtimes C_2$ (vgl. Aufgabe 35). Nach Beispiel 5.10 ist auch $D_8 \cong C_4 \rtimes C_2$.

Definition 6.28. 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 6.29.

(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 $\{x, y\} = \{1, \ldots, n\} \backslash \{\alpha_1, \ldots, \alpha_k\}$ und $\{x', y'\} = \{1, \ldots, n\} \backslash \{\beta_1, \ldots, \beta_k\}$. 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).

Satz 6.30. *Jede 2-transitive Operation ist primitiv.*

Beweis. Sei $\varphi\colon G \to \mathrm{Sym}(\Omega)$ 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 6.31. *Sei $1 \neq N \trianglelefteq G$ und $\varphi\colon G \to \mathrm{Sym}(N \setminus \{1\})$ 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 2.27 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 $gag^{-1} = a$ und $gbg^{-1} = b$ muss also auch $gcg^{-1} = c$ gelten. Dies zeigt $U = N$ und (iii) folgt. Wäre die Operation 4-transitiv, so wäre $|N \setminus \{1\}| \geq 4$ im Widerspruch zu (iii). □

Beispiel 6.32. Sei $G = S_4$ und $N = V_4$. Bekanntlich operiert N regulär auf $\{1, 2, 3, 4\}$. Nach Lemma 6.19 ist die Operation von $G_4 = S_3$ auf $\{1, 2, 3\}$ isomorph zur Operation von G_4 auf $N \setminus \{1\}$. Daher operieren G_4 und G tatsächlich 3-transitiv auf $N \setminus \{1\}$.

Satz 6.33. *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 Lemma 6.20. Wir argumentieren nun durch Induktion nach n. Sei $n = 5$ (vgl. Beispiel 5.19). 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 dem Frattini-Argument ist $G = NG_n$. Wir können also $G_n \not\subseteq N$ 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 6.29 operiert G_n $(n-3)$-transitiv auf $\Omega \setminus \{n\}$. Nach Lemma 6.19 ist diese Operation isomorph zur Operation auf $N \setminus \{1\}$ durch Konjugation. Satz 6.31 liefert nun $n = 6$ und $|N| = 4$. Dies widerspricht aber $|N| = n$. □

Satz 6.34. *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 6.33 folgt $N \cap A_n \in \{1, A_n\}$. Im zweiten Fall ist $N = A_n$. Im ersten Fall ist $|S_n| = |A_n N| = |A_n||N|$ und $|N| = 2$. Dies widerspricht aber Lemma 6.20. □

Satz 6.35. *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 echten Normalteiler mit Index $\leq 3! = 6$ (Aufgabe 6). 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 6.34), folgt $G \cong A_5$. □

Bemerkung 6.36. 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*).

Aufgaben

Aufgabe 1. Let G be a set with a binary operation $G \times G \to G$, $(x, y) \mapsto xy$ such that the following axioms hold

- $\forall x, y, z \in G : (xy)z = x(yz)$.
- $\exists e \in G : \forall x \in G : ex = x$.
- $\forall x \in G : \exists y \in G : xy = e$.

Show that this does *not* define a group.
Hint: Consider $G = \left\{ \left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 1 \\ 0 & 0 \end{smallmatrix}\right) \right\}$.

Aufgabe 2. Let G be a group. Show:

(a) A non-empty finite subset $H \subseteq G$ is a subgroup if and only if $xy \in H$ for all $x, y \in H$.

(b) Every subgroup of index 2 is normal.

(c) Let $G = \langle X \rangle$ and $H = \langle Y \rangle \leq G$. Then $H \trianglelefteq G$ if and only if $xyx^{-1} \in H$ for all $x \in X \cup X^{-1}$ and $y \in Y$.

Aufgabe 3 $(2+2+2+2+2$ points**).** Let U, V, W be subgroups of a (possibly infinite) group G. Show:

(a) $U \subseteq W \Longrightarrow UV \cap W = U(V \cap W)$.

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

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

(d) $|UV||U \cap V| = |U||V|$ (do not assume that UV is a group).

(e) $|G : U \cap V| \leq |G : U||G : V|$.

Aufgabe 4. Show that for every group G the following assertions are equivalent:

(a) G is abelian.

(b) The map $G \to G$, $x \mapsto x^{-1}$ is an automorphism.

(c) The map $G \to G$, $x \mapsto x^2$ is an endomorphism.

Now let $|G| < \infty$. When is $G \to G$, $x \mapsto x^2$ an automorphism?

Aufgabe 5. For $H \leq G$ we define

$$H^G := \Big\langle \bigcup_{g \in G} gHg^{-1} \Big\rangle,$$
$$H_G := \bigcap_{g \in G} gHg^{-1}.$$

Show:

(a) If $H \leq N \trianglelefteq G$, then $H^G \leq N$. Thus, H^G is the "smallest" normal subgroup containing H.

(b) If $N \trianglelefteq G$ with $N \leq H$, then $N \leq H_G$. Thus, H_G is the "largest" normal subgroup contained in H.

We call H^G the *normal closure* and H_G the *core* of H in G.

Aufgabe 6 $(2+4+2+4+2$ points**).** Let $H \leq G$ be groups with $n := |G : H| < \infty$. Show:

(a) G acts transitively by left multiplication on G/H, i. e. ${}^x(gH) := xgH$ for $x, g \in G$.

(b) The kernel of this action is H_G from Aufgabe 5. In particular, $|G : H_G|$ divides $n!$.

