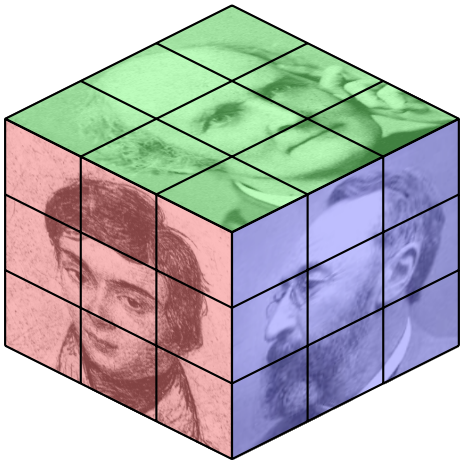
Gruppentheorie

Vorlesung im Wintersemester 2020/21

Benjamin Sambale
Leibniz Universität Hannover

Version: 25. Juni 2025



Inhaltsverzeichnis

Vorwort

Dieses Skript entstand aus Vorlesungen an der Technischen Universität Kaiserslautern (Wintersemester 2016/17) und an der Leibniz Universität Hannover (Wintersemester 2020/21). Diese Vorlesung richtet sich hauptsächlich an Bachelor- und Master-Studierende der Mathematik. Es werden Kenntnisse der Algebra 1 & 2 vorausgesetzt, wobei die wichtigsten Ergebnisse im ersten Kapitel ohne Beweise wiederholt werden (Beweise findet man zum Beispiel in meinem Algebra-Skript). Nachträglich sind einige Ergänzungen hinzugekommen: unter anderem Sätze von Gaschütz, Rose und Shemetkov über Komplemente sowie Alperins Fusionssatz, Puigs Hyperfokalsatz und Tates Verlagerungssatz mit einem relativ unbekannten Beweis von Brandis.

Ich danke Annika Bartelt, Luca Blaas, Jonathan Gruber, Gereon Koßmann, Julia Liebner und Scheima Sara Obeidi für wertvolle Fehlerhinweise.

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 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:[5]

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

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) Aus dem Assoziativgesetz folgt induktiv, dass ein Produkt von endlich vielen Gruppenelementen nicht von der Klammerung abhängt (wohl aber von der Reihenfolge). Zum Beispiel gilt

$$((ab)c)d = (a(bc))d = a((bc)d) = a(b(cd)) = (ab)(cd)$$

für $a, b, c, d \in G$.[6]

[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.
[5] Man kann Gruppen auch mit einem einzigen Axiom definieren, siehe [W. McCune und A. D. Sands, *Computer and Human Reasoning: Single Implicative Axioms for Groups and for Abelian Groups*, Amer. Math. Monthly 103 (1996), 888–892].
[6] Die Anzahl der verschiedenen Klammerung von n Faktoren ist die *Catalan-Zahl* $\frac{1}{n}\binom{2n-2}{n-1}$.

(iii) 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 $(x^{-1})^{-1} = y^{-1} = z = x$.

(iv) Achtung: Die Existenz der inversen Elemente ist *nicht* äquivalent zu $\forall x \in G : \exists y \in G : xy = e$ (rechtsinvers). Betrachte zum Beispiel $G = \left\{ \left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 1 \\ 0 & 0 \end{smallmatrix}\right) \right\}$ bzgl. Matrizenmultiplikation. Man muss also „linksneutral + linksinvers“ oder „rechtsneutral + rechtsinvers“ fordern.

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

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

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

Sicher ist dann $x^m x^n = x^{m+n}$ und $(x^m)^n = x^{mn}$ für $n, m \in \mathbb{Z}$. Man nennt $\inf\{n \geq 1 : x^n = 1\}$ die *Ordnung* von x. Dabei sei $\inf \varnothing = \infty$. Besteht G aus Potenzen von x, so heißt G *zyklisch*. 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 $\Omega = \{1, \dots, n\}$ 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 $I = \{1, \dots, n\}$ schreibt man auch $G_1 \times \dots \times G_n$ und G^n, falls $G := G_1 = \dots = G_n$.

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 $x_1^{\pm 1}\dots x_n^{\pm 1}$ mit $x_1,\dots,x_n \in U$ (dies entspricht den Linearkombinationen in der linearen Algebra). Im Fall $\langle U\rangle = G$ ist U ein *Erzeugendensystem* von G. Ist zusätzlich $U = \{x_1,\dots,x_n\}$, so schreibt man $G = \langle x_1,\dots,x_n\rangle$ 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* $\mathrm{SL}(n,K) := \{A \in \mathrm{GL}(n,K) : \det(A) = 1\} \leq \mathrm{GL}(n,K)$.

(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 $A_n := \mathrm{Alt}(\{1,\dots,n\})$ 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).

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

Beweis. Aufgabe 2. □

Satz 1.10. *Ist G endlich erzeugt und $H \leq G$ mit $|G:H| < \infty$, so ist auch H endlich erzeugt.*

Beweis. Sei $X = X^{-1}$ ein endliches Erzeugendensystem von G und R ein Repräsentantensystem für G/H mit $1 \in R$. Für $x \in X$ und $r \in R$ existieren $\alpha(x,r) \in H$ und $\gamma(x,r) \in R$ mit $xr = \gamma(x,r)\alpha(x,r)$. Jedes Element in H hat die Form $h = x_1 \dots x_n$ mit $x_1, \dots, x_n \in X$. Dabei gilt

$$\begin{aligned} h &= x_1 \dots x_n 1 = x_1 \dots x_{n-1}\gamma(x_n,1)\alpha(x_n,1) = x_1 \dots x_{n-2}\gamma(x_{n-1},\gamma(x_n,1))\alpha(x_{n-1},\gamma(x_n,1))\alpha(x_n,1) \\ &= \dots = \gamma(x_1,\dots)\alpha(x_1,\dots)\dots\alpha(x_n,1). \end{aligned}$$

Wegen $h \in H$ gilt dabei $\gamma(x_1,\dots) = 1$. Es folgt $H = \langle \alpha(x,r) : x \in X, r \in R \rangle$. □

Bemerkung 1.11. Der obige Beweis zeigt, dass man H mit $|X||G:H|$ Elementen erzeugen kann. Der Satz von Reidemeister-Schreier liefert die optimale Schranke $|G:H|(|X|-1)+1$ für die Anzahl der Erzeuger (ohne Beweis).

Definition 1.12. 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 1.13.

(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 1.14.

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

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

(iii) Für $H \leq G$ ist $H^G := \langle \bigcup_{g \in G} gHg^{-1} \rangle$ der *normale Abschluss* von H in G. Dies ist der „kleinste“ Normalteiler von G, der H enthält. Analog ist $H_G := \bigcap_{g \in G} gHg^{-1}$ der *Kern* von H in G, d. h. der „größte“ Normalteiler von G, der in H enthalten ist.

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

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

Definition 1.15. 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 1.16.

(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) Für Gruppen G, H ist die *Projektion* $G \times H \to G$, $(g, h) \mapsto g$ ein Epimorphismus.

(iv) 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.

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

Bemerkung 1.17.

(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 $f^{-1}(V) \trianglelefteq G$.[7] 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 1.18.

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

[7] In der Analysis sind Urbilder offener Mengen unter stetigen Abbildungen wieder offen, aber Bilder nicht unbedingt.

Beweis. Algebra. □

Definition 1.19. 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 1.20.

(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 1.21.

(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) Seien $H, K \leq G$. Dann operiert $H \times K$ durch ${}^{(h,k)}g := hgk^{-1}$ auf G. Die Bahnen haben die Form HgK und heißen *Doppelnebenklassen* von G nach (H, K). Ist H (bzw. K) normal, so ist $HgK = gHK$ eine Linksnebenklasse (bzw. Rechtsnebenklasse). Im Allgemeinen ist $|HgK| = |H(gKg^{-1})| = |H : H \cap gKg^{-1}||K|$ kein Teiler von $|G|$.

(iii) 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

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

(iv) 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 1.22. *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 1.23. 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 1.24 (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 1.25. 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 $G = N_1 \dots N_k$ ist F surjektiv. Sei $(x_1, \dots, x_k) \in \mathrm{Ker}(F)$. Angenommen es existiert $1 \leq l \leq k$ mit $x_l \neq 1$. Sei l maximal. Dann wäre $x_l^{-1} = x_1 \dots x_{l-1} \in N_l \cap N_1 \dots N_{l-1} = 1$. 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*

$$G = G_1 \oplus \dots \oplus G_s = H_1 \oplus \dots \oplus H_t$$

mit unzerlegbaren Gruppen $G_1, \dots, G_s, H_1, \dots, H_t$. Dann existiert für jedes i ein j mit

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

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

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 $i = 1, \dots, t$.

Fall 1: Es existiert ein i mit $H_{i1} < H_i$.
Sei $H := H_{11} \oplus \dots \oplus H_{t1} < G$. Wegen $g = \pi_1(g) \dots \pi_t(g)$ für alle $g \in G_1$ gilt $G_1 \leq H$. Nach Dedekind ist $H = G_1 \oplus (G_2 \dots G_s \cap H)$. 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. $H = K \oplus (G_2 \dots G_s \cap H)$ und $K \cap G_2 \dots G_s = 1$. Jedes Element in K hat die Form $\pi_j(g_1)$ für ein $g_1 \in G_1$. Für $g \in G_2 \dots G_s$ gilt

$$g\pi_j(g_1) = \pi_1(g) \dots \pi_j(gg_1) \dots \pi_t(g) = \pi_1(g) \dots \pi_j(g_1g) \dots \pi_t(g) = \pi_j(g_1)g.$$

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

Fall 2: Es gilt $G = H_{11} \oplus \dots \oplus H_{t1}$.
Dann ist $|G_1| \geq |\pi_i(G_1)| = |H_{i1}| = |H_i|$ für $i = 1, \dots, t$. 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 $G = H_iG_2 \dots G_s$ und wegen $|H_i| \leq |G_1|$ muss die Summe direkt sein. Wir können also $\rho_1(H_i) < G_1$ für $i = 1, \dots, t$ 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

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

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 (Aufgabe 7). 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 $1 < d_1 \mid \dots \mid d_t$ mit

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

(ii) Es existieren eindeutig bestimmte Primzahlpotenzen $1 < p_1^{a_1} \leq \dots \leq p_t^{a_t}$ und ein $s \geq 0$ mit

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

Beweis.

(i) **Schritt 1:** Existenz.
Sei $x_1, \dots, x_r$ 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 $g = x_1^{n_1}x_2^{n_2}\dots x_r^{n_r}$ mit $n_1, \dots, n_r \in \mathbb{Z}$ schreiben. Eine Gleichung der Form $x_1^{n_1}x_2^{n_2}\dots x_r^{n_r} = 1$ nennt man *Relation*. Gibt es nur die triviale Relation mit $n_1 = \dots = n_r = 0$, so ist $\mathbb{Z}^r \to G$, $(n_1, \dots, n_r) \mapsto x_1^{n_1}x_2^{n_2}\dots x_r^{n_r}$ ein Isomorphismus.

Nehmen wir nun an, dass auch nicht-triviale Relationen existieren. Wir wählen $x_1, \dots, x_r$ unter allen minimalen Erzeugendensystemen so, dass eine Relation mit minimalem Exponenten $d_1 > 0$ gilt.O. B. d. A. sei $x_1^{d_1}x_2^{n_2}\dots x_r^{n_r} = 1$. 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

$$1 = x_1^{d_1}x_2^{qd_1+u}\dots x_r^{n_r} = (x_1x_2^q)^{d_1}x_2^u x_3^{n_3}\dots x_r^{n_r}. \tag{2.1}$$

Da man jedes Element $x_1^{l_1}\dots x_r^{l_r}$ auch in der Form $(x_1x_2^q)^{l_1}x_2^{l_2-ql_1}x_3^{l_3}\dots x_r^{l_r}$ schreiben kann, ist $x_1x_2^q, x_2, \dots, x_r$ 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 $d_1 \mid n_3, \dots, d_1 \mid n_r$. Wir schreiben $n_i = q_i d_1$ für $i = 3, \dots, r$. Setzt man $z := x_1x_2^q x_3^{q_3}\dots x_r^{q_r}$, so ist $z, x_2, \dots, x_r$ wieder ein minimales Erzeugendensystem und die Relation wird zu $1 = z^{d_1}$. Damit hat z die Ordnung d_1, denn $1 = z^l = z^l x_2^0 \dots x_r^0$ mit $0 < l < d_1$ wäre ein Widerspruch zur Wahl vom d_1. Mit $H := \langle z \rangle$ und $G_1 := \langle x_2, \dots, x_r \rangle$ gilt $G = HG_1$. Im Fall $H \cap G_1 \neq 1$ gäbe es $l_1, \dots, l_r \in \mathbb{Z}$ mit $1 \neq z^{l_1} = x_2^{l_2}\dots x_r^{l_r}$ und $0 < l_1 < d_1$. Dann wäre aber $z^{l_1}x_2^{-l_2}\dots x_r^{-l_r} = 1$ 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 $y_2^{d_2}y_3^{n_3'}\dots y_r^{n_r'} = 1$ 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.

(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.

(i) Satz 2.11 zeigt, dass die Begriffe *torsionsfrei* und *frei abelsch* für endlich erzeugte Gruppen äquivalent sind. Für unendlich erzeugte abelsche Gruppen ist das im Allgemeinen falsch (Aufgabe 7).

(ii) 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.

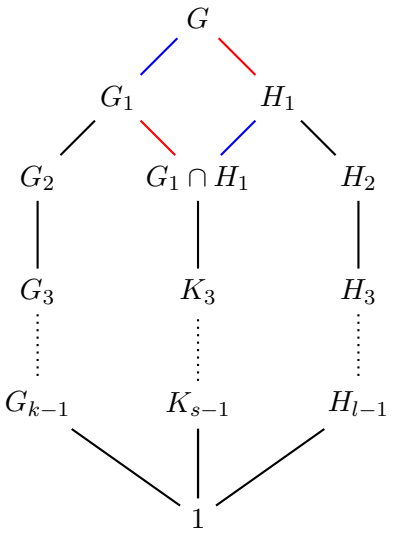
Satz 2.17 (Jordan-Hölder). *Seien* $1 = G_k \trianglelefteq \ldots \trianglelefteq G_0 = G$ *und* $1 = H_l \trianglelefteq \ldots \trianglelefteq H_0 = G$ *Kompositionsreihen einer endlichen Gruppe* G. *Dann ist* $k = l$ *und es existiert ein* $\pi \in S_k$ *mit* $G_{i-1}/G_i \cong H_{\pi(i)-1}/H_{\pi(i)}$ *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:[8]

- C_p (p Primzahl),
- A_n für $n \geq 5$ (Satz 6.38),
- Gruppen vom „Lie-Typ“ (PSL(n,q) (Satz 10.11), PSU(n,q) (Bemerkung 10.12), $\ldots, E_8(q)$),
- 26 sporadische Gruppen, deren größte die *Monstergruppe* ist mit ca. 10^{54} Elementen.

Der Beweis dieser Klassifikation (CFSG) 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.[9]

(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.[10]

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 13 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

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

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

[9] 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`]

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

Somit ist auch G/N auflösbar.

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

Beispiel 2.23.

(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) Offenbar ist $\mathrm{Z}(G)$ charakteristisch in G (Aufgabe 15).

(iii) In einer zyklischen Gruppe ist nach Satz 2.4 jede Untergruppe charakteristisch (Aufgabe 15).

(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 $k \geq 2$.[11]

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

[11] 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 $G^{(k)} = 1$ (falls es existiert) 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 $[X,Y,Z] = [Y,X,Z]$ (Aufgabe 25). 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*[12]

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

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. Im Allgemeinen nennt man $\mathrm{Z}_\infty(G):=\bigcup_{k\geq 0}\mathrm{Z}_k(G)$ das *Hyperzentrum* 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:

$$\text{Primzahlordnung}\Longrightarrow\text{zyklisch}\Longrightarrow\text{abelsch}\Longrightarrow\text{nilpotent}\Longrightarrow\text{überauflösbar}\Longrightarrow\text{auflösbar}$$

(iii) Wegen $Z_k(G)\leq\mathrm{Z}_{k+1}(G)$ für alle $k\in\mathbb{N}$ ist $\mathrm{Z}_\infty(G)\leq G$. Es gibt (unendlich erzeugte) nicht-nilpotente Gruppen mit $G=\mathrm{Z}_\infty(G)$ (z. B. $\times_{n=3}^{\infty}D_{2^n}$ nach Aufgabe 17). Diese nennt man *hyperzentral*.

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.

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

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

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

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

$$[\overline{G}, \overline{G}^{[n-1]}, \overline{G}^{[m]}] \subseteq [\overline{G}, \overline{G}^{[n+m-1]}] = \overline{G}^{[n+m]} = 1$$

und $[\overline{G}^{[n-1]}, \overline{G}^{[m]}, \overline{G}] = [\overline{G}^{[n-1]}, \overline{G}^{[m+1]}] \subseteq \overline{G}^{[n+m]} = 1$. Lemma 3.6 impliziert daher

$$[G^{[m]}, G^{[n]}]G^{[n+m]}/G^{[n+m]} = [\overline{G}^{[m]}, \overline{G}^{[n]}] = [\overline{G}^{[m]}, \overline{G}, \overline{G}^{[n-1]}] = 1.$$

Dies zeigt die Behauptung. □

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

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

Beispiel 3.13. Es gibt metabelsche Gruppen mit beliebig hoher Nilpotenzklasse (Diedergruppen der Form D_{2^n}, siehe Aufgabe 17).