(c) If $|G| < \infty$ and n is the smallest prime divisor of $|G|$, then $H \trianglelefteq G$ (this generalizes Exercise 2(b)).

(d) If $n > 1$, then $\bigcup_{g \in G} gHg^{-1} \neq G$.
Hint: Replacing G by G/H_G, we may assume that $|G| < \infty$.

(e) For $H := \left\{ \left(\begin{smallmatrix} * & * \\ 0 & * \end{smallmatrix}\right) \right\} < G := \mathrm{GL}(2, \mathbb{C})$ we have $G = \bigcup_{g \in G} gHg^{-1}$.
Hint: Similarity of matrices.

Aufgabe 7. Let G be a group. Show:

(a) If $G/\mathrm{Z}(G)$ is cyclic, then G is abelian (i. e. $G/\mathrm{Z}(G) = 1$).

(b) If $\mathrm{Aut}(G)$ is cyclic, then G is abelian and $|\mathrm{Aut}(G)|$ is even unless $G \cong C_2$.

(c) If $\mathrm{Z}(G) = 1$, then $\mathrm{C}_{\mathrm{Aut}(G)}(\mathrm{Inn}(G)) = 1$. In particular, $\mathrm{Z}(\mathrm{Aut}(G)) = 1$.

Aufgabe 8.

(a) Determine the number of abelian groups of order 72 up to isomorphism.

(b) Determine the isomorphism type of $\mathrm{Aut}(C_{24})$.

Aufgabe 9 $(4 + 4 + 2 + 4^*$ points**).** Let $3 \leq n \in \mathbb{N}$ and $\sigma, \tau \colon \mathbb{C} \to \mathbb{C}$ with $\sigma(z) := e^{\frac{2\pi \mathrm{i}}{n}} z$ and $\tau(z) := \overline{z}$ (complex conjugation) for $z \in \mathbb{C}$.

(a) Show $D_{2n} := \langle \sigma, \tau \rangle \leq \mathrm{Sym}(\mathbb{C})$, $\langle \sigma \rangle \trianglelefteq D_{2n}$ and $|D_{2n}| = 2n$.

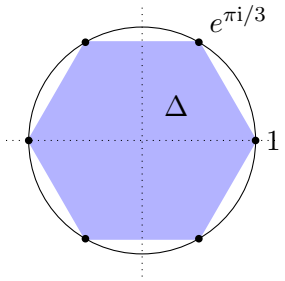
(b) Determine $\mathrm{Z}(D_{2n})$.

(c) Show $D_6 \cong S_3$.

(d) Show that D_{2n} is the symmetry group of the regular n-gon. More precisely, let $\Delta \subseteq \mathbb{C}$ be the convex hall of the n-th roots of unity. Then

$$D_{2n} = \big\{\alpha \colon \mathbb{C} \to \mathbb{C} : \alpha(\Delta) = \Delta,\ |\alpha(x) - \alpha(y)| = |x - y|\ \forall x, y \in \mathbb{C}\big\}.$$

We call D_{2n} the *dihedral group* of order $2n$.



Aufgabe 10. Let G and A be finite groups such that A acts on G via a homomorphism $A \to \mathrm{Aut}(G)$. A subnormal series $1 = N_0 \trianglelefteq \ldots \trianglelefteq N_k = G$ is called *A-invariant* if ${}^a N_i = N_i$ holds for all $i = 1, \ldots, k$ and $a \in A$. An A-invariant subnormal series is called an *A-composition series* if $N_0 < \ldots < N_k$ and the series cannot be refined further as an A-invariant series.

(a) Show that the factors N_i/N_{i-1} of an A-composition series are uniquely determined up to order and isomorphism as in the Jordan-Hölder theorem.
Hint: Follow the proof of Jordan-Hölder.

(b) Conclude that the chief factors of G are uniquely determined up to isomorphism.

Aufgabe 11 $(4 + 4 + 4 + 2$ points**).**

(a) Determine all $n \geq 3$ such that the dihedral group D_{2n} from Exercise 9 is indecomposable.

(b) Construct a group G with $N \trianglelefteq M \trianglelefteq G$ and $N \not\trianglelefteq G$ (this distinguishes subnormal series from normal series).

(c) Find all composition series of S_4.

(d) Determine the chief factors of $S_4 \times D_8$.

Aufgabe 12.

(a) Show that $\mathrm{Z}(G)$ is characteristic in G for every group G.

(b) Determine the normal subgroups and the characteristic subgroups of $S_3 \times S_3$.
Hint: Not every subgroup of a direct product is a direct product.

Aufgabe 13 $(1+1+2+2+2+2$ points$)$**.** Let G be a non-abelian group of order 8. Show:

(a) G contains an element x of order 4.

(b) For $y \in G \setminus \langle x \rangle$ we have $y^4 = 1$ and $yx = x^{-1}y$.

(c) The multiplication table of G is uniquely determined by the order of y.

(d) If $y^2 = 1$, then $G \cong D_8$.

(e) If $y^2 \neq 1$, then

$$G \cong Q_8 := \left\langle \begin{pmatrix} \mathrm{i} & 0 \\ 0 & -\mathrm{i} \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \right\rangle \leq \mathrm{GL}(2, \mathbb{C})$$

with $\mathrm{i} = \sqrt{-1}$. We call Q_8 the *quaternion group* of order 8.
Hint: It suffices to show that Q_8 has the desired properties.

(f) Construct all groups of order 8 up to isomorphism.
Hint: Show $D_8 \ncong Q_8$ by counting involutions.

Aufgabe 14. Let G be a group and $x, y \in G$. Show:

(a) $[x, x, y] = 1$ implies $[x^n, y] = [x, y]^n$ for all $n \in \mathbb{Z}$.

(b) $[x, x, y] = [y, x, y] = 1$ implies $(xy)^n = x^n y^n [y, x]^{\binom{n}{2}}$ for all $n \in \mathbb{N}$.

Aufgabe 15. Determine all $n \geq 3$ such that the dihedral group D_{2n} nilpotent. Compute the nilpotency class in those cases.

Aufgabe 16. Let $G = N \oplus M$ be a finite group. Show $\mathrm{F}(G) = \mathrm{F}(N) \oplus \mathrm{F}(M)$.
Note: Not every subgroup of $N \oplus M$ has the form $N_1 \oplus M_1$ with $N_1 \leq N$ and $M_1 \leq M$.

Aufgabe 17. Let P and Q be distinct Sylow p-subgroups of G such that $|P \cap Q|$ is as large as possible. Show

$$|\mathrm{Syl}_p(G)| \equiv 1 \pmod{|P : P \cap Q|}.$$

Note: This strengthens the congruence from Sylow's theorem.

Aufgabe 18 $(4 + 4^{+*} + 4$ points$)$**.**

(a) Determine all nilpotent groups of order 72 up to isomorphism.

(b) Construct at least four non-nilpotent groups of order 72. For each additional group, you earn a bonus point.
Hint: Exercise 11(a).

(c) Show that every group of order 220 has a normal subgroup of order 55.
Hint: Construct a smaller normal subgroup first.

Aufgabe 19.

(a) Compute $\Phi(S_4)$.

(b) Let $G = N \oplus M$ be a finite group. Prove $\Phi(G) = \Phi(N) \oplus \Phi(M)$.

(c) Determine the Frattini subgroup of a finite abelian group.
Hint: Do *not* use the definition.

Aufgabe 20.

(a) Prove $\Phi(G) \leq \mathrm{F}(G)$ and $\mathrm{F}(G/\Phi(G)) = \mathrm{F}(G)/\Phi(G)$ for every finite group G.

(b) Let P be a finite p-group with $Q \leq P$ and $N \trianglelefteq P$. Show $\Phi(Q) \leq \Phi(P)$ and $\Phi(P/N) = \Phi(P)N/N$.

(c) Prove $\Phi(P) = \langle x^2 : x \in P \rangle$ for every finite 2-group.

Aufgabe 21 (4 + 4 points)**.** Let $p > 2$ be a prime.

(a) Show that

$$P := \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} : a, b, c \in \mathbb{F}_p \right\}$$

is a non-abelian subgroup of $\mathrm{GL}(3, p)$ of order p^3 and exponent p (i. e. $x^p = 1$ for all $x \in P$).

(b) Let $R := \mathbb{Z}/p^2\mathbb{Z}$ and $\alpha, \beta \in \mathrm{Sym}(R)$ such that

$$\alpha(n + p^2\mathbb{Z}) := n + 1 + p^2\mathbb{Z}, \qquad \beta(n + p^2\mathbb{Z}) := (p + 1)n + p^2\mathbb{Z}$$

for all $n \in \mathbb{Z}$. Show that $P := \langle \alpha, \beta \rangle$ is a non-abelian group of order p^3 and exponent p^2.
Hint: $\beta \circ \alpha = \alpha^? \circ \beta$.

Aufgabe 22 (3 + 2 + 3 + 4 points)**.** A finite group G is called *complete* if $\mathrm{Z}(G) = 1 = \mathrm{Out}(G)$. Show:

(a) S_3 is complete.

(b) If G is complete, then $\mathrm{Aut}(G) \cong G$.

(c) If N is a complete normal subgroup of G, then $G = N \oplus \mathrm{C}_G(N)$.

(d) If S is a non-abelian simple group, then $\mathrm{Aut}(S)$ is complete.
Hint: Exercise 7.
Fun fact: If $\mathrm{Z}(G) = 1$, then the series $\mathrm{Aut}(G)$, $\mathrm{Aut}(\mathrm{Aut}(G)), \ldots$ terminates at a complete group after finitely many iterations (a theorem of Wielandt).

Aufgabe 23. Let N be a group and H_1, H_2 conjugate subgroups of $\mathrm{Aut}(N)$. Show $N \rtimes H_1 \cong N \rtimes H_2$.

Aufgabe 24.

(a) Decide which of the following subgroups of S_4 has a complement: A_4, $D_8 = \langle (1,2,3,4), (1,3) \rangle$, $V_4 = \langle (1,2)(3,4), (1,3)(2,4) \rangle$ and $C_2 = \langle (1,2)(3,4) \rangle$.

(b) Show that Q_8 is not (isomorphic to) a semidirect product of proper subgroups.

(c) Let G be a finite group and $x, y \in G$ non-commuting involutions (i.e. elements of order 2). Show $\langle x, y \rangle \cong D_{2n}$ for some $n \geq 3$.

Aufgabe 25. Let H be a Hall π-subgroup of G and $N \trianglelefteq G$. Show:

(a) $H \cap N$ is a Hall π-subgroup of N and HN/N is a Hall π-subgroup of G/N.