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

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

Sei $N_1 := N$ und $N_{i+1} := [G, N_i] \leq N$ 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 3.15 (Fitting)**.** *Sind N und M nilpotente Normalteiler von G, so ist auch NM nilpotent. Hat N Klasse n und M Klasse m, so hat NM höchstens Klasse $n + m$.*

Beweis. Für beliebige Normalteiler $X, Y, Z \trianglelefteq G$ und $x \in X$, $y \in Y$ und $z \in Z$ gilt

$$[x, yz] = [x, y] \cdot {}^{y}[x, z] \in [X, Y][X, Z]$$

nach Bemerkung 3.2. Dies zeigt $[X, YZ] \subseteq [X, Y][X, Z] \subseteq [X, YZ]$ und somit $[X, YZ] = [X, Y][X, Z]$. Analog ist $[XY, Z] = [X, Z][Y, Z]$. Daher ist $(NM)^{[n+m+1]}$ ein Produkt von Normalteilern der Form $[X_0, \ldots, X_{n+m}]$ mit $X_0, \ldots, X_{n+m} \in \{N, M\}$. O. B. d. A. können wir annehmen, dass N mindestens $n+1$ Mal unter den X_i auftritt (anderenfalls tritt M mindestens $m+1$ Mal auf). Wir zeigen durch

Induktion nach $n+m$, dass dann $[X_0,\dots,X_{n+m}] \subseteq N^{[n+1]}$ gilt. Ist $X_0 = M$, so gilt induktiv bereits $[X_1,\dots,X_{n+m}] \subseteq N^{[n+1]}$ und die Behauptung folgt. Gilt hingegen $X_0 = N$, so ist $[X_1,\dots,X_{n+m}] \subseteq N^{[n]}$ und $[X_0,\dots,X_{n+m}] \subseteq [N, N^{[n]}] = N^{[n+1]}$. Die Behauptung folgt nun aus Satz 3.9. □

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

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

Beispiel 3.18. 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 3.19. *Ist G endlich und auflösbar, so gilt $\mathrm{C}_G(\mathrm{F}(G)) \leq \mathrm{F}(G)$.*

Beweis. Sei $C := \mathrm{C}_G(\mathrm{F}(G)) \trianglelefteq G$. Wir nehmen indirekt $\overline{C} := C/\mathrm{Z}(\mathrm{F}(G)) = C/C \cap \mathrm{F}(G) \neq 1$ an. Da $\overline{C}$ auflösbar ist, gilt $N/\mathrm{Z}(\mathrm{F}(G)) := \mathrm{F}(\overline{C}) \neq 1$. Dabei ist $\mathrm{Z}(\mathrm{F}(G)) \leq N \cap \mathrm{Z}(C) \leq \mathrm{Z}(N)$ und $N/\mathrm{Z}(N) \cong \mathrm{F}(\overline{C})/(\mathrm{Z}(N)/\mathrm{Z}(\mathrm{F}(G)))$ 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 3.20. Für endliche, auflösbare Gruppen G gilt $G/\mathrm{Z}(\mathrm{F}(G)) = \mathrm{N}_G(\mathrm{F}(G))/\mathrm{C}_G(\mathrm{F}(G)) \leq \mathrm{Aut}(\mathrm{F}(G))$ und $G/\mathrm{F}(G) \leq \mathrm{Out}(\mathrm{F}(G))$ nach Satz 3.19.

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 $U \leq G$ eine p-Untergruppe. Die Bahnenlängen der Operation von U auf G/P durch Linksmultiplikation (siehe Aufgabe 4) sind dann Teiler von $|U|$, 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 1.22. 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) Sind $N, M \trianglelefteq G$ mit π-Faktorgruppen G/N und G/M, so ist auch $G/(N \cap M)$ eine π-Gruppe, denn

$$|G/(N \cap M)| = |G/N||N/(N \cap M)| = |G/N||NM/M| \mid |G/N||G/M|.$$

Es gibt daher einen kleinsten Normalteiler $\mathrm{O}^\pi(G)$ mit π-Faktorgruppe $G/\mathrm{O}^\pi(G)$. Man nennt $\mathrm{O}^\pi(G)$ das π-*Residuum* von G (analog $\mathrm{O}^p(G)$). Offenbar liegt jedes π'-Element in $\mathrm{O}^\pi(G)$. Umgekehrt erzeugen alle π'-Elemente von G einen Normalteiler mit π-Faktorgruppe. Dies zeigt $\mathrm{O}^\pi(G) = \langle g \in G : g\ \pi'\text{-Element}\rangle$. Für $H \leq G$ ist $H/(H \cap \mathrm{O}^\pi(G)) \cong H\mathrm{O}^\pi(G)/\mathrm{O}^\pi(G) \leq G/\mathrm{O}^\pi(G)$ eine π-Gruppe und es folgt $\mathrm{O}^\pi(H) \leq \mathrm{O}^\pi(G)$.

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

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

Satz 4.7. *Es gilt* $\mathrm{O}_p(G) = \bigcap_{P \in \mathrm{Syl}_p(G)} P$ *und* $\mathrm{O}^{p'}(G) = \langle P : P \in \mathrm{Syl}_p(G)\rangle$.

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

Nach Bemerkung 4.6 wird $\mathrm{O}^{p'}(G)$ von allen p-Elementen erzeugt. Jedes p-Element liegt in einer p-Sylowgruppe. Dies zeigt die zweite Behauptung. □

Satz 4.8. *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 4.9. 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 4.10. *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 3.14.

(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 4.8 ist jede Sylowgruppe nilpotent und daher auch G (Satz 3.15). □

Satz 4.11. *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 4.10 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 $Q_i \leq \mathrm{O}_{p_i}(G)$. □

Satz 4.12 (Baer)**.** *Für das Hyperzentrum gilt* $\mathrm{Z}_\infty(G) = \bigcap_{p\,||G|} \bigcap_{P \in \mathrm{Syl}_p(G)} \mathrm{N}_G(P)$.

Beweis. Offensichtlich ist $\mathrm{Z}_0(G) = 1 \leq \bigcap_{p\,||G|} \bigcap_{P \in \mathrm{Syl}_p(G)} \mathrm{N}_G(P) =: U$. Sei induktiv bereits $Z := \mathrm{Z}_k(G) \leq U$ gezeigt. Für $g \in \mathrm{Z}_{k+1}(G)$ und $P \in \mathrm{Syl}_p(G)$ ist $gZ \in \mathrm{Z}(G/Z) \leq \mathrm{N}_G(PZ/Z)$ und $g \in \mathrm{N}_G(PZ)$. Nach Sylow existiert ein $z \in Z \leq U \leq \mathrm{N}_G(P)$ mit $gPg^{-1} = zPz^{-1} = P$. Dies zeigt $g \in \mathrm{N}_G(P)$ und $\mathrm{Z}_{k+1}(G) \leq U$. Es folgt $\mathrm{Z}_\infty(G) \leq U$.

Für die Umkehrung sei $Z := \mathrm{Z}_\infty(G)$. Jede Sylowgruppe von G/Z hat die Form PZ/Z mit $P \in \mathrm{Syl}_p(G)$ und $\mathrm{N}_G(P)Z/Z \leq \mathrm{N}_{G/Z}(PZ/Z)$. Wir können daher $Z = 1$ annehmen und müssen $U = 1$ zeigen. Sei indirekt $U \neq 1$. Dann existiert ein $P \in \mathrm{Syl}_p(G)$ mit $U \cap P \neq 1$ nach Cauchy. Wegen $U \trianglelefteq G$ ist auch $U_0 := U \cap \mathrm{Z}(P) \neq 1$ nach Satz 3.14. Für alle $Q \in \mathrm{Syl}_p(G)$ ist $U_0 \leq P \cap \mathrm{N}_G(Q) = P \cap Q$. Dies zeigt $U_0 \leq \mathrm{O}_p(G)$ nach Satz 4.7. Wegen $\mathrm{Z}(G) = 1$ ist G keine p-Gruppe. Sei also $S \in \mathrm{Syl}_q(G)$ mit $q \neq p$. Dann ist $U_0 \leq \mathrm{N}_G(S) \cap \mathrm{O}_p(G) \leq \mathrm{C}_G(S)$ nach Lemma 2.5. Da $\mathrm{O}^p(G)$ von allen q-Sylowgruppen mit $q \neq p$ erzeugt wird (vgl. Satz 4.7), folgt $U_0 \leq \mathrm{C}_G(\mathrm{O}^p(G))$. Aus $G = \mathrm{O}^p(G)P$ und $U_0 \leq \mathrm{Z}(P)$ erhält man den Widerspruch $U_0 \leq \mathrm{Z}(G) = 1$. □

Definition 4.13. Die *Frattinigruppe* $\Phi(G)$ ist der Durchschnitt aller maximalen Untergruppen von G.[13] Für $G = 1$ setzt man $\Phi(G) = 1$.

Bemerkung 4.14. Für $G \neq 1$ ist sicher $\Phi(G) < G$. Außerdem ist $\Phi(G)$ charakteristisch in G.

Lemma 4.15. *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) $N \leq \Phi(G) \Longrightarrow \Phi(G/N) = \Phi(G)/N$.

[13] vgl. Jacobson-Radikal in der Ringtheorie

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. □

Satz 4.16 (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 4.15 zeigt $G = \mathrm{N}_G(P)$, d. h. $P \trianglelefteq G$. Dann ist auch $P \trianglelefteq \Phi(G)$ und die Behauptung folgt aus Satz 4.10.

(ii) Für $P \in \mathrm{Syl}_p(G)$ ist $P\Phi(G)/\Phi(G) \in \mathrm{Syl}_p(G/\Phi(G))$. Nach Satz 4.10 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 4.15 zeigt nun $G = \mathrm{N}_G(P)$ und $P \trianglelefteq G$. Die Behauptung folgt mit Satz 4.10.

(iii) Ist $D := G' \cap \mathrm{Z}(G) \not\subseteq \Phi(G)$, so existiert eine maximale Untergruppe $M < G$ mit $D \not\subseteq M$, 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 4.17 (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 4.10). 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 4.16. □

Satz 4.18. *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 $\Phi(P) \not\subseteq N$ 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 4.19 (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 4.20. *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 4.21. Sei P eine p-Gruppe und α ein nicht-trivialer p'-Automorphismus von P. Dann besagt Satz 4.20, 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 4.22. 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 4.19. Dies zeigt $P' = \Phi(P)$. Nach Satz 3.14 ist $P' \leq \mathrm{Z}(P)$ und nach Aufgabe 8 ist $P/\mathrm{Z}(P)$ nicht zyklisch. Also gilt $P' = \Phi(P) = \mathrm{Z}(P)$. Wir werden diese Gruppen später vollständig klassifizieren (Satz 9.9). Sei nun $\alpha \in \mathrm{Aut}(P)$ ein p'-Automorphismus. Nach Bemerkung 4.21 operiert α treu auf $P/\Phi(P)$. Wir können also $\alpha \in \mathrm{Aut}(P/\Phi(P)) \cong \mathrm{GL}(2, p)$ annehmen. Wegen

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

ist $|\langle\alpha\rangle|$ ein Teiler von $(p - 1)^2(p + 1)$.

Satz 4.23. *Seien p, q Primzahlen und $n \geq 1$. Dann ist jede Gruppe der Ordnung p^nq auflösbar.*

Beweis. Sei G ein minimales Gegenbeispiel. Sicher ist dann $p \neq q$. Sei $P \in \mathrm{Syl}_p(G)$. Im Fall $P \trianglelefteq G$ wäre G auflösbar, da P und G/P auflösbar sind (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 4.10. 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. □

Lemma 4.24. *Sei $N \trianglelefteq G$ mit nilpotenter Faktorgruppe G/N. Dann gilt:*

(i) Es existiert eine nilpotente Untergruppe $H \leq G$ mit $G = HN$.

(ii) Ist auch N nilpotent, so existiert eine nilpotente Untergruppe H mit $G = HN$ und $\mathrm{N}_G(H) = H$.

Beweis.

(i) Ist $N \leq \Phi(G)$, so ist $H = G$ nilpotent nach Frattini. Sei also $M < G$ maximal mit $N \not\subseteq M$. Dann ist $G = MN$ und $M/(M \cap N) \cong G/N$ ist nilpotent. Durch Induktion nach $|G|$ können wir annehmen, dass eine nilpotente Untergruppe $H \leq M$ mit $M = H(M \cap N)$ existiert. Es gilt nun $G = MN = H(M \cap N)N = HN$.

(ii) Wir wählen H wie in (i), sodass $|H|$ möglichst groß ist. Nach Dedekind ist $\mathrm{N}_G(H) = HN \cap \mathrm{N}_G(H) = H\mathrm{N}_N(G)$. Nach Voraussetzung sind H und $\mathrm{N}_N(H)$ nilpotente Normalteiler von $\mathrm{N}_G(H)$. Also ist auch $\mathrm{N}_G(H)$ nilpotent nach Fitting. Die Maximalität von $|H|$ zeigt $\mathrm{N}_G(H) = H$. □

Definition 4.25. Eine nilpotente Untergruppe $C \leq G$ heißt *Cartergruppe* von G, falls $\mathrm{N}_G(C) = C$ (*selbstnormalisierend*).

Beispiel 4.26.

(i) In einer nilpotenten Gruppe G ist G nach Satz 4.10 die einzige Cartergruppe.

(ii) Die 2-Sylowgruppen von S_4 sind Cartergruppen.

(iii) Sei C eine Cartergruppe von $G = A_5$. Da G keine Elemente der Ordnung 6, 10 oder 15 besitzt, muss C eine p-Gruppe sein. Nach Sylow und Satz 4.10 ist C sogar eine p-Sylowgruppe von G. Die Fälle $p \in \{3, 5\}$ sind wegen $|G : \mathrm{N}_G(C)| = |G : C| \not\equiv 1 \pmod{p}$ ausgeschlossen. Sei also $C = V_4$. Dann wäre aber $A_4 \leq \mathrm{N}_G(C) = C$. Somit besitzt A_5 keine Cartergruppe. Der folgende Satz impliziert, dass A_5 nicht auflösbar ist.

Satz 4.27 (Carter). *Jede auflösbare Gruppe besitzt genau eine Cartergruppe bis auf Konjugation.*

Beweis. Wir argumentieren durch Induktion nach $|G|$ und wählen einen minimalen Normalteiler $N \trianglelefteq G$. Nach Satz 2.28 ist N eine (elementar)abelsche p-Gruppe.

Nach Induktion besitzt G/N eine Cartergruppe K/N. Lemma 4.24 liefert eine nilpotente Untergruppe $C \leq K$ mit $K = CN$ und $\mathrm{N}_K(C) = C$. Es folgt

$$\mathrm{N}_G(C)N/N \leq \mathrm{N}_G(K)/N \leq \mathrm{N}_{G/N}(K/N) = K/N$$

und $\mathrm{N}_G(C) = \mathrm{N}_K(C) = C$. Also ist C eine Cartergruppe von G.

Sei umgekehrt $D \leq G$ eine Cartergruppe von G. Dann ist DN/N nilpotent und im Fall $DN = G$ auch selbstnormalisierend in G/N. Sei nun $DN < G$. Nach Induktion sind dann die Cartergruppen von DN konjugiert. Das Frattini-Argument liefert $\mathrm{N}_G(DN) = \mathrm{N}_G(D)N = DN$. Also ist DN/N in jedem Fall eine Cartergruppe von G/N. Nach Induktion sind CN und DN konjugiert. O. B. d. A. sei $CN = G = DN$. Ist G nilpotent, so gilt $C = G = D$ nach Satz 4.10. Sei also $C, D < G$. Da N abelsch ist, gilt $G = CN \leq \mathrm{N}_G(C \cap N)$. Die Minimalität von N ergibt $C \cap N = 1 = D \cap N$. Da G nicht nilpotent ist, existiert ein Primteiler $q \neq p$ von $|C| = |D|$. Sei $Q \in \mathrm{Syl}_q(C) \subseteq \mathrm{Syl}_q(G)$. Da C nilpotent ist, folgt $C \leq \mathrm{N}_G(Q)$. Im Fall $Q \trianglelefteq G$ ist $Q \leq D$. Als Cartergruppen von G/Q sind dann C/Q und D/Q konjugiert nach Induktion. Sei also $\mathrm{N}_G(Q) < G$. Wegen $G = CN \leq \mathrm{N}_G(\mathrm{N}_N(Q))$ ist $\mathrm{N}_N(Q) = 1$ und $\mathrm{N}_G(Q) = C$. Analog existiert $R \in \mathrm{Syl}_q(G)$ mit $\mathrm{N}_G(R) = D$. Nach Sylow sind Q und R sowie $\mathrm{N}_G(Q)$ und $\mathrm{N}_G(R)$ konjugiert. □

Bemerkung 4.28. Mit der Klassifikation der einfachen Gruppen hat Vdovin bewiesen, dass jede Gruppe höchstens eine Cartergruppe bis auf Konjugation besitzt. Die p-Sylowgruppen einer beliebigen Gruppe können also nur für höchstens eine Primzahl p selbstnormalisierend sein. Besitzt G selbstnormalisierende p-Sylowgruppen für $p > 3$, so ist G auflösbar nach einem Satz von Guralnick-Malle-Navarro.

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 $N \trianglelefteq G$. In Abschnitt 7 suchen wir hingegen *normale* Komplemente $H \trianglelefteq G$.

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

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

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

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

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

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

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

Beispiel 5.4.

(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 4.10 hat jede Sylowgruppe einer nilpotenten Gruppe ein Komplement.

(v) Nach Aufgabe 24 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 $C_4 \ncong C_2^2$.

Satz 5.5 (Rose)**.** *Für jede endliche Gruppe G sind die folgenden Aussagen äquivalent:*

(1) $\mathrm{Z}(G) = 1$ *und* $\mathrm{Inn}(G)$ *besitzt ein Komplement in* $\mathrm{Aut}(G)$*.*

(2) Ist G ein Normalteiler einer endlichen Gruppe H, so besitzt G ein Komplement in H.