(b) $\mathrm{N}_G(\mathrm{N}_G(H)) = \mathrm{N}_G(H)$.

(c) If $\Phi(G)$ is a Hall subgroup of G, then $\Phi(G) = 1$.

Aufgabe 26. A finite group G is called *Frobenius group* if there exists a subgroup $1 < H < G$ such that $H \cap gHg^{-1} = 1$ for all $g \in G \setminus H$ (in some sense the opposite of being normal). Show that H is a Hall subgroup of G.

Aufgabe 27 $(2 + 2 + 4$ points$)$**.**

(a) Show that A_5 has no Hall $\{2, 5\}$-subgroup.

(b) Show that not every $\{2, 3\}$-subgroup of A_5 lies in a Hall $\{2, 3\}$-subgroup.

(c) Construct a finite group with non-conjugate Hall subgroups of the same order.
Hint: Consider H and $\{h^{\mathrm{t}} : h \in H\}$ in $\mathrm{GL}(3, 2)$.
Remark: $\mathrm{PSL}(2, 11)$ contains even non-isomorphic Hall subgroups of the same order.

Aufgabe 28. Show for $n \geq 3$:

(a) Every permutation of S_n is a product of at most $n - 1$ transpositions.

(b) $S_n = \langle (1,2), (1,3), \ldots, (1,n) \rangle = \langle (1,2), (2,3), \ldots, (n-1,n) \rangle = \langle (1,2,\ldots,n), (1,2) \rangle$.

(c) $A_n = \langle (a,b,c) : 1 \leq a < b < c \leq n \rangle = \langle (1,2,3), (1,2,4), \ldots, (1,2,n) \rangle = \langle (1,2,3), (2,3,4), \ldots, (n-2, n-1, n) \rangle$.

Aufgabe 29. Determine the transitive permutation groups of degree at most 4. Which of them are primitive or regular?

Aufgabe 30 (6 points)**.** In how many ways can you color the faces of a tetrahedron when n colors are available (distinct faces may have the same color)?
Hint: $|G| = 12$.

Aufgabe 31 $(1 + 3 + 3$ points$)$**.** Show that A_5 is a primitive permutation group of degree 5, 6 and 10.

Aufgabe 32. Show that a finite solvable group G is a primitive permutation group, if and only if there exists a minimal normal subgroup $A \trianglelefteq G$ such that $\mathrm{C}_G(A) = A$.

Aufgabe 33. Let G be a non-regular transitive permutation group such that every non-trivial element has at most one fixed point. Show that G is a Frobenius group (Exercise 26).

Aufgabe 34 (Embedding theorem)**.** Let G be a finite group, $N \trianglelefteq G$ and $H := G/N$. Show that G is isomorphic to a subgroup of $N \wr H$.
Hint: Apply Satz 6.26 to the regular action.

Aufgabe 35 (6 points)**.** Show that the Sylow p-subgroups of S_{p^n} are isomorphic to $C_p \wr \ldots \wr C_p$ with n "factors".
Remark: The isomorphism type does not depend on parentheses, i. e. $(C_p \wr C_p) \wr C_p \cong C_p \wr (C_p \wr C_p)$.

Aufgabe 36. Let $n \in \mathbb{N}$. Show that $\mathrm{SL}(2, \mathbb{F}_{2^n})$ acts 3-transitively on the set of all 1-dimensional subspaces of $\mathbb{F}_{2^n}^2$.

Anhang

Tabelle 1: Anzahl von Gruppen der Ordnung ≤ 2000

	1	2	3	4	5	6	7	8	9	10
0+	1	1	1	2	1	2	1	5	2	2
10+	1	5	1	2	1	14	1	5	1	5
20+	2	2	1	15	2	2	5	4	1	4
30+	1	51	1	2	1	14	1	2	2	14
40+	1	6	1	4	2	2	1	52	2	5
50+	1	5	1	15	2	13	2	2	1	13
60+	1	2	4	267	1	4	1	5	1	4
70+	1	50	1	2	3	4	1	6	1	52
80+	15	2	1	15	1	2	1	12	1	10
90+	1	4	2	2	1	231	1	5	2	16
100+	1	4	1	14	2	2	1	45	1	6
110+	2	43	1	6	1	5	4	2	1	47
120+	2	2	1	4	5	16	1	2328	2	4
130+	1	10	1	2	5	15	1	4	1	11
140+	1	2	1	197	1	2	6	5	1	13
150+	1	12	2	4	2	18	1	2	1	238
160+	1	55	1	5	2	2	1	57	2	4
170+	5	4	1	4	2	42	1	2	1	37
180+	1	4	2	12	1	6	1	4	13	4
190+	1	1543	1	2	2	12	1	10	1	52
200+	2	2	2	12	2	2	2	51	1	12
210+	1	5	1	2	1	177	1	2	2	15
220+	1	6	1	197	6	2	1	15	1	4
230+	2	14	1	16	1	4	2	4	1	208
240+	1	5	67	5	2	4	1	12	1	15
250+	1	46	2	2	1	56092	1	6	1	15
260+	2	2	1	39	1	4	1	4	1	30
270+	1	54	5	2	4	10	1	2	4	40
280+	1	4	1	4	2	4	1	1045	2	4
290+	2	5	1	23	1	14	5	2	1	49
300+	2	2	1	42	2	10	1	9	2	6
310+	1	61	1	2	4	4	1	4	1	1640
320+	1	4	1	176	2	2	2	15	1	12
330+	1	4	5	2	1	228	1	5	1	15
340+	1	18	5	12	1	2	1	12	1	10
350+	14	195	1	4	2	5	2	2	1	162
360+	2	2	3	11	1	6	1	42	2	4
370+	1	15	1	4	7	12	1	60	1	11
380+	2	2	1	20169	2	2	4	5	1	12
390+	1	44	1	2	1	30	1	2	5	221
400+	1	6	1	5	16	6	1	46	1	6
410+	1	4	1	10	1	235	2	4	1	41
420+	1	2	2	14	2	4	1	4	2	4
430+	1	775	1	4	1	5	1	6	1	51
440+	13	4	1	18	1	2	1	1396	1	34
450+	1	5	2	2	1	54	1	2	5	11
460+	1	12	1	51	4	2	1	55	1	4
470+	2	12	1	6	2	11	2	2	1	1213
480+	1	2	2	12	1	261	1	14	2	10
490+	1	12	1	4	4	42	2	4	1	56
500+	1	2	1	202	2	6	6	4	1	8
510+	1	10494213	15	2	1	15	1	4	1	49
520+	1	10	1	4	6	2	1	170	2	4
530+	2	9	1	4	1	12	1	2	2	119

Tabelle 1: Anzahl von Gruppen der Ordnung ≤ 2000

	1	2	3	4	5	6	7	8	9	10
540+	1	2	2	246	1	24	1	5	4	16
550+	1	39	1	2	2	4	1	16	1	180
560+	1	2	1	10	1	2	49	12	1	12
570+	1	11	1	4	2	8681	1	5	2	15
580+	1	6	1	15	4	2	1	66	1	4
590+	1	51	1	30	1	5	2	4	1	205
600+	1	6	4	4	7	4	1	195	3	6
610+	1	36	1	2	2	35	1	6	1	15
620+	5	2	1	260	15	2	2	5	1	32
630+	1	12	2	2	1	12	2	4	2	21541
640+	1	4	1	9	2	4	1	757	1	10
650+	5	4	1	6	2	53	5	4	1	40
660+	1	2	2	12	1	18	1	4	2	4
670+	1	1280	1	2	17	16	1	4	1	53
680+	1	4	1	51	1	15	2	42	2	8
690+	1	5	4	2	1	44	1	2	1	36
700+	1	62	1	1387	1	2	1	10	1	6
710+	4	15	1	12	2	4	1	2	1	840
720+	1	5	2	5	2	13	1	40	504	4
730+	1	18	1	2	6	195	2	10	1	15
740+	5	4	1	54	1	2	2	11	1	39
750+	1	42	1	4	2	189	1	2	2	39
760+	1	6	1	4	2	2	1	1090235	1	12
770+	1	5	1	16	4	15	5	2	1	53
780+	1	4	5	172	1	4	1	5	1	4
790+	2	137	1	2	1	4	1	24	1	1211
800+	2	2	1	15	1	4	1	14	1	113
810+	1	16	2	4	1	205	1	2	11	20
820+	1	4	1	12	5	4	1	30	1	4
830+	2	1630	2	6	1	9	13	2	1	186
840+	2	2	1	4	2	10	2	51	2	10
850+	1	10	1	4	5	12	1	12	1	11
860+	2	2	1	4725	1	2	3	9	1	8
870+	1	14	4	4	5	18	1	2	1	221
880+	1	68	1	15	1	2	1	61	2	4
890+	15	4	1	4	1	19349	2	2	1	150
900+	1	4	7	15	2	6	1	4	2	8
910+	1	222	1	2	4	5	1	30	1	39
920+	2	2	1	34	2	2	4	235	1	18
930+	2	5	1	2	2	222	1	4	2	11
940+	1	6	1	42	13	4	1	15	1	10
950+	1	42	1	10	2	4	1	2	1	11394
960+	2	4	2	5	1	12	1	42	2	4
970+	1	900	1	2	6	51	1	6	2	34
980+	5	2	1	46	1	4	2	11	1	30
990+	1	196	2	6	1	10	1	2	15	199
1000+	1	4	1	4	2	2	1	954	1	6
1010+	2	13	1	23	2	12	2	2	1	37
1020+	1	4	2	49487367289[13]	4	66	2	5	19	4
1030+	1	54	1	4	2	11	1	4	1	231
1040+	1	2	1	36	2	2	2	12	1	40
1050+	1	4	51	4	2	1028	1	5	1	15
1060+	1	10	1	35	2	4	1	12	1	4
1070+	4	42	1	4	2	5	1	10	1	583
1080+	2	2	6	4	2	6	1	1681	6	4

[13]Diese Zahl wurde nach 20 Jahren korrigiert in [D. Burrell, *On the number of groups of order 1024*, Comm. Alg. 50 (2022), 2408–2410]