Beweis.

(1)⇒(2): Für $N := \mathrm{C}_H(G) \trianglelefteq H$ ist $G \cap N = \mathrm{Z}(G) = 1$ und $\mathrm{Inn}(G) \cong GN/N \trianglelefteq H/N \leq \mathrm{Aut}(G)$. Also existiert $K/N \leq H/N$ mit $H = GK$ und $GN \cap K = N$. Es folgt $G \cap K \leq G \cap GN \cap K = G \cap N = 1$.

(2)⇒(1): Angenommen $|\mathrm{Z}(G)|$ ist durch eine Primzahl p teilbar. Sei $x \in \mathrm{Z}(G)$ mit Ordnung p und sei p^n die maximale Ordnung eines p-Elements in G. Sei $C = \langle y \rangle \cong C_{p^{n+1}}$ und

$$Z := \langle (x^{-1}, y^{p^n}) \rangle \leq \mathrm{Z}(G \times C).$$

Wir definieren $H := (G \times C)/Z$ (ein Zentralprodukt, siehe Definition 9.14). Offenbar ist $f\colon G \to H$, $g \mapsto (g, 1)Z$ ein Monomorphismus. Nach Voraussetzung besitzt $f(G)$ ein Komplement $K \leq H$. Nach Konstruktion ist $[f(G), K] = 1$ und $H = f(G) \times K$. Wegen $|K| = |H|/|G| = p^n$ besitzt H kein Element der Ordnung p^{n+1}. Andererseits ist aber $C \to H$, $y \mapsto (1, y)Z$ ein Monomorphismus. Dieser Widerspruch zeigt $\mathrm{Z}(G) = 1$. Nun besitzt $\mathrm{Inn}(G) \cong G$ ein Komplement in $\mathrm{Aut}(G)$. □

Bemerkung 5.6. 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 ${}^g(xy) = ({}^g x)({}^g y)$.

Lemma 5.7. *Sei $\varphi\colon H \to \mathrm{Aut}(N)$ ein Homomorphismus für Gruppen H, N. Dann wird $G := N \times H$ mittels*

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

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 neutrales Element. 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 5.8. Man nennt G das *semidirekte Produkt* von N mit H und schreibt $G = N \rtimes_\varphi H$. [14]

Bemerkung 5.9.

(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 5.10. *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.

[14] seltener findet man die Notation $N \leftthreetimes H$

Für die zweite Behauptung betrachten wir die kurze exakte Folge

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

Nach Bemerkung 5.3 genügt es zu zeigen, dass diese Folge zerfällt. Dies sieht man mit dem Homomorphismus $H \to G$, $h \mapsto (1, h)$. □

Beispiel 5.11.

(i) Nach Aufgabe 3 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 6). 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 24 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 5.12. *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 4.19. 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 29 ist der Isomorphietyp dieser Gruppe durch p und q eindeutig bestimmt. □

Beispiel 5.13. Bis auf Isomorphie sind C_{21} und $C_7 \rtimes C_3$ die einzigen Gruppen der Ordnung 21.

Lemma 5.14. *Sei $N \trianglelefteq G$ und $H \leq G$ minimal bzgl. der Eigenschaft $G = HN$. Dann ist $H \cap N \leq \Phi(H)$.*

Beweis. Im Fall $H \cap N \nleq \Phi(H)$ existiert eine maximale Untergruppe $M < H$ mit $M(H \cap N) = H$ (beachte $H \cap N \trianglelefteq H$). Dann wäre aber $G = HN = MN$ ein Widerspruch zur Wahl von H. □

Satz 5.15. *Sei A das Produkt aller abelschen minimalen Normalteiler von G. Dann sind die folgenden Aussagen äquivalent:*

(1) Jeder abelsche Normalteiler von G besitzt ein Komplement.

(2) A besitzt ein Komplement.

(3) $\Phi(G) = 1$.

Beweis.

(1)⇒(2): Für zwei abelsche minimale Normalteiler $B, C \trianglelefteq G$ gilt $[B, C] \leq B \cap C = 1$. Daher ist A abelsch und (2) folgt.

(2)⇒(3): Sei $G = A \rtimes K$ und indirekt $\Phi(G) \neq 1$. Sei $N \leq \Phi(G)$ ein minimaler Normalteiler von G. Da $\Phi(G)$ nilpotent ist, gilt $N \leq A$. Als Produkt von (vertauschbaren) elementarabelschen Gruppen ist A ein direktes Produkt von Gruppen von Primzahlordnung. Insbesondere ist $\Phi(A) = 1$ nach Aufgabe 23. Daher existiert eine maximale Untergruppe $B < A$ mit $A = NB$. Nun ist $G = AK = NBK = \Phi(G)BK = BK$ im Widerspruch zu $|BK| = |B||K| < |A||K| = |G|$.

(3)⇒(1): Sei $1 \neq N \trianglelefteq G$ abelsch und $H \leq G$ wie in Lemma 5.14. Dann gilt $H \cap N \trianglelefteq H$ und $H \cap N \trianglelefteq N$, da N abelsch ist. Dies zeigt $H \cap N \trianglelefteq HN = G$. Aus Lemma 4.15 folgt $H \cap N \leq \Phi(G) = 1$, d. h. H ist ein Komplement von N in G. □

Bemerkung 5.16. 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 5.17. Sei $A \trianglelefteq G$ abelsch und $A \leq H \leq G$. Sei K ein Komplement von A in H. Für $x, y \in G$ mit $xH = yH$ existiert genau ein $\kappa_{x,y} \in K$ mit $x^{-1}yA = \kappa_{x,y}A$. Sei $\mathcal{R}$ die Menge der Repräsentantensysteme für G/H. Für $R, S \in \mathcal{R}$ sei

$$(R|S) := \prod_{\substack{(r,s)\in R\times S\\ rH=sH}} r\kappa_{r,s}s^{-1} \in A$$

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

Lemma 5.18. *Für $R, S, T \in \mathcal{R}$, $g \in G$ und $a \in A$ 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) $(aR|S) = a^{|G:H|}(R|S)$.

Beweis.

(i) Aus $\kappa_{r,r}A = A$ folgt $(R|R) = 1$. Wegen $\kappa_{r,s}^{-1}A = (r^{-1}s)^{-1}A = s^{-1}rA = \kappa_{s,r}A$ gilt

$$(R|S)^{-1} = \prod_{\substack{(r,s)\in R\times S\\ rH=sH}} (r\kappa_{r,s}s^{-1})^{-1} = \prod_{\substack{(r,s)\in R\times S\\ rH=sH}} s\kappa_{s,r}r^{-1} = (S|R).$$

(ii) Aus $\kappa_{r,s}\kappa_{s,t}A = r^{-1}ss^{-1}tA = r^{-1}tA = \kappa_{r,t}A$ folgt

$$(R|S)(S|T) = \prod_{\substack{(r,s)\in R\times S\\ rH=sH}} r\kappa_{r,s}s^{-1} \prod_{\substack{(s,t)\in S\times T\\ sH=tH}} s\kappa_{s,t}t^{-1} = \prod_{\substack{(r,t)\in R\times T\\ rH=tH}} r\kappa_{r,t}t^{-1} = (R|T).$$

(iii) Für $x, y \in R$ gilt $gxH = gyH \Leftrightarrow xH = yH \Leftrightarrow x = y$. Dies zeigt $gR, gS \in \mathcal{R}$. Wegen $\kappa_{gr,gs}A = (gr)^{-1}gsA = r^{-1}sA = \kappa_{r,s}$ ist

$$(gR|gS) = \prod_{\substack{(gr,gs)\in gR\times gS\\ grH=gsH}} gr\kappa_{gr,gs}s^{-1}g^{-1} = g\Big(\prod_{\substack{(r,s)\in R\times S\\ rH=sH}} r\kappa_{r,s}s^{-1}\Big)g^{-1} = g(R|S)g^{-1}.$$

(iv) Es gilt $\kappa_{ar,s}A = (ar)^{-1}sA = r^{-1}sA = \kappa_{r,s}A$. Da A abelsch ist, kann man a aus den $|G:H|$ Faktoren herausziehen:

$$(aR|S) = \prod_{\substack{(ar,s)\in aR\times S\\ arH=sH}} ar\kappa_{ar,s}s^{-1} = a^{|G:H|}\prod_{\substack{(r,s)\in R\times S\\ rH=sH}} r\kappa_{r,s}s^{-1} = a^{|G:H|}(R|S). \qquad \square$$

Bemerkung 5.19. Für $x, y \in G$ schreiben wir im Folgenden $x^y := y^{-1}xy$ und $x^{-y} := (x^y)^{-1}$. Offenbar gilt $x^1 = x$, $(x^y)^z = x^{yz}$ und $(xy)^z = x^z y^z$ für $x, y, z \in G$.

Definition 5.20. Seien $H \leq G$ endliche Gruppen. Eine Abbildung $\alpha\colon G \to H$ mit $\alpha(xy) = \alpha(x)^y\alpha(y)$ für alle $x, y \in G$ heißt *verschränkter Homomorphismus*. Wie üblich sei $\mathrm{Ker}(\alpha) := \{x \in G : \alpha(x) = 1\}$.

Lemma 5.21. *Für jeden verschränkten Homomorphismus $\alpha\colon G \to H$ gilt $\mathrm{Ker}(\alpha) \leq G$.*

Beweis. Aus $\alpha(1) = \alpha(1\cdot 1) = \alpha(1)^1\alpha(1) = \alpha(1)^2$ folgt $\alpha(1) = 1$. Für $x, y \in \mathrm{Ker}(\alpha)$ gilt $\alpha(xy) = \alpha(x)^y\alpha(y) = 1^y 1 = 1$, also $xy \in \mathrm{Ker}(\alpha)$. $\square$

Satz 5.22 (Gaschütz)**.** *Sei $A \trianglelefteq G$ abelsch und $A \leq H \leq G$ mit $\mathrm{ggT}(|A|, |G:H|) = 1$. Dann gilt*

(i) Besitzt A ein Komplement in H, so auch in G.

(ii) Sind L_1, L_2 Komplemente von A in G mit $H \cap L_1 = H \cap L_2$, so sind L_1 und L_2 in G konjugiert.

(iii) Sind je zwei Komplemente von A in H konjugiert, so sind auch je zwei Komplemente von A in G konjugiert.

Beweis (Brandis).

(i) Sei K ein Komplement von A in H und $R \in \mathcal{R}$ mit den Bezeichnungen aus Definition 5.17. Für $x \in G$ sei $\alpha(x) := (x^{-1}R|R) \in A$. Nach Lemma 5.18 gilt

$$\alpha(xy) = (y^{-1}x^{-1}R|R) = (y^{-1}x^{-1}R|y^{-1}R)(y^{-1}R|R) = (x^{-1}R|R)^y(y^{-1}|R) = \alpha(x)^y\alpha(y)$$

für $x, y \in G$. Also ist α ein verschränkter Homomorphismus und $L := \mathrm{Ker}(\alpha) \leq G$ nach Lemma 5.21. Für $a \in A$ gilt $\alpha(a) = (a^{-1}R|R) = a^{-|G:H|}(R|R) = a^{-|G:H|}$. Wegen $\mathrm{ggT}(|A|, |G:H|) = 1$ ist die Einschränkung $\alpha_{|A}$ ein Automorphismus von A. Insbesondere ist $L \cap A = 1$. Für $g \in G$ existiert außerdem ein $a \in A$ mit $1 = \alpha(g)\alpha(a) = \alpha(g)^a\alpha(a) = \alpha(ga)$. Dies zeigt $g = (ga)a^{-1} \in LA$. Also ist L ein Komplement von A in G.

(ii) Nach Beispiel 5.4 ist $K := H \cap L_i$ ein Komplement von A in H. Wir konstruieren $(R|S)$ bzgl. K. Seien $R_1, R_2 \in \mathcal{R}$ mit $R_i \subseteq L_i$. Für $i = 1, 2$ konstruieren wir α_i wie in (i) mit Hilfe von R_i. Für $x \in L_i$ und $r, s \in R_i$ gilt

$$xrH = sH \implies (xr)^{-1}s \in H \cap L_i = K \implies \kappa_{xr,x} = (xr)^{-1}s.$$

Dies zeigt

$$\alpha_i(x^{-1}) = (xR_i|R_i) = \prod_{\substack{(xr,s)\in xR_1\times R_1\\ xrH=sH}} xr\kappa_{xr,s}s^{-1} = 1$$

und $L_i \leq \mathrm{Ker}(\alpha_i)$. Nach (i) ist $|L_i| = |\mathrm{Ker}(\alpha_i)|$, also $L_i = \mathrm{Ker}(\alpha_i)$ für $i = 1, 2$.

Sei nun $a := (R_1|R_2) \in A$ und $x \in G$. Nach (i) existiert $b \in A$ mit $\alpha_2(b) = a$. Es gilt

$$\alpha_1(x) = (x^{-1}R_1|R_1) \overset{5.18}{=} (x^{-1}R_1|x^{-1}R_2)(x^{-1}R_2|R_2)(R_2|R_1) = a^x\alpha_2(x)a^{-1}$$
$$= \alpha_2(b)^x\alpha_2(x)\alpha_2(b)^{-1} \overset{\text{(i)}}{=} \alpha_2(bx)\alpha_2(b^{-1}) = \alpha_2(bx)^{b^{-1}}\alpha_2(b^{-1}) = \alpha_2(bxb^{-1}).$$

Es folgt $L_2 = \mathrm{Ker}(\alpha_2) = b\mathrm{Ker}(\alpha_1)b^{-1} = bL_1b^{-1}$.

(iii) Seien L_1, L_2 Komplemente von A in G. Dann sind $H \cap L_1, H \cap L_2$ Komplemente von A in H. Nach Voraussetzung existiert $h \in H$ mit $H \cap hL_1h^{-1} = h(H \cap L_1)h^{-1} = H \cap L_2$. Die Behauptung folgt nun aus (ii). □

Satz 5.23. *Sei $A \trianglelefteq G$ abelsch. Genau dann besitzt A ein Komplement in G, wenn jede Sylowgruppe von A ein Komplement in einer Sylowgruppe von G besitzt.*

Beweis. Sei K ein Komplement von A in G und $K_p \in \mathrm{Syl}_p(K)$. Sei $K_p \leq P \in \mathrm{Syl}_p(G)$. Da A abelsch ist, ist $A \cap P = \mathrm{O}_p(A) \trianglelefteq G$ die einzige p-Sylowgruppe von A und $(A \cap P) \cap K_p \leq A \cap K = 1$. Wegen $|A \cap P||K_p| = |A|_p|K|_p = |G|_p = |P|$ ist K_p ein Komplement von $A \cap P$ in P.

Die Umkehrung beweisen wir durch Induktion nach der Anzahl der Primteiler $p_1, \ldots, p_s$ von $|A|$. Sei $P_1 \in \mathrm{Syl}_{p_1}(G)$. Dann besitzt $A \cap P_1 = \mathrm{O}_{p_1}(A) \trianglelefteq G$ ein Komplement in P_1 und nach Gaschütz auch ein Komplement K_1 in G. Sei also $s \geq 2$. Für $i \geq 2$ sei $P_i \in \mathrm{Syl}_{p_i}(K_1) \subseteq \mathrm{Syl}_{p_i}(G)$. Dann besitzt $(A \cap K_1) \cap P_i = A \cap P_i$ ein Komplement in P_i. Nach Induktion besitzt $A \cap K_1$ ein Komplement K in K_1. Es gilt nun $G = (A \cap P_1)K_1 = (A \cap P_1)(A \cap K_1)K \leq AK$ und $A \cap K = A \cap K_1 \cap K = 1$. □

Satz 5.24 (Evans-Shin)**.** *Seien K und L Komplemente des abelschen Normalteilers $A \trianglelefteq G$. Ist jede Sylowgruppe von K zu einer Sylowgruppe von L konjugiert, so sind K und L konjugiert.*

Beweis. Sei G ein minimales Gegenbeispiel. Sei p ein Primteiler von $|A|$ und $B := \mathrm{O}_{p'}(A)$. Nehmen wir $B \neq 1$ an. Dann sind KB/B und LB/B Komplemente von A/B in G/B. Ist P eine Sylowgruppe von K, so ist PB/B eine Sylowgruppe von KB/B. Nach Voraussetzung existiert ein $g \in G$, sodass gKg^{-1} eine Sylowgruppe von L ist. Offenbar ist $gKg^{-1}B/B$ eine Sylowgruppe von LB/B. Da G ein minimales Gegenbeispiel ist, existiert ein $g \in G$ mit $H := gKg^{-1}B = LB$. Nun sind gKg^{-1} und L Komplemente von B in H mit den gleichen Voraussetzung. Wegen $B < A$ folgt der Widerspruch, dass gKg^{-1} und L in G konjugiert sind. Also ist $B = 1$ und A ist eine p-Gruppe. Nach Konjugation dürfen wir annehmen, dass K und L eine gemeinsame p-Sylowgruppe P besitzen. Dann ist $H := PA \in \mathrm{Syl}_p(G)$. Nun folgt die Behauptung aus Satz 5.22(ii). □

Satz 5.25. *Seien K und L Komplemente des abelschen Normalteilers $A \trianglelefteq G$. Dann existiert ein $\alpha \in \mathrm{Aut}(G)$ mit $\alpha(K) = L$ und $\alpha_A = \mathrm{id}_A$.*

Beweis. Wegen $K \cong G/A \cong L$ existiert ein Isomorphismus $\varphi\colon K \to L$ mit $\varphi(x) \equiv x \pmod{A}$ für alle $x \in K$. Da A abelsch ist, gilt $\varphi(x)a\varphi(x)^{-1} = xax^{-1}$ für alle $x \in K$ und $a \in A$. Offenbar ist $\alpha\colon G \to G$, $xa \mapsto \varphi(x)a$ für $x \in K$ und $a \in A$ eine wohldefinierte Bijektion. Für $x, y \in K$ und $a, b \in A$ gilt

$$\alpha(xa \cdot yb) = \alpha(xy \cdot y^{-1}ayb) = \varphi(xy)y^{-1}ayb = \varphi(x)\varphi(y)\varphi(y)^{-1}a\varphi(y)b = \varphi(x)a\varphi(y)b = \alpha(xa)\alpha(yb).$$

Also ist $\alpha \in \mathrm{Aut}(G)$ mit $\alpha(K) = \varphi(K) = L$ und $\alpha_A = \mathrm{id}_A$. □

Satz 5.26. *Sei G eine endliche Gruppe mit elementarabelschen Sylowgruppen (für jede Primzahl). Dann besitzt jeder Normalteiler von G ein Komplement.*

Beweis. Sei $N \trianglelefteq G$. Wir argumentieren durch Induktion nach $|N|$. Angenommen N besitzt eine nicht-normale p-Sylowgruppe P. Nach Bemerkung 4.6 ist $G = N\mathrm{N}_G(P)$ und $\mathrm{N}_N(P) < N$. Nach Induktion besitzt $\mathrm{N}_N(P)$ ein Komplement K in $\mathrm{N}_G(P)$. Es gilt $G = N\mathrm{N}_G(P) = N\mathrm{N}_N(P)K = NK$ und $N \cap K = N \cap \mathrm{N}_N(P) \cap K = 1$. Wir können daher annehmen, dass N nilpotent ist (Satz 4.10). Nach Voraussetzung ist N sogar abelsch und jede Sylowgruppe von N besitzt ein Komplement in einer (elementarabelschen) Sylowgruppe von G (Beispiel 5.4). Die Behauptung folgt nun aus Satz 5.23. □

Bemerkung 5.27. Die einfache Gruppe A_6 (siehe Satz 6.38) mit 2-Sylowgruppe D_8 zeigt, dass die Umkehrung von Satz 5.26 falsch ist.

Satz 5.28. *Für jede auflösbare Gruppe G sind die folgenden Aussagen äquivalent:*

(1) Jeder Normalteiler von G besitzt ein Komplement.

(2) Für alle $N \trianglelefteq G$ gilt $\Phi(G/N) = 1$.

Beweis.

(1)⇒(2): Sei $M/N := \Phi(G/N) \trianglelefteq G/N$. Sei $K \leq G$ ein Komplement von M in G. Dann gilt

$$G/N = MK/N = \Phi(G/N) \cdot KN/N = KN/N$$

also $G = KN$. Es folgt $M = KN \cap M = N(K \cap M) = N$, d. h. $\Phi(G/N) = 1$.

(2)⇒(1): Induktion nach $|G|$: Sei $1 \neq N \trianglelefteq G$. Sei $M \leq N$ ein minimaler Normalteiler von G. Da G auflösbar ist, ist M (elementar)abelsch. Wegen $\Phi(G) = \Phi(G/1) = 1$ besitzt M nach Satz 5.15 ein Komplement H in G. Wegen $H \cong G/M$ überträgt sich die Voraussetzung von G nach H mit dem zweiten Isomorphiesatz. Nach Induktion besitzt $H \cap N \trianglelefteq H$ ein Komplement K in H. Es gilt $G = HM = K(H \cap N)M \leq KN$ und $K \cap N = K \cap H \cap N = 1$, d. h. K ist ein Komplement von N in G. □

Satz 5.29 (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 4.8 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. Dann folgt die Behauptung aus Gaschütz mit $N = A = H$.

Schritt 2: Eindeutigkeit.
Fall 1: N auflösbar.
Induktion nach $|N|$: Ist N abelsch, so folgt die Behauptung aus Gaschütz mit $N = A = H$. 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 5.30.

(i) 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 5.29 also eigentlich überflüssig (der Beweis hat 250 Seiten).

(ii) Im Gegensatz zu Schur-Zassenhaus ist der Satz von Gaschütz für nichtabelsche Normalteiler A im Allgemeinen falsch.[15]

Folgerung 5.31. *Für $N \trianglelefteq G$ existiert ein $H \leq G$ mit $G = NH$, sodass $|H|$ und $|G/N|$ die gleichen Primteiler haben.*

Beweis. Wähle H wie in Lemma 5.14 (notfalls $H = G$). Angenommen $H \cap N$ enthält eine nicht-triviale p-Sylowgruppe P von H. Da $H \cap N \leq \Phi(H)$ nilpotent ist, gilt $P \trianglelefteq H$. Nach Schur-Zassenhaus besitzt P ein Komplement K in H. Damit folgt der Widerspruch $H = PK \leq \Phi(H)K = K$. Also ist jeder Primteiler von $|H|$ auch ein Teiler von $|H : H \cap N| = |HN/N| = |G/N|$. □

Bemerkung 5.32. Offenbar verallgemeinert Folgerung 5.31 den Satz von Schur-Zassenhaus. In Satz 7.47 lernen wir eine weitere Verallgemeinerung kennen.

Definition 5.33. 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 5.34.

(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 4.10).

(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 (erneut), dass A_5 nicht auflösbar ist.

[15] Das Zentralprodukt (siehe Definition 9.14) $G = \mathrm{SL}(2, 3) * C_4$ mit $A \cong Q_8$ und $H = Q_8 * C_4$ ist ein Gegenbeispiel für Satz 5.22(i) und $G = \mathrm{GL}(2, 3)$ mit $A = \mathrm{O}_2(G) \cong Q_8$ und $H \in \mathrm{Syl}_2(G)$ ist ein Gegenbeispiel für (ii) und (iii).

Satz 5.35 (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 5.36.

(i) Man kann umgekehrt zeigen, dass G auflösbar ist, falls p'-Hallgruppen für jeden Primteiler p von $|G|$ existieren (siehe Unterabschnitt A.1). Dies verallgemeinert Burnsides $p^a q^b$-Satz.

(ii) Gross hat im Fall $2 \notin \pi$ bewiesen, dass je zwei π-Hallgruppen einer beliebigen endlichen Gruppe konjugiert sind. Der Beweis benutzt die CFSG. 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 5.30).

Satz 5.37. *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. □

Definition 5.38. Seien $p_1, \ldots, p_n$ die Primteiler von $|G|$ und $P_i \in \mathrm{Syl}_{p_i}(G)$. Man nennt $(P_1, \ldots, P_n)$ ein *Sylowsystem* von G, falls $P_i P_j \leq G$ für alle $1 \leq i, j \leq n$ gilt (nach Lemma 1.9 ist dies äquivalent zu $P_i P_j = P_j P_i$). Sei $\mathcal{S}(G)$ die Menge aller Sylowsysteme von G.

Lemma 5.39. *Seien $p_1, \ldots, p_n$ die Primteiler von $|G|$. Sei $\mathcal{H}$ die Menge aller Folgen $(H_1, \ldots, H_n)$, sodass H_i für $i = 1, \ldots, n$ eine p_i'-Hallgruppe von G ist. Dann sind die Abbildungen*

$$\mathcal{H} \to \mathcal{S}(G), \qquad (H_i)_i \mapsto \Big(\bigcap_{j\neq i} H_j\Big)_i$$

$$\mathcal{S}(G) \to \mathcal{H}, \qquad (P_i)_i \mapsto \Big(\prod_{j\neq i} P_j\Big)_i$$

zueinander inverse Bijektionen.

Beweis. Sei $|G| = p_1^{a_1} \ldots p_n^{a_n}$ die Primfaktorzerlegung von $|G|$ und $(H_1, \ldots, H_n) \in \mathcal{H}$. Wir zeigen $|G : H_{i_1} \cap \ldots \cap H_{i_k}| = p_{i_1}^{a_1} \ldots p_{i_k}^{a_k}$ für $1 \leq i_1 < \ldots < i_k \leq n$ durch Induktion nach k. Der Fall $k = 1$ ist die Hallgruppeneigenschaft. Da $|G : H|$ und $|G : H_{i_1}|$ teilerfremd sind, folgt

$$|G : H_{i_1} \cap H| = |G : H_{i_1}||G : H| = p_{i_1}^{a_1} \ldots p_{i_k}^{a_k}$$

aus Lemma 1.9. Der Fall $k = n - 1$ liefert $P_i := \bigcap_{j\neq i} H_j \in \mathrm{Syl}_{p_i}(G)$ für $i = 1, \ldots, n$. Wegen $P_iP_j \subseteq \bigcap_{i\neq l\neq j} H_l$ und $|\bigcap_{i\neq l\neq j} H_l| = |P_i||P_j|$ ist

$$P_iP_j = \bigcap_{i\neq l\neq j} H_l = P_jP_i.$$

Dies zeigt $(P_1, \ldots, P_n) \in \mathcal{S}(G)$.

Sei umgekehrt $(P_1, \ldots, P_n) \in \mathcal{S}(G)$ gegeben. Wir zeigen $P_{i_1} \ldots P_{i_k} \leq G$ für $i_1 < \ldots < i_k$. Dies ist klar für $k = 1$. Sei $P := P_{i_2} \ldots P_{i_k} \leq G$. Aus der Eigenschaft des Sylowsystems folgt

$$P_{i_1}P = P_{i_2}P_{i_1}P_{i_3} \ldots P_{i_k} = \ldots = P_{i_2} \ldots P_{i_k}P_{i_1} = PP_{i_1} \leq G.$$

Offenbar ist $H_i := \prod_{j\neq i} P_j$ eine p_i'-Hallgruppe und $(H_1, \ldots, H_n) \in \mathcal{H}$. Wegen

$$\prod_{j\neq i} \bigcap_{l\neq j} H_l \subseteq H_i, \qquad P_i \subseteq \bigcap_{j\neq i} \prod_{l\neq j} P_j$$

sind die angegebenen Abbildungen zueinander invers. □

Bemerkung 5.40. Wir nennen Sylowsysteme (P_i) und (Q_i) von G *konjugiert*, falls ein g mit $gP_ig^{-1} = Q_i$ für alle i existiert. Der folgende Satz ist eine Verallgemeinerung von Sylow für auflösbare Gruppen.

Satz 5.41 (Hall)**.** *Jede auflösbare Gruppe G besitzt ein Sylowsystem und je zwei Sylowsysteme von G sind konjugiert.*

Beweis. Seien $p_1, \ldots, p_n$ die Primteiler von $|G|$. Nach Hall besitzt G für jedes i eine p_i'-Hallgruppe H_i. Nach Lemma 5.39 ist $S := (P_1, \ldots, P_n)$ mit $P_i := \bigcap_{j\neq i} H_j$ ein Sylowsystem von G. Wegen $H_i = \prod_{j\neq i} P_j$ gilt $\bigcap_{i=1}^n \mathrm{N}_G(H_i) = \bigcap_{i=1}^n \mathrm{N}_G(P_i)$. Da Hallgruppen der gleichen Ordnung konjugiert sind, ist $|G : \mathrm{N}_G(H_i)|$ die Anzahl der p_i'-Hallgruppen in G. Wegen $H_i \leq \mathrm{N}_G(H_i)$ ist $|G : \mathrm{N}_G(H_i)|$ eine p_i-Potenz. Insbesondere sind die $|G : \mathrm{N}_G(H_i)|$ paarweise teilerfremd. Aus Lemma 1.9 und Lemma 5.39 folgt

$$|\mathcal{S}(G)| = |\mathcal{H}| = \prod_{i=1}^n |G : \mathrm{N}_G(H_i)| = |G : \mathrm{N}_G(H_1) \cap \ldots \cap \mathrm{N}_G(H_n)| = |G : \mathrm{N}_G(P_1) \cap \ldots \cap \mathrm{N}_G(P_n)| = |{}^G S|.$$

Dies zeigt, dass jedes Sylowsystem zu S konjugiert ist. □

Satz 5.42 (Hall-Higman-Lemma)**.** *Sei jeder Kompositionsfaktor von G eine π-Gruppe oder eine π'-Gruppe. Gilt $\mathrm{O}_\pi(G) = 1$, so ist $\mathrm{C}_G(\mathrm{O}_{\pi'}(G)) \leq \mathrm{O}_{\pi'}(G)$.*

Beweis. Sei $N := \mathrm{O}_{\pi'}(G)$. Dann ist $\mathrm{C}_G(N)N/N \trianglelefteq G/N$. Im Fall $\mathrm{C}_G(N) \not\subseteq N$ existiert ein minimaler Normalteiler $M/N \trianglelefteq G/N$ mit $M \leq \mathrm{C}_G(N)N$. Als Hauptfaktor ist M/N eine direkte Summe von isomorphen Kompositionsfaktoren (Satz 2.28). Wegen $\mathrm{O}_{\pi'}(G/N) = 1$ muss M/N nach Voraussetzung eine π-Gruppe sein. Nach Schur-Zassenhaus ist $M = N \rtimes H$ mit $H \neq 1$. Da $\mathrm{C}_G(N)N/\mathrm{C}_G(N) \cong N/\mathrm{Z}(N)$ eine π'-Gruppe ist, gilt $H \leq \mathrm{C}_G(N)$ und $M = N \times H$. Dann wäre aber $H \leq \mathrm{O}_\pi(M) \leq \mathrm{O}_\pi(G) = 1$. □

Satz 5.43 (Galois)**.** *Sei N ein minimaler Normalteiler der auflösbaren Gruppe G mit $\mathrm{C}_G(N) \leq N$. Dann besitzt N ein Komplement in G und je zwei Komplemente sind in G konjugiert.*

Beweis. Bekanntlich ist N eine elementarabelsche p-Gruppe für eine Primzahl p. Wir können $N < G$ annehmen. Sei M/N ein minimaler Normalteiler von G/N. Dann ist M/N eine elementarabelsche q-Gruppe für eine Primzahl q. Nehmen wir zunächst $q = p$ an. Dann ist M ein p-Normalteiler von G und M. Nach Satz 3.14 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. □

Bemerkung 5.44. Der folgende Satz ist nützlich für die Konstruktion von minimalen Gegenbeispielen.

Satz 5.45 (Schmidt)**.** *Sei jede echte Untergruppe von G nilpotent, aber G selbst nicht. Dann ist $G \cong Q \rtimes C_{p^n}$ mit $Q \in \mathrm{Syl}_q(G)$ für Primzahlen p, q und $n \geq 1$.*

Beweis. Induktion nach $|G|$: Nehmen wir zunächst an es existiert ein echter Normalteiler $N \neq 1$. Nach Voraussetzung ist N nilpotent. Für $U/N < G/N$ ist $U < G$ nilpotent und damit auch U/N. Nach Induktion ist also G/N auflösbar. Daher ist auch G auflösbar. Nehmen wir nun an, dass G nichtabelsch und einfach ist. Seien M_1 und M_2 zwei verschiedene maximale Untergruppen von G, sodass $D := M_1 \cap M_2$ möglichst groß ist. Nehmen wir $D \neq 1$ an. Nach Satz 4.10 ist dann

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

für $i = 1, 2$. Nun liegt $\mathrm{N}_G(D)$ in einer maximalen Untergruppe $M_3 < G$. Wegen $\mathrm{N}_{M_i}(D) \leq M_i \cap M_3$ ist dann $M_i = M_3$ nach Wahl von M_1 und M_2. Dies liefert aber den Widerspruch $M_1 = M_3 = M_2$. Also ist $D = 1$, d. h. je zwei verschiedene maximale Untergruppen von G schneiden sich trivial. Sei

$M_1, \dots, M_s$ ein Repräsentantensystem für die Konjugationsklassen von maximalen Untergruppen. Wegen $\mathrm{N}_G(M_i) = M_i$ hat M_i genau $|G : M_i|$ Konjugierte. Es gilt daher

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

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

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

Satz 5.46 (Wielandt)**.** *Sei $H \leq G$ eine nilpotente Hallgruppe und $U \leq G$ mit $|U| \mid |H|$. Dann existiert ein $g \in G$ mit $gUg^{-1} \leq H$. Insbesondere sind alle Untergruppen der Ordnung $|H|$ zu H konjugiert und daher nilpotent.*

Beweis. Induktion nach $|U|$. O. B. d. A. sei $U \neq 1$. Jede echte Untergruppe von U ist dann zu einer Untergruppe von H konjugiert. Insbesondere ist jede echte Untergruppe von U nilpotent. Nach Satz 5.45 existiert eine Zerlegung $U = Q \rtimes P$ mit $1 \neq P \in \mathrm{Syl}_p(U)$ und $Q \trianglelefteq U$ (auch wenn U nilpotent ist). Analog ist $H = H_1 \oplus H_2$ mit $H_1 \in \mathrm{Syl}_p(H) \subseteq \mathrm{Syl}_p(G)$. Nach Induktion existiert ein $x \in G$ mit $xQx^{-1} \leq H$ und damit $xQx^{-1} \leq \mathrm{O}_{p'}(H) = H_2$. Es gilt dann $\langle H_1, xUx^{-1} \rangle \leq \mathrm{N}_G(xQx^{-1})$. Wegen $H_1 \in \mathrm{Syl}_p(\mathrm{N}_G(xQx^{-1}))$ existiert ein $y \in \mathrm{N}_G(xQx^{-1})$ mit $yxPx^{-1}y^{-1} \leq H_1$. Wegen $yxQx^{-1}y^{-1} = xQx^{-1} \leq H_2$ ist dann

$$yxUx^{-1}y^{-1} = (yxPx^{-1}y^{-1})(yxQx^{-1}y^{-1}) \leq H_1 H_2 = H.$$ □

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*

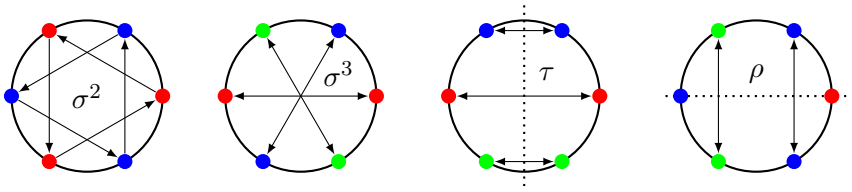
$$s = \frac{1}{|G|} \sum_{g \in G} f(g).$$

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

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

Beispiel 6.5. Wir zählen Halsketten mit sechs Perlen, 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 6). 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

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

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 $\varphi\colon \Omega \to \Omega'$ und ein $\alpha \in \mathrm{Aut}(G)$ mit ${}^{\alpha(g)}\varphi(\omega) = \varphi({}^g\omega)$ für $g \in G$ und $\omega \in \Omega$ gibt. Ggf. sind Ω und Ω' *isomorphe G-Mengen*. In den Anwendungen ist oft $\alpha = \mathrm{id}_G$.