Tabelle 1: Anzahl von Gruppen der Ordnung ≤ 2000

	1	2	3	4	5	6	7	8	9	10
1090+	1	77	1	2	2	15	1	16	1	51
1100+	2	4	1	170	1	4	5	5	1	12
1110+	1	12	2	2	1	46	1	4	2	1092
1120+	1	8	1	5	14	2	2	39	1	4
1130+	2	4	1	254	1	42	2	2	1	41
1140+	1	2	5	39	1	4	1	11	1	10
1150+	1	157877	1	2	4	16	1	6	1	49
1160+	13	4	1	18	1	4	1	53	1	32
1170+	1	5	1	2	2	279	1	4	2	11
1180+	1	4	3	235	2	2	1	99	1	8
1190+	2	14	1	6	1	11	14	2	1	1040
1200+	1	2	1	13	2	16	1	12	5	27
1210+	1	12	1	2	69	1387	1	16	1	20
1220+	2	4	1	164	4	2	2	4	1	12
1230+	1	153	2	2	1	15	1	2	2	51
1240+	1	30	1	4	1	4	1	1460	1	55
1250+	4	5	1	12	2	14	1	4	1	131
1260+	1	2	2	42	3	6	1	5	5	4
1270+	1	44	1	10	3	11	1	10	1	1116461
1280+	5	2	1	10	1	2	4	35	1	12
1290+	1	11	1	2	1	3609	1	4	2	50
1300+	1	24	1	12	2	2	1	18	1	6
1310+	2	244	1	18	1	9	2	2	1	181
1320+	1	2	51	4	2	12	1	42	1	8
1330+	5	61	1	4	1	12	1	6	1	11
1340+	2	4	1	11720	1	2	1	5	1	112
1350+	1	52	1	2	2	12	1	4	4	245
1360+	1	4	1	9	5	2	1	211	2	4
1370+	2	38	1	6	15	195	15	6	2	29
1380+	1	2	1	14	1	32	1	4	2	4
1390+	1	198	1	4	8	5	1	4	1	153
1400+	1	2	1	227	2	4	5	19324	1	8
1410+	1	5	4	4	1	39	1	2	2	15
1420+	4	16	1	53	6	4	1	40	1	12
1430+	5	12	1	4	2	4	1	2	1	5958
1440+	1	4	5	12	2	6	1	14	4	10
1450+	1	40	1	2	2	179	1	1798	1	15
1460+	2	4	1	61	1	2	5	4	1	46
1470+	1	1387	1	6	2	36	2	2	1	49
1480+	1	24	1	11	10	2	1	222	1	4
1490+	3	5	1	10	1	41	2	4	1	174
1500+	1	2	2	195	2	4	1	15	1	6
1510+	1	889	1	2	2	4	1	12	2	178
1520+	13	2	1	15	4	4	1	12	1	20
1530+	1	4	5	4	1	408641062	1	2	60	36
1540+	1	4	1	15	2	2	1	46	1	16
1550+	1	54	1	24	2	5	2	4	1	221
1560+	1	4	1	11	1	30	1	928	2	4
1570+	1	10	2	2	13	14	1	4	1	11
1580+	2	6	1	697	1	4	3	5	1	8
1590+	1	12	5	2	2	64	1	4	2	10281
1600+	1	10	1	5	1	4	1	54	1	8
1610+	2	11	1	4	1	51	6	2	1	477
1620+	1	2	2	56	5	6	1	11	5	4
1630+	1	1213	1	4	2	5	1	72	1	68
1640+	2	2	1	12	1	2	13	42	1	38
1650+	1	9	2	2	2	137	1	2	5	11

Tabelle 1: Anzahl von Gruppen der Ordnung ≤ 2000

	1	2	3	4	5	6	7	8	9	10
1660+	1	6	1	21507	5	10	1	15	1	4
1670+	1	34	2	60	2	4	5	2	1	1005
1680+	2	5	2	5	1	4	1	12	1	10
1690+	1	30	1	10	1	235	1	6	1	50
1700+	309	4	2	39	7	2	1	11	1	36
1710+	2	42	2	2	5	40	1	2	2	39
1720+	1	12	1	4	3	2	1	47937	1	4
1730+	2	5	1	13	1	35	4	4	1	37
1740+	1	4	2	51	1	16	1	9	1	30
1750+	2	64	1	2	14	4	1	4	1	1285
1760+	1	2	1	228	1	2	5	53	1	8
1770+	2	4	2	2	4	260	1	6	1	15
1780+	1	110	1	12	2	4	1	12	1	4
1790+	5	1083553	1	12	1	5	1	4	1	749
1800+	1	4	2	11	3	30	1	54	13	6
1810+	1	15	2	2	9	12	1	10	1	35
1820+	2	2	1	1264	2	4	6	5	1	18
1830+	1	14	2	4	1	117	1	2	2	178
1840+	1	6	1	5	4	4	1	162	2	10
1850+	1	4	1	16	1	1630	2	2	2	56
1860+	1	10	15	15	1	4	1	4	2	12
1870+	1	1096	1	2	21	9	1	6	1	39
1880+	5	2	1	18	1	4	2	195	1	120
1890+	1	9	2	2	1	54	1	4	4	36
1900+	1	4	1	186	2	2	1	36	1	6
1910+	15	12	1	8	1	4	5	4	1	241004
1920+	1	5	1	15	4	10	1	15	2	4
1930+	1	34	1	2	4	167	1	12	1	15
1940+	1	2	1	3973	1	4	1	4	1	40
1950+	1	235	11	2	1	15	1	6	1	144
1960+	1	18	1	4	2	2	2	203	1	4
1970+	15	15	1	12	2	39	1	4	1	120
1980+	1	2	2	1388	1	6	1	13	4	4
1990+	1	39	1	2	5	4	1	66	1	963