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

Satz 6.9. *Sei $\omega_1, \dots, \omega_s$ ein Repräsentantensystem für die Bahnen einer Operation $f\colon G \to \mathrm{Sym}(\Omega)$. 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 1.22 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 $\Delta \subseteq \{1, \dots, n\}$ mit $1 < |\Delta| < n$. Für verschiedene Elemente $\alpha, \beta \in \Delta$ existiert dann ein 3-Zyklus $g \in A_n$ mit ${}^g\alpha = \alpha$ und ${}^g\beta \in \Omega \setminus \Delta$. Also ist Δ kein Block und S_n und A_n sind primitiv.

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

Satz 6.16. *Sei $G \to \mathrm{Sym}(\Omega)$ eine transitive Operation und $\omega \in \Omega$. Dann ist die Abbildung $H \to {}^H\omega$ eine Bijektion zwischen der Menge der Untergruppen $H \leq G$ mit $G_\omega < H < G$ und der Menge der Blöcke, die ω enthalten. mit $G_\omega < H < G$. Insbesondere ist G genau dann primitiv, wenn G_ω eine maximale Untergruppe ist.*

Beweis. Nach Satz 6.9 können wir $\Omega = G/G_\omega$ annehmen. Der Punkt ω entspricht dabei der trivialen Nebenklasse $1G_\omega$. Für $G_\omega < H < G$ ist H/G_ω ein Block, der $1G_\omega$ enthält, denn $1 < |H : G_\omega| < |\Omega|$ und $gH \cap H \in \{H, \varnothing\}$ für $g \in G$. Sei umgekehrt $\Delta \subseteq \Omega$ ein Block, der $1G_\omega$ enthält. Sei

$$H := \{g \in G : gG_\omega \in \Delta\} \supseteq G_\omega.$$

Für $x, y \in H$ gilt $xG_\omega = x(1G_\omega) \in \Delta \cap x\Delta$. Da Δ ein Block ist, folgt $xyG_\omega \in x\Delta = \Delta$ und $xy \in H$. Dies zeigt $H \leq G$. Offenbar ist auch $|G_\omega| < |\Delta||G_\omega| = |H| < |G|$. □

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. Wieder dürfen wir $\Omega = G/G_\omega$ mit $\omega \in \Omega$ nach Satz 6.9 annehmen. Nach Satz 6.16 ist $\Delta = H/G_\omega$ für eine maximale Untergruppe $H < G$. Wir wissen bereits, dass G transitiv auf $\mathcal{B}$ operiert (Bemerkung 6.14). Dabei ist H gerade der Stabilisator von $\Delta \in \mathcal{B}$. Nach Satz 6.16 ist die Operation auf $\mathcal{B}$ primitiv. □

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 4 und Satz 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.[16] Die Bestimmung der maximalen Untergruppe der Monstergruppe (und damit aller sporadischen Gruppen) wurde 2024 abgeschlossen.[17] Im Folgenden beschreiben wir die primitiven auflösbaren Gruppen.

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 ${}^g\varphi(x) = {}^{gx}\omega = {}^{(gxg^{-1})g}\omega = {}^{gxg^{-1}}\omega = \varphi({}^gx)$. □

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. □

[16] Siehe Tabelle 3 und OEIS
[17] siehe arXiv:2411.12230

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 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 4). Wegen $\mathrm{Ker}(\varphi) \cap V \leq H \cap V = 1$ ist dann $\mathrm{Ker}(\varphi) \leq \mathrm{C}_G(V) \leq V$ und $\mathrm{Ker}(\varphi) = 1$. Also ist G eine Permutationsgruppe auf G/H. Offenbar ist H der Stabilisator der trivialen Nebenklasse $1H$. Um zu zeigen, dass G primitiv ist, können wir nach Satz 6.16 beweisen, dass H maximal in G ist. Sei also $H < M \leq G$. Dann ist $1 \neq M \cap V \trianglelefteq M$, 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 oder Satz 9.8). 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.

(iii) Der nächste Satz zeigt, dass Sylows Satz optimal ist.

Satz 6.24 (McCarthy). *Sei $d \in \mathbb{N}$ keine Primzahlpotenz. Dann existiert eine endliche Gruppe G, deren Ordnung durch d teilbar ist und die keine Untergruppe der Ordnung d besitzt.*

Beweis. Nach Voraussetzung besitzt d einen Primteiler p mit $d = p^a n$, $p \nmid n$ und $p^a < \sqrt{d}$. Für die Ordnung e von $p + n\mathbb{Z} \in (\mathbb{Z}/n\mathbb{Z})^\times$ gilt $p^a < \sqrt{d} < n < p^e$. Sei

$$G := \mathrm{AGL}(1, p^e) \cong \mathbb{F}_{p^e} \rtimes \mathbb{F}_{p^e}^\times.$$

Dann ist d ein Teiler von $|G| = p^e(p^e - 1)$. Angenommen $H \leq G$ hat Ordnung d. Mit G besitzt auch H eine normale p-Sylowgruppe P. Wegen $H/P \leq \mathbb{F}_{p^e}^\times$ haben die Bahnen der Konjugationsoperation von H auf $P \setminus \{1\}$ die Länge n. Insbesondere ist $\sqrt{d} < n < |P| = p^a$. Widerspruch. □

Satz 6.25 (Galois). *Sei $\alpha \in \mathbb{Q}[X]$ irreduzibel mit Primzahlgrad p. Dann sind folgende Aussagen äquivalent:*

(1) α ist durch Radikale auflösbar.

(2) Die Galoisgruppe von α liegt in $\mathrm{AGL}(1, p) \cong C_p \rtimes C_{p-1}$.

(3) Für je zwei verschiedene Nullstellen $x, y \in \mathbb{C}$ von α ist $\mathbb{Q}(x, y)$ ein Zerfällungskörper von α.

Beweis. Nach dem Fundamentalsatz der Algebra besitzt α genau p paarweise verschiedene Nullstellen $x_1, \ldots, x_p \in \mathbb{C}$. Sei $G := \mathrm{Gal}(\mathbb{Q}(x_1, \ldots, x_p)|\mathbb{Q})$ die Galoisgruppe von α. Da α irreduzibel ist, operiert G treu und transitiv auf $\{x_1, \ldots, x_p\}$. Da p eine Primzahl ist, operiert G sogar primitiv.

(1)⇒(2): Mit α ist auch G auflösbar. Daher folgt (2) aus Satz 6.21.

(2)⇒(3): Sei $G \leq \mathrm{AGL}(1, p)$. Da G transitiv operiert, ist p ein Teiler von $|G|$. Also gilt $G = N \rtimes G_x$ mit $N \cong C_p$. Die Operation von G_x auf $\{x_1, \ldots, x_p\}$ ist isomorph zur Operation auf N. Dies zeigt $G_x \cap G_y = 1$. Nach dem Hauptsatz der Galoistheorie gilt $|\mathbb{Q}(x_1, \ldots, x_p) : \mathbb{Q}(x, y)| = |G_x \cap G_y| = 1$, d. h. $\mathbb{Q}(x_1, \ldots, x_p) = \mathbb{Q}(x, y)$.

(3)⇒(1): Wie oben gilt $G_x \cap G_y = 1$. Dies zeigt $|G| = |G : G_x||G_x : G_x \cap G_y| = pd$ mit $d \mid p - 1$. Nach Sylow besitzt G eine normale p-Sylowgruppe. Nach Satz 6.21 ist G auflösbar. Also ist auch α auflösbar. □

Folgerung 6.26. *Sei $\alpha \in \mathbb{Q}[X]$ irreduzibel und auflösbar mit Primzahlgrad $p > 2$. Dann besitzt α entweder eine oder genau p reelle Nullstellen.*

Beweis. Da p ungerade ist, besitzt α nach dem Zwischenwertsatz mindestens eine reelle Nullstelle $x \in \mathbb{R}$. Ist auch $y \in \mathbb{R}$ eine Nullstelle, so liegen nach Satz 6.25 alle Nullstellen in $\mathbb{Q}(x, y) \subseteq \mathbb{R}$. □

Definition 6.27. Seien G, H Gruppen und Ω eine G-Menge. 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 $\varphi\colon G \to \mathrm{Aut}(H^\Omega)$. Man nennt

$$H \wr G := H^\Omega \rtimes_\varphi G$$

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

Bemerkung 6.28. Im Fall $\Omega = \{1, \dots, n\}$ identifizieren wir H^Ω mit H^n. Für Elemente $(h_1, \dots, h_n, g)$, $(h'_1, \dots, h'_n, g') \in H \wr G$ gilt dann

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

Außerdem ist $|H \wr G| = |H|^n |G|$.

Satz 6.29. *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 $\Gamma = \{\Delta = \Delta_1, \dots, \Delta_n\}$. Wir wählen $g_i \in G$ mit ${}^{g_i}\Delta_i = \Delta$ für $i = 1, \dots, n$. Für $x \in G$ sei ${}^x\Delta_i = \Delta_{x(i)}$. Dann ist

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

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

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

Für $x, y \in G$ gilt nun

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

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. $g_i x g^{-1}_{x^{-1}(i)} = g_i x g_i^{-1}$ operiert trivial auf Δ. Also operiert x trivial auf ${}^{g_i^{-1}}\Delta = \Delta_i$ für $i = 1, \dots, n$. Insgesamt operiert x trivial auf Ω und es folgt $x = 1$. Daher ist F injektiv und die Behauptung folgt. □

Beispiel 6.30. Die Diedergruppe D_8 operiert imprimitiv auf den vier Ecken des Quadrats (zwei diagonal gegenüberliegende Ecken bilden einen Block). Satz 6.29 zeigt $D_8 \cong C_2 \wr C_2 \cong C_2^2 \rtimes C_2$. Nach Beispiel 5.11 ist auch $D_8 \cong C_4 \rtimes C_2$. Im Gegensatz zu direkten Produkten sind die Faktoren eines semidirekten Produkts im Allgemeinen also nicht eindeutig bestimmt.

Definition 6.31. 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 6.32.

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

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

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

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

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

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

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

Lemma 6.33. *Sei $\varphi\colon G \to \mathrm{Sym}(\Omega)$ eine transitive Operation, $\omega \in \Omega$ und $k \geq 2$. Genau dann ist φ k-transitiv, wenn G_ω $(k-1)$-transitiv auf $\Omega \setminus \{\omega\}$ operiert.*

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

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

Lemma 6.34. *Ist $G \to S_n$ k-transitiv, so ist $n(n-1)\ldots(n-k+1) \mid |G|$.*

Beweis. Induktion nach k: Im Fall $k = 1$ ist G transitiv und die Bahnengleichung liefert $n \mid |G|$. Sei nun $k \geq 2$. Dann ist G transitiv und nach Lemma 6.33 ist G_1 $(k-1)$-transitiv auf $\{2, \ldots, n\}$. Nach Induktion ist also $(n-1)\ldots(n-k+1) \mid |G_1|$. Wegen $|G : G_1| = n$ folgt die Behauptung. □

Satz 6.35. *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 6.36. *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 6.37. 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 6.38. *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 5.34). 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 $N \cap G_n \trianglelefteq G_n$ und damit $N_n = N \cap G_n = 1$. Also operiert N regulär auf Ω und $|N| = n$. Nach Beispiel 6.32 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 6.36 liefert nun $n = 6$ und $|N| = 4$. Dies widerspricht aber $|N| = n$. □

Satz 6.39. *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 $1 \neq N \trianglelefteq S_n$. Dann ist $N \cap A_n \trianglelefteq A_n$. Aus Satz 6.38 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 6.40. *Ist G eine einfache Gruppe der Ordnung 60, so ist $G \cong A_5$.*

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

Die Operation auf den Nebenklassen G/H liefert nun einen Monomorphismus $G \to S_5$. Da A_5 die einzige Untergruppe der Ordnung 60 in S_5 ist (Satz 6.39), folgt $G \cong A_5$. □

Bemerkung 6.41. Mit Hilfe der CFSG 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*[18]).

7 Verlagerung und normale Komplemente

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

Bemerkung 7.2.

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

(ii) Ist G p-nilpotent für ein $p \mid |G| \neq p$, so ist G nicht einfach.

Beispiel 7.3. Wegen $A_3 \trianglelefteq S_3$ ist S_3 2-nilpotent, aber nicht 3-nilpotent. Andererseits ist A_4 3-nilpotent, aber nicht 2-nilpotent.

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

Beweis. Ist G nilpotent und p eine Primzahl, so ist $\mathrm{O}_{p'}(G) = \bigoplus_{q \neq p} \mathrm{O}_q(G)$ nach Satz 4.10. Also ist $G/\mathrm{O}_{p'}(G)$ eine p-Gruppe und G ist p-nilpotent. Sei nun umgekehrt G p-nilpotent für jede Primzahl p. Dann ist

$$D := \bigtimes_{p \mid |G|} G/\mathrm{O}_{p'}(G)$$

nach Satz 4.10 nilpotent. Andererseits hat der Homomorphismus $G \to D$, $g \mapsto (g\mathrm{O}_{p'}(G))_{p \mid |G|}$ Kern $\bigcap_{p \mid |G|} \mathrm{O}_{p'}(G) = 1$. Wegen $|G| = |D|$ ist G zur nilpotenten Gruppe D isomorph. □

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

[18] Siehe Skript zur kombinatorischen Gruppentheorie

Beweis. Sei G p-nilpotent und $H \leq G$. Dann ist $\mathrm{O}_{p'}(G) \cap H \leq \mathrm{O}_{p'}(H)$ und

$$H/(H \cap \mathrm{O}_{p'}(G)) \cong H\mathrm{O}_{p'}(G)/\mathrm{O}_{p'}(G) \leq G/\mathrm{O}_{p'}(G)$$

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

$$(G/N)/(\mathrm{O}_{p'}(G)N/N) \cong G/\mathrm{O}_{p'}(G)N \cong (G/\mathrm{O}_{p'}(G))/(\mathrm{O}_{p'}(G)N/\mathrm{O}_{p'}(G))$$

ist eine p-Gruppe. Also ist auch G/N p-nilpotent. □

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

$$V_{H/K} \colon G \to H/K, \qquad g \mapsto \prod_{r \in R} (\overline{gr})^{-1} grK$$

heißt *Verlagerung* (engl. *transfer*) von G nach H/K. Da H/K abelsch ist, spielt die Reihenfolge der Faktoren im Produkt keine Rolle.

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

Beweis. Für Repräsentantensysteme R und S von G/H definieren wir

$$(R|S) := \prod_{\substack{(r,s) \in R \times S, \\ rH = sH}} s^{-1} rK \in H/K$$

ähnlich wie in Definition 5.17. Dann gilt $V_{H/K}(g) = (gR|R)$ für $g \in G$. Wie in Lemma 5.18 zeigt man

$$(gR|R) = (gR|gS)(gS|S)(S|R) = (R|S)(gS|S)(R|S)^{-1} = (gS|S).$$

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

$$V_{H/K}(gh) = (ghR|R) = (g(hR)|hR)(hR|R) = (gR|R)(hR|R) = V_{H/K}(g)V_{H/K}(h).$$ □

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

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

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

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

Definition 7.10. Für $H \leq G$ nennt man

$$\mathrm{Foc}_G(H) := \big\langle [g,h] : g \in G, h, [g,h] \in H \big\rangle$$

die *Fokalgruppe* von H in G.

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

Satz 7.12. *Sei $H \leq G$ und $F := \mathrm{Foc}_G(H)$ mit $\mathrm{ggT}(|G:H|, |H:F|) = 1$. Für $N := \mathrm{Ker}(V_{H/F}) \trianglelefteq G$ gilt dann*

(i) $H \cap N = H \cap G' = F$.

(ii) $HN = G$.

(iii) $G/G' = HG'/G' \oplus N/G'$.

(iv) $\boxed{G/N \cong H/F.}$

Beweis.

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

$$h = h^{a|G:H|+b|H:F|} \in F.$$

Somit gilt $H \cap N \leq F$.

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

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

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

Bemerkung 7.13. Die Voraussetzung $\mathrm{ggT}(|G:H|, |H:F|) = 1$ in Satz 7.12 ist zum Beispiel für π-Hallgruppen H erfüllt. Nach Aufgabe 32 ist ggf. HG'/G' eine π-Hallgruppe von G/G'. Nach Satz 7.12(iii) ist dann N der kleinste Normalteiler mit abelscher π-Faktorgruppe. Dies zeigt $N = \mathrm{O}^\pi(G)G'$.

Folgerung 7.14 (Higmans Fokalsatz)**.** *Für $P \in \mathrm{Syl}_p(G)$ gilt $\mathrm{Foc}_G(P) = G' \cap P \in \mathrm{Syl}_p(G')$.*

Beweis. Wähle $H = P$ in Satz 7.12. □

Satz 7.15 (Taunt)**.** *Sei $H \leq G$ mit $\mathrm{ggT}(|G:H|, |H:H'|) = 1$. Dann ist $G' \cap \mathrm{Z}(G) \cap H \leq H'$.*

Beweis. Wie üblich liegt G' im Kern von $V_{H/H'}$. Für $x \in G' \cap \mathrm{Z}(G) \cap H$ gilt daher $V_{H/H'}(x) = 1$. Wegen $x \in \mathrm{Z}(G)$ ist andererseits $V_{H/H'}(x) = x^{|G:H|}H'$ nach Beispiel 7.9, also $x^{|G:H|} \in H'$. Aus $x \in H$ folgt außerdem $x^{|H:H'|} \in H'$. Mit $\mathrm{ggT}(|G:H|, |H:H'|) = 1$ ergibt sich $x \in H'$. □

Satz 7.16 (Alperins Fusionssatz)**.** *Sei $P \in \mathrm{Syl}_p(G)$. Sei $\mathcal{P}$ die Menge aller Untergruppen $Q \leq P$ mit folgenden Eigenschaften:*

(i) $\mathrm{N}_P(Q) \in \mathrm{Syl}_p(\mathrm{N}_G(Q))$,

(ii) $\mathrm{O}_p(\mathrm{N}_G(Q)) = Q$,

(iii) $\mathrm{C}_P(Q) = \mathrm{Z}(Q)$.

Dann gilt

$$G' \cap P = \big\langle [\mathrm{N}_G(Q), Q] : Q \in \mathcal{P} \big\rangle.$$

Beweis. Offensichtlich ist $F := \langle [\mathrm{N}_G(Q), Q] : Q \in \mathcal{P} \rangle \leq G' \cap P$. Für die umgekehrte Inklusion zeigen wir allgemeiner: Ist $A \leq P$ und $g \in G$ mit ${}^gA \leq P$, so gilt

$$[g, A] := \langle [g, a] : a \in A \rangle \leq F.$$

Mit Higmans Fokalsatz folgt dann $G' \cap P = \mathrm{Foc}_G(P) \leq F$.

Wir argumentieren durch Induktion nach $|P : A|$. Im Fall $P = A$ ist $g \in \mathrm{N}_G(P)$ und die Behauptung gilt wegen $P \in \mathcal{P}$. Sei nun $A < P$. Nach Satz 3.14 ist $A < \mathrm{N}_P(A) \leq A_1 \in \mathrm{Syl}_p(\mathrm{N}_G(A))$. Nach Sylow existiert $x \in G$ mit ${}^xA_1 \leq P$. Für $Q := {}^xA$ gilt einerseits

$${}^xA_1 \leq {}^x\mathrm{N}_G(A) \cap P = \mathrm{N}_P(Q) \leq \mathrm{N}_G(Q)$$

und andererseits ${}^xA_1 \in \mathrm{Syl}_p(\mathrm{N}_G(Q))$. Dies zeigt ${}^x\mathrm{N}_P(A) \leq \mathrm{N}_P(Q) \in \mathrm{Syl}_p(\mathrm{N}_G(Q))$. Also gilt (i) für Q und nach Induktion ist $[x, A] \leq [x, \mathrm{N}_P(A)] \leq F$. Wegen ${}^{xg^{-1}}\mathrm{N}_P({}^gA) \leq \mathrm{N}_G(Q)$ existiert $y \in \mathrm{N}_G(Q)$ mit ${}^{yxg^{-1}}\mathrm{N}_P({}^gA) \leq \mathrm{N}_P(Q)$ nach Sylow. Man erhält $[yxg^{-1}, {}^gA] \leq [yxg^{-1}, \mathrm{N}_P({}^gA)] \leq F$ nach Induktion.

Sind (ii) und (iii) für Q erfüllt, so gilt $[y, Q] \leq [\mathrm{N}_G(Q), Q] \leq F$ nach Konstruktion. Sei nun

$$Q < \tilde{Q} := \mathrm{O}_p(\mathrm{N}_G(Q)) \leq \mathrm{N}_P(Q).$$

Dann ist $y \in \mathrm{N}_G(\tilde{Q})$ und induktiv folgt $[y, Q] \leq [y, \tilde{Q}] \leq F$. Sei schließlich $\tilde{Q} := Q\mathrm{C}_P(Q) > Q$. Wegen $\mathrm{C}_P(Q) = \mathrm{N}_P(Q) \cap \mathrm{C}_G(Q) \in \mathrm{Syl}_p(\mathrm{C}_G(Q))$ existiert $z \in \mathrm{C}_G(Q)$ mit ${}^{zy}\mathrm{C}_P(Q) = \mathrm{C}_P(Q)$. Nun gilt $zy \in \mathrm{N}_G(\tilde{Q})$ und $[y, Q] \leq [zy, \tilde{Q}] \leq F$ nach Induktion. In jedem Fall ist somit $[y, Q] \in F$. Für $a \in A$ folgt

$$[g, a] = (gag^{-1})a^{-1} \equiv y(xax^{-1})y^{-1}a^{-1} \equiv xax^{-1}a^{-1} \equiv 1 \pmod{F}. \qquad \square$$

Satz 7.17 (Puigs Hyperfokalsatz)**.** *Für $P \in \mathrm{Syl}_p(G)$ gilt*

$$\mathrm{O}^p(G) \cap P = \big\langle [\mathrm{O}^p(\mathrm{N}_G(Q)), Q] : Q \leq P \big\rangle = \big\langle [g, x] : g \in G \text{ } p'\text{-Element}, \ x, [g, x] \in P \big\rangle.$$

Beweis. Sei

$$S := \big\langle [\mathrm{O}^p(\mathrm{N}_G(Q)), Q] : Q \leq P \big\rangle \trianglelefteq P,$$
$$T := \big\langle [g, x] : g \in G \text{ } p'\text{-Element}, x, [g, x] \in P \big\rangle \trianglelefteq P.$$

Sei $x \in Q \leq P$ und $g \in \mathrm{O}^p(\mathrm{N}_G(Q))$. Nach Bemerkung 4.6 ist g ein Produkt von p'-Elementen $g_1, \ldots, g_n \in \mathrm{N}_G(Q)$. Für $n = 1$ ist $[g, x] \in T$. Sei nun $n \geq 2$ und $[g_2 \ldots g_n, x] \in T$ bereits gezeigt. Wegen $[g_2 \ldots g_n, x] \in Q \leq P$ ist $[g_1, g_2 \ldots g_n, x] \in T$. Es folgt

$$[g, x] = {}^{g_1}[g_2 \ldots g_n, x][g_1, x] \equiv [g_2 \ldots g_n, x][g_1, x] \equiv 1 \pmod{T}.$$

Dies zeigt $S \leq T$.

Jedes p'-Element $g \in G$ liegt in $\mathrm{O}^p(G)$. Für $x, [g, x] \in P$ ist daher $[g, x] = g(xg^{-1}x^{-1}) \in \mathrm{O}^p(G) \cap P$. Also gilt $T \leq \mathrm{O}^p(G) \cap P$ und es bleibt $\mathrm{O}^p(G) \cap P \leq S$ zu zeigen. Für $H := \mathrm{O}^p(G)$ ist $H \cap P \in \mathrm{Syl}_p(H)$. Für $Q \leq H \cap P$ ist $\mathrm{O}^p(\mathrm{N}_H(Q)) \leq \mathrm{O}^p(\mathrm{N}_G(Q))$ nach Bemerkung 4.6. Wir dürfen daher $G = H$ annehmen. Dann ist $P \leq G'$ und Alperin zeigt

$$P = G' \cap P = \langle [\mathrm{N}_G(Q), Q] : Q \in \mathcal{P} \rangle.$$

Für $Q \in \mathcal{P}$ gilt $\mathrm{N}_P(Q) \in \mathrm{Syl}_p(\mathrm{N}_G(Q))$ und $\mathrm{N}_G(Q) = \mathrm{N}_P(Q)\mathrm{O}^p(\mathrm{N}_G(Q))$. Für $x \in Q$, $y \in \mathrm{N}_P(Q)$ und $g \in \mathrm{O}^p(\mathrm{N}_G(Q))$ gilt

$$[yg, x] = {}^y[g, x][y, x] = [{}^y g, {}^g x][y, x] \in [\mathrm{O}^p(\mathrm{N}_G(Q)), Q]P' \leq SP'.$$

Insgesamt ist nun $P = SP' = S\Phi(P) = S$ nach Lemma 4.15. □

Satz 7.18 (Frobenius' Verlagerungssatz)**.** *Sei $P \in \mathrm{Syl}_p(G)$, sodass $\mathrm{N}_G(Q)/\mathrm{C}_G(Q)$ für alle $Q \leq P$ eine p-Gruppe ist. Dann ist G p-nilpotent.*

Beweis. Nach Voraussetzung ist $[\mathrm{O}^p(\mathrm{N}_G(Q)), Q] \leq [\mathrm{C}_G(Q), Q] = 1$ für alle $Q \leq P$. Aus Puigs Satz folgt $\mathrm{O}^p(G) \cap P = 1$. Daher ist $\mathrm{O}^p(G)$ ein normales Komplement von P. □

Bemerkung 7.19.

(i) Es genügt in Satz 7.18, die Untergruppen $Q \in \mathcal{P}$ aus Alperins Fusionssatz zu berücksichtigen. Es gilt dann nämlich $G' \cap P = P'$ und die Behauptung folgt aus Satz 7.38.

(ii) Für $p > 2$ haben Thompson und Glauberman bewiesen, dass G bereits dann p-nilpotent ist, falls $\mathrm{N}_G(K(P))/\mathrm{C}_G(K(P))$ eine p-Gruppe ist, wobei $K(P)$ eine gewisse charakteristische Untergruppe von P ist, deren Definition kompliziert ist. Die analoge Aussage für $p = 2$ gilt nicht, denn es gibt einfache Gruppen G (wie $\mathrm{PSL}(2, 17)$, siehe Satz 10.11), sodass $P \in \mathrm{Syl}_2(G)$ eine maximale Untergruppe ist. Für $Q \trianglelefteq P$ ist dann $\mathrm{N}_G(Q) = P$.

Satz 7.20 (Grüns erster Verlagerungssatz)**.** *Für $P \in \mathrm{Syl}_p(G)$ gilt*

$$G' \cap P = [\mathrm{N}_G(P), P]\langle P \cap Q' : Q \in \mathrm{Syl}_p(G)\rangle.$$

Beweis. Sicher ist

$$H := [\mathrm{N}_G(P), P]\langle P \cap Q' : Q \in \mathrm{Syl}_p(G)\rangle \leq P \cap G' \overset{7.14}{=} \mathrm{Foc}_G(P).$$

Nehmen wir $H < P \cap G'$ an. Wegen $P' \leq H$ ist $H \trianglelefteq P$. Sei $x \in P \cap G' \setminus H$ mit minimaler Ordnung.

Zur Berechnung der Verlagerung $V_{P/H}(x)$ nach Bemerkung 7.8 zerlegen wir G in Doppelnebenklassen der Form PyP. Offenbar ist PyP eine Vereinigung von Linksnebenklassen nach P und $\langle x\rangle$ operiert durch Linksmultiplikation auf der Menge dieser Nebenklassen. Sei $y = y_1, \ldots, y_n \in Py$ ein Repräsentantensystem der entsprechenden Bahnen mit Bahnenlängen $p^{a_1} \leq \ldots \leq p^{a_n}$ (notfalls y durch ein y_i ersetzen). Die Bahnengleichung ergibt

$$\sum_{i=1}^{n} p^{a_i} = \frac{|PyP|}{|P|} = \frac{|PyPy^{-1}|}{|P|} = |P : P \cap yPy^{-1}| =: p^t.$$

Es gilt $x^{p^{a_i}} y_i P = y_i P$ also $y_i^{-1} x^{p^{a_i}} y_i \in P$ und speziell $y^{-1} x^{p^{a_1}} y \in P$.

Fall 1: $t > 0$.
Die Bahn von $y_i P$ liefert in $V_{P/H}(x)$ den Beitrag $z_i H$ mit $z_i := y_i^{-1} x^{p^{a_i}} y_i \in P$ (Bemerkung 7.8). Es gilt

$$z_i^{-1} y^{-1} x^{p^{a_i}} y = y_i^{-1}[x^{-p^{a_i}}, y_i y^{-1}] y_i \in y_i^{-1} P' y_i.$$

Wegen $a_i \geq a_1$ ist $y^{-1} x^{p^{a_i}} y$ eine Potenz von $y^{-1} x^{p^{a_1}} y \in P$. Dies zeigt

$$z_i^{-1} y^{-1} x^{p^{a_i}} y \in P \cap y_i^{-1} P' y_i \in H.$$

Man kann den Beitrag z_iH in $V_{P/H}(x)$ also durch $y^{-1}x^{p^{a_i}}yH$ ersetzen. All diese Beiträge liefern zusammen $y^{-1}x^{p^t}yH$. Wegen $x \in G'$ gilt $y^{-1}x^{p^t}y \in P \cap G'$ und die Wahl von x zeigt $y^{-1}x^{p^t}y \in H$. Diese Doppelnebenklassen liefern also keinen Beitrag zu $V_{P/H}(x)$.

Fall 2: $t = 0$.
Hier ist $P = yPy^{-1}$, also $y \in \mathrm{N}_G(P)$. Der Beitrag von $yP = y_1P$ in $V_{P/H}(x)$ ist

$$y^{-1}xyH = x[x^{-1}, y^{-1}]H = xH$$

(beachte: $a_1 = 0$). Die Anzahl dieser Doppelnebenklassen $PyP = yP$ ist $k := |\mathrm{N}_G(P) : P| \not\equiv 0 \pmod p$. Insgesamt ergibt sich $V_{P/H}(x) = x^kH$. Bekanntlich gilt $x \in G' \subseteq \mathrm{Ker}(V_{P/H})$ und es folgt $x^k \in H$. Da k nicht durch p teilbar ist, erhält man den Widerspruch $x \in H$. □

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

Beweis. Wegen $P \leq \mathrm{N}_G(P) = \mathrm{C}_G(P)$ ist P abelsch. Grüns Verlagerungssatz (oder Alperins Fusionssatz) zeigt $G' \cap P = [\mathrm{N}_G(P), P] = 1$. Daher folgt die Behauptung aus Satz 7.12. □

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

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

Beispiel 7.23.

(i) Sei $|G| = 11^2 \cdot 12$. Wir zeigen, dass G auflösbar ist. Sei $P \in \mathrm{Syl}_{11}(G)$. Im Fall $P \trianglelefteq G$ sind P und G/P auflösbar und daher auch G. Sei also $P \not\trianglelefteq G$. Nach Sylow ist $|G : \mathrm{N}_G(P)| = 12$ also $\mathrm{N}_G(P) = P$. Wegen $|P| = 11^2$ ist P abelsch und es folgt $\mathrm{N}_G(P) = P \leq \mathrm{C}_G(P) \leq \mathrm{N}_G(P)$. Nach Satz 7.21 existiert ein $N \trianglelefteq G$ mit $|N| = 12$. Wieder sind N und G/N auflösbar und daher auch G.

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

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

Beweis. Wir zeigen zunächst durch Induktion nach $|G|$, dass G auflösbar ist. Sei p der kleinste Primteiler von $|G|$. Nach Satz 7.22 ist $G/\mathrm{O}_{p'}(G)$ eine p-Gruppe und damit auflösbar. Offenbar sind auch die Sylowgruppen von $\mathrm{O}_{p'}(G)$ zyklisch. Nach Induktion ist also auch $\mathrm{O}_{p'}(G)$ auflösbar. Die Behauptung folgt nun aus Lemma 2.22.

Nun ist G/G' abelsch und alle Sylowgruppen von G/G' sind zyklisch. Also ist auch G/G' zyklisch. Mit dem gleichen Argument genügt es zu zeigen, dass G' abelsch ist. Nehmen wir indirekt $G'' \neq 1$ an. Ersetzt man G durch G/G''', so kann man annehmen, dass G'' abelsch ist. Sicher ist dann G'' zyklisch. Also ist $G/\mathrm{C}_G(G'') \leq \mathrm{Aut}(G'') \cong (\mathbb{Z}/|G''|\mathbb{Z})^\times$ abelsch (Satz 2.4). Dies zeigt $G' \leq \mathrm{C}_G(G'')$ und $G'' \leq \mathrm{Z}(G')$. Da auch G'/G'' zyklisch ist, muss schließlich G' abelsch sein (Aufgabe 8(a)). Dies widerspricht aber $G'' \neq 1$. □

Bemerkung 7.25. Man kann in der Situation von Satz 7.24 weiter zeigen, dass G' eine Hallgruppe ist. Es gilt somit $G \cong C_m \rtimes C_n$ mit $\mathrm{ggT}(n,m) = 1$ nach Schur-Zassenhaus.

Beispiel 7.26. Gruppen quadratfreier Ordnung sind metabelsch.

Satz 7.27. *Für jede abelsche Hallgruppe $H \leq G$ und $N := \mathrm{N}_G(H)$ gilt:*

(i) $\boxed{H = \mathrm{C}_H(N) \oplus [H,N].}$

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

(iii) $\mathrm{C}_H(N) = V_{H/1}(H)$.