Tabelle 2: Nichtabelsche einfache Gruppen der Ordnung $\leq 10^6$

G	$\lvert G\rvert$	$\mathrm{Out}(G)$	$M(G)$
$A_5 \cong \mathrm{SL}(2,2^2) \cong \mathrm{PSL}(2,5)$	$60 = 2^2 \cdot 3 \cdot 5$	C_2	C_2
$\mathrm{GL}(3,2) \cong \mathrm{PSL}(2,7)$	$168 = 2^3 \cdot 3 \cdot 7$	C_2	C_2
$A_6 \cong \mathrm{PSL}(2,3^2)$	$360 = 2^3 \cdot 3^2 \cdot 5$	C_2^2	C_6
$\mathrm{SL}(2,2^3)$	$504 = 2^3 \cdot 3^2 \cdot 7$	C_3	1
$\mathrm{PSL}(2,11)$	$660 = 2^2 \cdot 3 \cdot 5 \cdot 11$	C_2	C_2
$\mathrm{PSL}(2,13)$	$1092 = 2^2 \cdot 3 \cdot 7 \cdot 13$	C_2	C_2
$\mathrm{PSL}(2,17)$	$2448 = 2^4 \cdot 3^2 \cdot 17$	C_2	C_2
A_7	$2520 = 2^3 \cdot 3^2 \cdot 5 \cdot 7$	C_2	C_6
$\mathrm{PSL}(2,19)$	$3420 = 2^2 \cdot 3^2 \cdot 5 \cdot 19$	C_2	C_2
$\mathrm{SL}(2,2^4)$	$4080 = 2^4 \cdot 3 \cdot 5 \cdot 17$	C_4	1
$\mathrm{SL}(3,3)$	$5616 = 2^4 \cdot 3^3 \cdot 13$	C_2	1
$\mathrm{SU}(3,3)$	$6048 = 2^5 \cdot 3^3 \cdot 7$	C_2	1
$\mathrm{PSL}(2,23)$	$6072 = 2^3 \cdot 3 \cdot 11 \cdot 23$	C_2	C_2
$\mathrm{PSL}(2,5^2)$	$7800 = 2^3 \cdot 3 \cdot 5^2 \cdot 13$	C_2^2	C_2
M_{11}	$7920 = 2^4 \cdot 3^2 \cdot 5 \cdot 11$	1	1
$\mathrm{PSL}(2,3^3)$	$9828 = 2^2 \cdot 3^3 \cdot 7 \cdot 13$	C_6	C_2
$\mathrm{PSL}(2,29)$	$12180 = 2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 29$	C_2	C_2
$\mathrm{PSL}(2,31)$	$14880 = 2^5 \cdot 3 \cdot 5 \cdot 31$	C_2	C_2
$A_8 \cong \mathrm{GL}(4,2)$	$20160 = 2^6 \cdot 3^2 \cdot 5 \cdot 7$	C_2	C_2
$\mathrm{PSL}(3,2^2)$	$20160 = 2^6 \cdot 3^2 \cdot 5 \cdot 7$	D_{12}	$C_{12} \times C_4$
$\mathrm{PSL}(2,37)$	$25308 = 2^2 \cdot 3^2 \cdot 19 \cdot 37$	C_2	C_2
$\mathrm{SU}(4,2) \cong \mathrm{PSp}(4,3)$	$25920 = 2^6 \cdot 3^4 \cdot 5$	C_2	C_2
$\mathrm{Sz}(8)$	$29120 = 2^6 \cdot 5 \cdot 7 \cdot 13$	C_3	C_2^2
$\mathrm{SL}(2,2^5)$	$32736 = 2^5 \cdot 3 \cdot 11 \cdot 31$	C_5	1
$\mathrm{PSL}(2,41)$	$34440 = 2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 41$	C_2	C_2
$\mathrm{PSL}(2,43)$	$39732 = 2^2 \cdot 3 \cdot 7 \cdot 11 \cdot 43$	C_2	C_2
$\mathrm{PSL}(2,47)$	$51888 = 2^4 \cdot 3 \cdot 23 \cdot 47$	C_2	C_2
$\mathrm{PSL}(2,7^2)$	$58800 = 2^4 \cdot 3 \cdot 5^2 \cdot 7^2$	C_2^2	C_2
$\mathrm{SU}(3,2^2)$	$62400 = 2^6 \cdot 3 \cdot 5^2 \cdot 13$	C_4	1
$\mathrm{PSL}(2,53)$	$74412 = 2^2 \cdot 3^3 \cdot 13 \cdot 53$	C_2	C_2
M_{12}	$95040 = 2^6 \cdot 3^3 \cdot 5 \cdot 11$	C_2	C_2
$\mathrm{PSL}(2,59)$	$102660 = 2^2 \cdot 3 \cdot 5 \cdot 29 \cdot 59$	C_2	C_2
$\mathrm{PSL}(2,61)$	$113460 = 2^2 \cdot 3 \cdot 5 \cdot 31 \cdot 61$	C_2	C_2
$\mathrm{PSU}(3,5)$	$126000 = 2^4 \cdot 3^2 \cdot 5^3 \cdot 7$	C_3	C_3
$\mathrm{PSL}(2,67)$	$150348 = 2^2 \cdot 3 \cdot 11 \cdot 17 \cdot 67$	C_2	C_2
J_1	$175560 = 2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 19$	1	1
$\mathrm{PSL}(2,71)$	$178920 = 2^3 \cdot 3^2 \cdot 5 \cdot 7 \cdot 71$	C_2	C_2
A_9	$181440 = 2^6 \cdot 3^4 \cdot 5 \cdot 7$	C_2	C_2
$\mathrm{PSL}(2,73)$	$194472 = 2^3 \cdot 3^2 \cdot 37 \cdot 73$	C_2	C_2
$\mathrm{PSL}(2,79)$	$246480 = 2^4 \cdot 3 \cdot 5 \cdot 13 \cdot 79$	C_2	C_2
$\mathrm{SL}(2,2^6)$	$262080 = 2^6 \cdot 3^2 \cdot 5 \cdot 7 \cdot 13$	C_6	1
$\mathrm{PSL}(2,3^4)$	$265680 = 2^4 \cdot 3^4 \cdot 5 \cdot 41$	$C_4 \times C_2$	C_2
$\mathrm{PSL}(2,83)$	$285852 = 2^2 \cdot 3 \cdot 7 \cdot 41 \cdot 83$	C_2	C_2
$\mathrm{PSL}(2,89)$	$352440 = 2^3 \cdot 3^2 \cdot 5 \cdot 11 \cdot 89$	C_2	C_2
$\mathrm{SL}(3,5)$	$372000 = 2^5 \cdot 3 \cdot 5^3 \cdot 31$	C_2	1
M_{22}	$443520 = 2^7 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11$	C_2	C_{12}
$\mathrm{PSL}(2,97)$	$456288 = 2^5 \cdot 3 \cdot 7^2 \cdot 97$	C_2	C_2
$\mathrm{PSL}(2,101)$	$515100 = 2^2 \cdot 3 \cdot 5^2 \cdot 17 \cdot 101$	C_2	C_2
$\mathrm{PSL}(2,103)$	$546312 = 2^3 \cdot 3 \cdot 13 \cdot 17 \cdot 103$	C_2	C_2
J_2	$604800 = 2^7 \cdot 3^3 \cdot 5^2 \cdot 7$	C_2	C_2
$\mathrm{PSL}(2,107)$	$612468 = 2^2 \cdot 3^3 \cdot 53 \cdot 107$	C_2	C_2
$\mathrm{PSL}(2,109)$	$647460 = 2^2 \cdot 3^3 \cdot 5 \cdot 11 \cdot 109$	C_2	C_2
$\mathrm{PSL}(2,113)$	$721392 = 2^4 \cdot 3 \cdot 7 \cdot 19 \cdot 113$	C_2	C_2
$\mathrm{PSL}(2,11^2)$	$885720 = 2^3 \cdot 3 \cdot 5 \cdot 11^2 \cdot 61$	C_2^2	C_2
$\mathrm{PSL}(2,5^3)$	$976500 = 2^2 \cdot 3^2 \cdot 5^3 \cdot 7 \cdot 31$	C_6	C_2
$\mathrm{Sp}(4,2^2)$	$979200 = 2^8 \cdot 3^2 \cdot 5^2 \cdot 17$	C_2	1