Beweis. Wir fassen $V_{H/1}$ als Abbildung nach H auf und schreiben $V_H := V_{H/1}$. Sei $g \in H$ und $V_H(g) = \prod_{i=1}^n x_i^{-1} g^{t_i} x_i \in H$ wie in Bemerkung 7.8. Für $i = 1, \ldots, n$ ist dann $g^{t_i}, x_i^{-1} g^{t_i} x_i \in H$ und $\langle H, x_i H x_i^{-1} \rangle \leq \mathrm{C}_G(g^{t_i})$, da H abelsch ist. Nach Satz 5.46 (Wielandt) sind die nilpotenten Hallgruppen H und $x_i H x_i^{-1}$ in $\mathrm{C}_G(g^{t_i})$ konjugiert. Sei also $c_i \in \mathrm{C}_G(g^{t_i})$ mit $c_i x_i H x_i^{-1} c_i^{-1} = H$ für $i = 1, \ldots, n$. Dann ist $c_i x_i \in N$ und

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

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

Offenbar ist

$$[H,N] = \langle [h,x] : h \in H, x \in N \rangle \leq \mathrm{Foc}_G(H) \leq H \cap G' \leq H \cap \mathrm{Ker}(V_H)$$

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

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

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

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

$$x^{-1} V_H(g) x = \prod_{r \in R} x^{-1} (\overline{gr})^{-1} grx = \prod_{r \in R} (\widetilde{grx})^{-1} grx = \prod_{s \in Rx} (\widetilde{gs})^{-1} gs \overset{7.7}{=} V_H(g).$$

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

Bemerkung 7.28. In der Situation von Satz 7.27 gilt $G/\mathrm{Ker}(V_{H/F}) \cong H/F \cong \mathrm{C}_H(N)$ mit $F := \mathrm{Foc}_G(H)$ nach Satz 7.12. Auf diese Weise kann man häufig Normalteiler konstruieren.

Beispiel 7.29. Sei $P \cong C_4 \times C_2$ eine 2-Sylowgruppe von G und $N := \mathrm{N}_G(P)$. Nach Satz 4.18 ist

$$\Phi(P) = \langle x^2 : x \in P \rangle \cong C_2.$$

Da $\Phi(P)$ charakteristisch in P ist, ist $\Phi(P) \trianglelefteq N$. Wegen $|\Phi(P)| = 2$ ist sogar $\Phi(P) \leq P \cap \mathrm{Z}(N) \neq 1$. Nach Bemerkung 7.28 existiert ein $K \trianglelefteq G$ mit $G/K \cong P \cap \mathrm{Z}(N)$. Insbesondere ist G nicht einfach. Sei $1 \neq \alpha \in \mathrm{Aut}(P)$ mit ungerader Ordnung. Nach Bemerkung 4.21 operiert α nicht-trivial auf $P/\Phi(P) \cong C_2^2$. Es gilt $\mathrm{Aut}(C_2^2) \cong \mathrm{GL}(2,2) \cong S_3$. Also muss α die drei maximalen Untergruppe von P transitiv permutieren. Andererseits muss α die charakteristische Untergruppe $\{x \in P : x^2 = 1\} \cong C_2^2$ festhalten. Dieser Widerspruch zeigt, dass $\mathrm{Aut}(P)$ eine 2-Gruppe ist. Daher ist auch $N/\mathrm{C}_G(P)$ eine 2-Gruppe. Wegen $P \leq \mathrm{C}_G(P)$ ist sogar $N = \mathrm{C}_G(P)$. Nach Burnsides Verlagerungssatz ist G 2-nilpotent.

Satz 7.30. *Jede auflösbare Untergruppe $H \leq G$ mit $H \cap gHg^{-1} = 1$ für alle $g \in G \setminus H$ besitzt ein normales Komplement in G (vgl. Aufgabe 33).*

Beweis (Shaw). Induktion nach $|H|$: Wir können $H \neq 1$ annehmen. Dann ist $H' < H$. Sei $h \in H$ und $V_{H/H'}(h) = \prod_{i=1}^n x_i^{-1} h^{t_i} x_i H'$ wie in Bemerkung 7.8. Dabei können wir $x_1 = 1$ annehmen. Wegen $hx_1H = H = x_1H$ ist dann $t_1 = 1$ und $x_1^{-1}h^{t_1}x_1 = h$. Für $i > 1$ ist $x_i \notin H$ und $x_i^{-1}h^{t_i}x_i \in H \cap x_i^{-1}Hx_i = 1$. Dies zeigt $V_{H/H'}(h) = hH'$ für alle $h \in H$. Insbesondere ist $V_{H/H'}(H) = H/H'$ und $\mathrm{Ker}(V_{H/H'}) \cap H = H'$. Sei $N := \mathrm{Ker}(V_{H/H'})$. Für $g \in G$ existiert ein $h \in H$ mit $V_{H/H'}(g) = V_{H/H'}(h)$ und $g = hh^{-1}g \in HN$. Also ist $G = HN$. Für $g \in N \setminus H' = N \setminus H$ ist $gH'g^{-1} \cap H' \subseteq gHg^{-1} \cap H = 1$. Nach Induktion besitzt H' ein normales Komplement K in N. Nach Aufgabe 33 sind H' und K Hallgruppen von N. Insbesondere ist K charakteristisch in N und damit normal in G. Es gilt $H \cap K = H \cap N \cap K = H' \cap K = 1$ und $G = HN = HH'K = HK$. Die Behauptung folgt. □

Bemerkung 7.31. Frobenius hat gezeigt, dass die Auflösbarkeitsbedingung in Satz 7.30 überflüssig ist. Man kennt dafür jedoch keinen Beweis, der ohne Charaktertheorie auskommt.

Satz 7.32. *Sei G eine nichtabelsche einfache Gruppe und $P \in \mathrm{Syl}_p(G)$ mit $|P| = p^n > 1$. Dann gilt eine der beiden folgenden Aussagen:*

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

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

Beweis. Nehmen wir zuerst an, dass P abelsch ist. Nach Satz 7.21 ist dann $P \leq \mathrm{C}_G(P) < \mathrm{N}_G(P)$. Sei $g \in \mathrm{N}_G(P) \setminus \mathrm{C}_G(P)$. Da P die einzige p-Sylowgruppe in $\mathrm{N}_G(P)$ ist, ist g kein p-Element. Indem man g durch eine geeignete Potenz ersetzt (Lemma 2.1), kann man annehmen, dass g Ordnung $q^s \neq 1$ für eine Primzahl $q \neq p$ hat. Nach Bemerkung 4.21 operiert $\langle g \rangle$ nicht-trivial auf $P/\Phi(P)$. Da $P/\Phi(P)$ elementarabelsch ist, ist $\mathrm{Aut}(P/\Phi(P)) \leq \mathrm{GL}(n,p)$ und $q \mid |\mathrm{GL}(n,p)| = (p^n - 1)(p^n - p) \dots (p^n - p^{n-1})$. Wegen $q \neq p$ ist dann auch

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

Sei nun P nichtabelsch. Insbesondere ist dann $n \geq 3$ und $\Phi(P) \neq 1$. Nach Satz 7.18 existiert eine Untergruppe $Q \leq P$, sodass $\mathrm{N}_G(Q)/\mathrm{C}_G(Q)$ keine p-Gruppe ist. Wir wählen wieder einen Primteiler $q \neq p$ von $|\mathrm{N}_G(Q)/\mathrm{C}_G(Q)|$. Wegen $|Q : \Phi(Q)| \leq p^{n-1}$ erhält man dann wie eben $q \mid (p^{n-1} - 1)(p^{n-2} - 1) \dots (p^2 - 1)(p - 1)$. Wegen $p^2 - 1 = (p+1)(p-1)$ kann man dabei den Faktor $p-1$ weglassen. Außerdem ist $q \mid |G : P|$, da $q \neq p$. Im Fall $q \mid |\mathrm{N}_G(P) : P|$ gilt Aussage (i). Also können wir $q \mid |G : \mathrm{N}_G(P)|$ annehmen. Somit gilt (ii). □

Beispiel 7.33. Nach Satz 4.23 und Beispiel 7.26 ist die Ordnung einer nichtabelschen einfachen Gruppe das Produkt von mindestens vier Primzahlen. Sei G eine einfache Gruppe der Ordnung $pqrs$ mit Primzahlen $p \leq q \leq r \leq s$. Nach Satz 7.22 ist $p = q$ und nach Satz 4.23 ist $q < r$. Außerdem ist

$$1 \neq \mathrm{ggT}(rs, (p^2-1)(p-1)) = \mathrm{ggT}(rs, p+1)$$

nach Satz 7.32. Dies zeigt $p = q = 2$ und $r = 3$. Nehmen wir $s = 3$ an. Nach Sylow gilt dann $\mathrm{N}_G(S) = S$ für $S \in \mathrm{Syl}_3(G)$. Dies widerspricht aber Satz 7.21. Also ist $s \geq 5$. Sei $S \in \mathrm{Syl}_s(G)$. Dann ist $|G : \mathrm{N}_G(S)|$ ein Teiler von 12 und $|G : \mathrm{N}_G(S)| \equiv 1 \pmod{s}$ nach Sylow. Es folgt

$$6 \leq 1 + s \leq |G : \mathrm{N}_G(S)| \in \{6, 12\}.$$

Der Fall $|G : \mathrm{N}_G(S)| = 12$ widerspricht wie eben Satz 7.21. Also ist $s = 5$ und $G \cong A_5$ nach Satz 6.40.

Lemma 7.34 (Brandis)**.** *Sei $G = HN$ mit $H \leq G$ und $N \trianglelefteq G$. Sei $K := H \cap N$ und $K' \leq K_0 \leq K$ mit $K_0 \trianglelefteq H$ und $\mathrm{ggT}(|K/K_0|, |G : H|) = 1$. Angenommen die Verlagerung $V\colon N \to K/K_0$ ist trivial. Dann gilt $H = KL$ mit $L \leq H$ und $K \cap L = K_0$.*

Beweis. Sei R ein Repräsentantensystem für N/K. Für $x \in N$ sei $\overline{x} \in R$ mit $xK = \overline{x}K$. Wir definieren

$$\alpha\colon H \to K/K_0, \quad x \mapsto \prod_{r \in R} r^{-x}\overline{r^x}K_0$$

(da K/K_0 abelsch ist, spielt die Reihenfolge der Faktoren keine Rolle). Wegen $K_0 \trianglelefteq H$ ist $R = \{\overline{r^x} : r \in R\}$. Für $x, y \in H$ gilt

$$\alpha(x)^y\alpha(y) = \prod_{r \in R} r^{-xy}(\overline{r^x})^y K_0 \prod_{r \in R} \overline{r^x}^{-y}\overline{r^{xy}}K_0 = \prod_{r \in R} r^{-xy}\overline{r^{xy}}K_0 = \alpha(xy),$$

d. h. α ist ein verschränkter Homomorphismus (Definition 5.20). Nach Lemma 5.21 ist $L := \mathrm{Ker}(\alpha) \leq H$. Für $x \in K$ gilt $r^x K = x^{-1}rK$ und

$$\alpha(x) = \prod_{r \in R} x^{-1}r^{-1}x\overline{r^x}K_0 = x^{-|N:K|} \prod_{r \in R} r^{-1}x\overline{x^{-1}r}K_0 \overset{7.6}{=} x^{-|N:K|}V(x^{-1})^{-1} = x^{-|N:K|}K_0.$$

Wegen $|N : K| = |N : N \cap H| = |HN : H| = |G : H|$ und $\mathrm{ggT}(|K/K_0|, |G : H|) = 1$ ist $\alpha_{|K}$ surjektiv und $L \cap K = K_0$. Für $h \in H$ existiert $x \in K$ mit $\alpha(h) = \alpha(x)^{-1}$. Da K/K_0 abelsch ist, gilt $\alpha(hx) = \alpha(h)\alpha(x) = 1$, d. h. $hx \in \mathrm{Ker}(\alpha) = L$. Dies zeigt $h = (hx)x^{-1} \in LK$ und $H = KL$. □

Satz 7.35. *Sei $P \in \mathrm{Syl}_p(G)$ und $Q = P \cap \mathrm{O}^p(G)$. Dann existiert $R \leq P$ mit $P = QR$ und $Q \cap R = Q'$.*

Beweis. Sei $H := P$, $N := \mathrm{O}^p(G)$, $K := Q$ und $K_0 := Q'$ in Lemma 7.34. Sicher gilt $G = HN$ und $\mathrm{ggT}(|K/K_0|, |G : H|) = 1$. Da Q' charakteristisch in $Q \trianglelefteq H$ ist, gilt auch $K_0 \trianglelefteq H$. Wegen $\mathrm{O}^p(N) \trianglelefteq G$ ist $\mathrm{O}^p(N) = N$. Insbesondere muss die Verlagerung $N \to K/K_0$ trivial sein. Nun folgt die Behauptung aus Lemma 7.34. □

Folgerung 7.36 (Gaschütz)**.** *Sind die p-Sylowgruppen von $\mathrm{O}^p(G)$ abelsch, so besitzt $\mathrm{O}^p(G)$ ein Komplement in G.*

Beweis. In der Situation von Satz 7.35 ist $\mathrm{O}^p(G) \cap R = Q \cap R = Q' = 1$ und $G = P\mathrm{O}^p(G) = RQ\mathrm{O}^p(G) = R\mathrm{O}^p(G)$. □

Bemerkung 7.37. Der nächste Satz ist eine Lokalisierung von Wielandts Satz 4.17.

Satz 7.38. *Für $P \in \mathrm{Syl}_p(G)$ sind die folgenden Aussagen äquivalent:*

(1) G ist p-nilpotent.

(2) $G' \cap P \leq \Phi(P)$.

(3) $\mathrm{O}^p(G) \cap P \leq \Phi(P)$.

Gegebenenfalls ist $G' \cap P = P'$.

Beweis. Ist G p-nilpotent, so ist

$$G' \cap P \leq P'\mathrm{O}_{p'}(G) \cap P = P'(\mathrm{O}_{p'}(G) \cap P) = P' \leq G' \cap P$$

nach Dedekind. Insbesondere ist dann $G' \cap P \leq \Phi(P)$. Sei nun $N = \mathrm{O}^p(G)G'$. Nach Satz 7.12 und Bemerkung 7.13 gilt $G' \cap P = N \cap P$. Aus $G' \cap P \leq \Phi(P)$ folgt daher $Q := \mathrm{O}^p(G) \cap P \leq N \cap P \leq \Phi(P)$.

Sei schließlich $Q \leq \Phi(P)$. Nach Satz 7.35 existiert $R \leq P$ mit $P = QR = \Phi(P)R$ und $Q \cap R = Q'$. Mit Lemma 4.15 ergibt sich $P = R$ und $Q = Q \cap P = Q'$, also $Q = 1$. Somit ist G p-nilpotent. □

Folgerung 7.39. *Sei $P \in \mathrm{Syl}_p(G)$, sodass je zwei in G konjugierte Elemente $x, y \in P$ bereits in P konjugiert sind. Dann ist G p-nilpotent.*

Beweis. Sei $g \in G$ und $x, [g,x] \in P$. Dann ist auch $gxg^{-1} = [g,x]x \in P$. Nach Voraussetzung existiert $z \in P$ mit $gxg^{-1} = zxz^{-1}$. Es folgt $[g,x] = [z,x] \in P'$ und $G' \cap P = \mathrm{Foc}_G(P) = P'$. Die Behauptung ergibt sich aus Satz 7.38. □

Definition 7.40. Für eine Primzahl p sei

$$\mathrm{A}^p(G)/\mathrm{O}^p(G) := (G/\mathrm{O}^p(G))', \qquad \mathrm{E}^p(G)/\mathrm{O}^p(G) := \Phi(G/\mathrm{O}^p(G)).$$

Bemerkung 7.41. Nach Satz 4.18 ist $\mathrm{A}^p(G)$ (bzw. $\mathrm{E}^p(G)$) der kleinste Normalteiler von G mit (elementar)abelscher p-Faktorgruppe. Für $P \in \mathrm{Syl}_p(G)$ gilt $G = P\mathrm{O}^p(G)$ und daher $\mathrm{A}^p(G) = P'\mathrm{O}^p(G)$ sowie $\mathrm{E}^p(G) = P'\langle x^p : x \in P\rangle\mathrm{O}^p(G) = \Phi(P)\mathrm{O}^p(G)$.

Satz 7.42 (Tates Verlagerungssatz)**.** *Sei $H \leq G$ mit $p \nmid |G : H|$. Dann sind folgende Aussagen äquivalent:*

(1) $G/\mathrm{O}^p(G) \cong H/\mathrm{O}^p(H)$.

(2) $G/\mathrm{A}^p(G) \cong H/\mathrm{A}^p(H)$.

(3) $G/\mathrm{E}^p(G) \cong H/\mathrm{E}^p(H)$.

Beweis. Die Implikationen (1)⇒(2)⇒(3) sind trivial. Sei nun $G/\mathrm{E}^p(G) \cong H/\mathrm{E}^p(H)$ und $P \in \mathrm{Syl}_p(H)$. Wegen $p \nmid |G:H|$ ist $P \in \mathrm{Syl}_p(G)$ und $G = H\mathrm{O}^p(G)$. Aus $H/H \cap \mathrm{O}^p(G) \cong H\mathrm{O}^p(G)/\mathrm{O}^p(G) = G/\mathrm{O}^p(G)$ folgt $\mathrm{O}^p(H) \leq \mathrm{O}^p(G)$ und analog $\mathrm{E}^p(H) = \mathrm{E}^p(G) \cap H$. Sei $\overline{H} := H/\mathrm{O}^p(H)$. Wir benutzen Lemma 7.34 mit $N := \mathrm{O}^p(G)$, $K := H \cap N$ und $K_0/\mathrm{O}^p(H) := \Phi(\overline{K})$. Dann ist $K/K_0 \cong \overline{K}/\Phi(\overline{K})$ eine abelsche p-Gruppe und die Verlagerung $N \to K/K_0$ trivial. Man erhält also $H = KL$ mit $L \leq K$ und $K \cap L = K_0$. Nach Dedekind ist

$$\overline{H} = \overline{L\Phi(P)K} = \overline{L(\Phi(P)\mathrm{O}^p(G) \cap H)} = \overline{L(\mathrm{E}^p(G) \cap H)} = \overline{L\mathrm{E}^p(H)} = \overline{L}\Phi(\overline{H}) \overset{4.15}{=} \overline{L}.$$

Es folgt $\overline{K} = \overline{K \cap L} = \overline{K_0} = \Phi(\overline{K}) = 1$. Dies zeigt

$$G/\mathrm{O}^p(G) = H\mathrm{O}^p(G)/\mathrm{O}^p(G) \cong H/(H \cap \mathrm{O}^p(G)) = H/K = H/\mathrm{O}^p(H). \qquad \square$$

Bemerkung 7.43.