Tabelle 3: Primitive Permutationsgruppen vom Grad $d \leq 15$

d	G
2	$S_2 = C_2$
3	$A_3 = C_3,\ S_3$
4	$A_4,\ S_4$
5	$C_5,\ D_{10},\ \mathrm{AGL}(1,5) = C_5 \rtimes C_4,\ A_5,\ S_5$
6	$A_5,\ S_5,\ A_6,\ S_6$
7	$C_7,\ D_{14},\ C_7 \rtimes C_3,\ \mathrm{AGL}(1,7) = C_7 \rtimes C_6,\ \mathrm{GL}(3,2),\ A_7,\ S_7$
8	$\mathrm{AGL}(1,8),\ \mathrm{A\Gamma L}(1,8),\ \mathrm{AGL}(3,2),\ \mathrm{PGL}(2,7),\ A_8,\ S_8$
9	$C_3^2 \rtimes C_4,\ S_3 \wr C_2,\ M_9 = C_3^2 \rtimes Q_8,\ \mathrm{AGL}(1,9),\ \mathrm{A\Gamma L}(1,9),$ $\mathrm{ASL}(2,3),\ \mathrm{AGL}(2,3),\ \mathrm{SL}(2,8),\ \mathrm{P\Gamma L}(2,8),\ A_9,\ S_9$
10	$A_5,\ S_5,\ \mathrm{PSL}(2,9),\ \mathrm{PGL}(2,9),\ \mathrm{P\Sigma L}(2,9),\ M_{10},\ \mathrm{P\Gamma L}(2,9),\ A_{10},\ S_{10}$
11	$C_{11},\ D_{22},\ C_{11} \rtimes C_5,\ \mathrm{AGL}(1,11),\ \mathrm{PSL}(2,11),\ M_{11},\ A_{11},\ S_{11}$
12	$M_{11},\ M_{12},\ \mathrm{PSL}(2,11),\ \mathrm{PGL}(2,11),\ A_{12},\ S_{12}$
13	$C_{13},\ D_{26},\ C_{13} \rtimes C_3,\ C_{13} \rtimes C_4,\ C_{13} \rtimes C_6,\ \mathrm{AGL}(1,13),\ \mathrm{SL}(3,3),\ A_{13},\ S_{13}$
14	$\mathrm{PSL}(2,13),\ \mathrm{PGL}(2,13),\ A_{14},\ S_{14}$
15	$A_6,\ S_6,\ A_7,\ A_8,\ A_{15},\ S_{15}$

Stichwortverzeichnis

W

Z