(i) Satz 7.42 wurde von Tate 1964 mit kohomologischen Methoden bewiesen, während Thompson 1970 einen charaktertheoretischen Beweis vorlegte. Brandis' gruppentheoretischer Zugang von 1978 ist weitgehend unbekannt. So schreibt etwa Isaacs 2008 in seinem Buch, dass es keinen „einfachen" Beweis zu geben scheint. Gagola und Isaacs gaben später einen gruppentheoretischen Beweis, der jedoch deutlich aufwendiger als der obige Beweis ist.

(ii) Der Beweis von Satz 7.42 zeigt, dass die in (1)–(3) gelisteten Faktorgruppen bereits dann isomorph sind, wenn ihre Ordnungen übereinstimmen. Nach Burnsides Basissatz bedeutet (3) dann, dass $G/\mathrm{O}^p(G)$ und $H/\mathrm{O}^p(H)$ minimale Erzeugendensysteme der gleichen Mächtigkeit besitzen.

(iii) Gelten die äquivalenten Aussagen in Satz 7.42, so sagt man: H *kontrolliert* die Verlagerung in G. Ggf. ist G genau dann p-nilpotent, wenn H p-nilpotent ist. Besonders interessant ist die Wahl $H := \mathrm{N}_G(P)$, wobei $P \in \mathrm{Syl}_p(G)$. Ist P abelsch, so gilt $G' \cap P = [H,P] \leq H' \cap P \leq G' \cap P$ nach Grün. Wegen $G/\mathrm{A}^p(G) \cong P/(G' \cap P) \cong H/\mathrm{A}^p(H)$ (Satz 7.12) kontrolliert H in diesem Fall die Verlagerung. Dies wird im nächsten Satz verallgemeinert.

Satz 7.44 (Grüns zweiter Verlagerungssatz)**.** *Sei $P \in \mathrm{Syl}_p(G)$. Für alle $g \in G$ mit ${}^g\mathrm{Z}(P) \leq P$ sei ${}^g\mathrm{Z}(P) = \mathrm{Z}(P)$. Dann kontrolliert $\mathrm{N}_G(\mathrm{Z}(P))$ die Verlagerung in G.*

Beweis. Sei $Z := \mathrm{Z}(P)$ und $H := \mathrm{N}_G(Z)$. Da Z charakteristisch in P ist, gilt $P \leq \mathrm{N}_G(P) \leq H$. Es genügt $G' \cap P \leq H' \cap P$ zu zeigen. Nach Grüns ersten Satz brauchen wir nur $R := P \cap Q' \leq H'$ für alle $Q \in \mathrm{Syl}_p(G)$ zu beweisen. Sei $g \in G$ mit ${}^gP = Q$. Dann ist $Z \leq \mathrm{C}_G(P) \leq \mathrm{N}_G(R)$ und ${}^gZ \leq \mathrm{C}_G(Q) \leq \mathrm{N}_G(R)$. Wir wählen $P_1 \in \mathrm{Syl}_p(\mathrm{N}_G(R))$ und $x \in \mathrm{N}_G(R)$ mit $Z \leq P_1$ und ${}^{xg}Z \leq P_1$. Nach Sylow existiert $y \in G$ mit ${}^yP_1 \leq P$. Es folgt ${}^yZ \leq P$. Die Voraussetzung impliziert nun $y \in H$. Analog ist $yxg \in H$ und daher $xg \in H$. Dies zeigt $R = {}^xR \leq P \cap {}^{xg}P' \leq H'$. $\square$

Bemerkung 7.45.

(i) Yoshidas Verlagerungssatz besagt, dass $\mathrm{N}_G(P)$ die Verlagerung kontrolliert, falls P keine zu $C_p \wr C_p$ isomorphe Faktorgruppe besitzt (wobei C_p regulär auf sich selbst operiert). Insbesondere gilt dies, falls $|P| < |C_p \wr C_p| = p^{p+1}$ oder falls die Nilpotenzklasse von P kleiner als p ist (Aufgabe 44).

(ii) Der nächste Satz hat Ähnlichkeit mit Lemma 5.14.

Satz 7.46 (Roquette)**.** *Sei $G = HN$ mit $H \leq G$ und $N \trianglelefteq G$. Sei $H \cap N \leq \Phi(H)$ und $\mathrm{ggT}(|H \cap N|, |G:H|) = 1$. Dann besitzt H ein normales Komplement in G.*

Beweis. Wir können annehmen, dass N als Normalteiler bzgl. der Eigenschaft $G = HN$ minimal ist. Sei $K := H \cap N$ und π die Menge der Primteiler von $|K|$. Dann ist $M := \mathrm{O}^\pi(N)$ charakteristisch in N und normal in G. Nun ist $\mathrm{ggT}(|K|, |N : K|) = \mathrm{ggT}(|K|, |G : H|) = 1$ und $N = KM$ nach Lemma 1.9(vi). Es folgt $HM = HKM = HN = G$ und die Minimalität von N zeigt $N = M$. Also besitzt N keine echten π-Faktorgruppen. Insbesondere ist die Verlagerung $N \to K/K'$ trivial. Lemma 7.34 mit $K_0 = K'$ liefert $L \leq H$ mit $H = KL$ und $K \cap L = K_0$. Nach Voraussetzung ist $H = KL = \Phi(H)L = L$ und daher $K = K_0 = K'$. Nach Frattini ist $\Phi(H)$ und somit auch K nilpotent. Man erhält $K = 1$, d. h. N ist ein normales Komplement von H. □

Satz 7.47 (Shemetkov)**.** *Sei $N \trianglelefteq G$. Sei π eine Menge von Primzahlen p mit folgender Eigenschaft: Es existiert $P \in \mathrm{Syl}_p(G)$, sodass $P \cap N$ abelsch ist und ein Komplement in P besitzt. Dann existiert $H \leq G$ mit $G = HN$, sodass $H \cap N$ eine π'-Gruppe ist.*

Beweis. Wir argumentieren durch Induktion nach $|G| + |N| + |\pi|$.

Fall 1: $N' < N$.
Sei p eine Primzahl mit $M := \mathrm{O}^p(N) < N$. Im Fall $M = 1$ folgt die Behauptung mit $G = H$ falls $p \notin \pi$ oder mit Satz 5.23 falls $p \in \pi$. Sei also $M \neq 1$ und $\overline{G} := G/M$. Sei $q \in \pi$. Nach Voraussetzung existiert eine q-Sylowgruppe $G_q = N_q \rtimes R$ von G, wobei $N_q \in \mathrm{Syl}_q(N)$ abelsch ist. Offenbar sind $\overline{N_q} \leq \overline{G_q}$ Sylowgruppen von $\overline{N}$ bzw. $\overline{G}$ und $\overline{N_q}$ ist abelsch. Wegen $R \cap N \leq R \cap G_q \cap N = R \cap N_q = 1$ ist $N_qM \cap RM = (N_qM \cap R)M = M$ und $\overline{G_q} = \overline{N_q} \rtimes \overline{R}$. Nach Induktion existiert $K/M \leq \overline{G}$ mit $G = KN$, sodass $(K \cap N)/M$ eine π'-Gruppe ist.

Für $q \neq p$ ist jede q-Sylowgruppe von M auch eine q-Sylowgruppe von N und besitzt daher ein Komplement in K. Sei nun $q = p$ und $K_p \in \mathrm{Syl}_p(K)$. Nach Folgerung 7.36 besitzt $M = \mathrm{O}^p(K_pM)$ ein Komplement R in K_pM. Es gilt

$$|R| = |K_pM : M| = |K_p : K_p \cap M| = |K : M|_p.$$

Nach Sylow muss R eine p-Sylowgruppe von M_p von M normalisieren, denn deren Anzahl ist 1 modulo p. Nun ist R ein Komplement von M_p in der Sylowgruppe $M_p \rtimes R$ von K. Wegen $M < N$ gilt die Behauptung für $M \leq K$ nach Induktion, d. h. es existiert $H \leq K$ mit $K = HM$, sodass $H \cap M$ eine π'-Gruppe ist. Dann ist $G = KN = HMN = HN$ und wegen

$$(H \cap N)/(H \cap M) \cong (H \cap N)M/M = (K \cap N)/M$$

ist auch $H \cap N$ eine π'-Gruppe.

Fall 2: $N = N'$.
Im Fall $\pi = \varnothing$ gilt die Behauptung mit $H = G$. Sei also $p \in \pi$ und $\tau := \pi \setminus \{p\}$. Nach Induktion existiert $K \leq G$ mit $G = KN$, sodass $K \cap N$ eine τ'-Gruppe ist. Wir können annehmen, dass $K \cap N$ keine π'-Gruppe ist, d. h. p teilt $|K \cap N|$. Sei $P \in \mathrm{Syl}_p(K \cap N)$. Nach Lemma 5.14 dürfen wir $K \cap N \leq \Phi(K)$ voraussetzen. Insbesondere ist $K \cap N \trianglelefteq K$ nilpotent und $P = \mathrm{O}_p(K \cap N) \trianglelefteq K \leq \mathrm{N}_G(P)$. Wir betrachten

$$L := K\mathrm{C}_N(P) \leq \mathrm{N}_G(P).$$

Nach Voraussetzung existiert eine abelsche p-Sylowgruppe N_p von N, die P enthält. Sicher ist $N_p \in \mathrm{Syl}_p(\mathrm{C}_N(P))$ und N_p besitzt ein Komplement in L. Sei nun $q \in \tau$. Eine q-Sylowgruppe K_q von K normalisiert ein $\mathrm{C}_N(P)_q \in \mathrm{Syl}_q(\mathrm{C}_N(P))$. Da $K \cap N$ eine τ'-Gruppe ist, gilt $K_q \cap \mathrm{C}_N(P)_q = 1$ und $\mathrm{C}_N(P)_q \rtimes K_q \in \mathrm{Syl}_q(L)$. Nach Taunt gilt $N_p \cap \mathrm{Z}(N) = N_p \cap \mathrm{Z}(N) \cap N' = 1$. Insbesondere ist $\mathrm{C}_N(P) < N$ und wir können Induktion auf $\mathrm{C}_N(P) \trianglelefteq L$ anwenden. Dies liefert $H \leq L$ mit $L = H\mathrm{C}_N(P)$, sodass

$H \cap \mathrm{C}_N(P)$ eine π'-Gruppe ist. Dann ist $G = KN = K\mathrm{N}_N(P)N = LN = HN$. Wegen $|N : \mathrm{C}_N(P)| \not\equiv 0 \pmod{p}$ ist

$$(H \cap N)/(H \cap \mathrm{C}_N(P)) \cong (H \cap N)\mathrm{C}_N(P)/\mathrm{C}_N(P)$$

eine p'-Gruppe. Andererseits ist

$$(H \cap N)\mathrm{C}_N(P)/\mathrm{C}_N(P) \cong (K \cap N)\mathrm{C}_N(P)/\mathrm{C}_N(P) \cong (K \cap N)/(K \cap \mathrm{C}_N(P))$$

eine τ'-Gruppe. Insgesamt ist $H \cap N$ eine π'-Gruppe. □

Folgerung 7.48. *Sei $N \trianglelefteq G$. Für jeden Primteiler p von $|G : N|$ besitze N eine abelsche p-Sylowgruppe mit einem Komplement in einer Sylowgruppe von G. Dann besitzt N ein Komplement in G.*

Beweis. Sei π die Menge aller Primteiler von $|G : N|$. Satz 7.47 liefert $H \leq G$ mit $G = HN$, sodass $H \cap N$ eine π'-Gruppe ist. Mit Lemma 5.14 können wir andererseits erreichen, dass $H \cap N$ eine π-Gruppe ist (siehe Beweis von Folgerung 5.31). Also ist $H \cap N = 1$. □

8 Erzeuger und Relationen

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

Definition 8.1. Ein *Alphabet* sei eine beliebige Menge A, deren Elemente wie *Buchstaben* nennen. Ein *Wort* w ist eine Folge der Form $w = a_1^{\epsilon_1} \dots a_n^{\epsilon_n}$ mit $a_1, \dots, a_n \in A$ und $\epsilon_1, \dots, \epsilon_n \in \{\pm 1\}$. Dabei ist auch das *leere Wort* mit $n = 0$ zugelassen. Gilt $a_i \neq a_{i+1}$ oder $\epsilon_i = \epsilon_{i+1}$ für $i = 1, \dots, n-1$, so heißt w *reduziert*. Offenbar kann man jedes Wort w in ein reduziertes Wort $\overline{w}$ überführen, indem man Teile der Form aa^{-1} oder $a^{-1}a$ sukzessiv streicht (nach Aufgabe 57 ist $\overline{w}$ eindeutig bestimmt). Auf der Menge W aller Wörter definiert $w \sim v :\Longleftrightarrow \overline{w} = \overline{v}$ eine Äquivalenzrelation. Die Menge der Äquivalenzklassen $F_A := \{[w] : w \in W\}$ bildet dann eine Gruppe bzgl. Konkatenation, d. h.

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

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

Bemerkung 8.2.

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

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

(iii) Sei $w = a_1^{\epsilon_1} \dots a_n^{\epsilon_n} \in F_A \setminus \{1\}$ mit endlicher Ordnung. Nach eventueller Konjugation mit $a_1^{-\epsilon_1}$ können wir $a_1^{\epsilon_1} \neq a_n^{-\epsilon_n}$ annehmen. Dann wären aber sämtliche Potenzen w^n mit $n \in \mathbb{N}$ reduziert. Dieser Widerspruch zeigt, dass F_A torsionsfrei ist.

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

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

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

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

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

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

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

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

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

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

Bemerkung 8.8.

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

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

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

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

Beispiel 8.9.

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

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

(iii) Sei $G := \langle x, y, z \mid xyx^{-1} = y^2, yzy^{-1} = z^2, zxz^{-1} = x^2 \rangle$. Für $a, b \in \mathbb{N}$ gilt

$$x^a y^b = x^{a-1} x y^b x^{-1} x = x^{a-1} y^{2b} x = x^{a-2} y^{4b} x^2 = \ldots = y^{2^a b} x^a.$$

Durch zyklische Vertauschung von x, y, z erhält man analoge Gleichungen. Es folgt

$$z^2 y^2 x = z^2 xy = x^4 z^2 y = x^4 yz = y^{16} x^4 z = y^{16} z x^2$$

und $x = z^{-1} y^{-16} z^2 y^2 \in \langle y, z \rangle$. Also ist $G = \langle y, z \rangle$. Wegen $N := \langle z \rangle \trianglelefteq G$ und $G/N = \langle yN \rangle$ ist G auflösbar. Andererseits ist $y = xyx^{-1}y^{-1} \in G'$ und analog $x, z \in G'$. Dies zeigt $G = 1$ (anderenfalls wäre $G = G' < G$).

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

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

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

der gesuchte Epimorphismus. □

Beispiel 8.11.

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

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

Bemerkung 8.12 (Coxeter-Todd-Algorithmus)**.** Um die Größe einer Gruppe $G = \langle X \mid R \rangle$ nach oben abzuschätzen, sucht man zunächst eine „bekannte“ Untergruppe $H \leq G$ (zum Beispiel $H = \langle x \rangle$ für ein $x \in X$). Danach wählt man eine Liste L von Linksnebenklassen nach H, sodass G die Elemente von L durch Linksmultiplikation permutiert. Da im Allgemeinen G transitiv auf G/H operiert, muss L bereits alle Nebenklassen nach H enthalten. Dies zeigt $|G| \leq |L||H|$ (Nebenklassen dürfen mehrfach in L auftauchen).

Satz 8.13 (Carmichael)**.** *Für $n \geq 2$ gilt*

$$A_n \cong \langle x_1, \ldots, x_{n-2} \mid x_1^3 = \cdots = x_{n-2}^3 = 1, \ (x_i x_j)^2 = 1 \ (i \neq j) \rangle.$$

Beweis. Sei G die Gruppe auf der rechten Seite. Für $n = 2$ ist $A_2 = 1 = \langle \varnothing \rangle = G$. Sei daher $n \geq 3$ und $m := n - 2$. Sei $H := \langle x_1, \ldots, x_{m-1} \rangle \leq G$. Nach von Dyck ist H eine Faktorgruppe von A_{n-1}. Insbesondere ist $|H| \leq \frac{1}{2}(n-1)!$. Für $i \neq j$ gilt $x_i x_j = (x_i x_j)^{-1} = x_j^{-1} x_i^{-1} = x_j^2 x_i^2$ in G. Wir betrachten die n Nebenklassen

$$L := \{H,\ x_m H,\ x_m^2 H,\ x_{m-1}^2 x_m H,\ x_{m-2}^2 x_m H, \ldots, x_1^2 x_m H\}.$$

Für $i, j < m$ mit $i \neq j$ gilt

$$\begin{aligned} x_i H &= H, \\ x_i x_m H &= x_m^2 x_i^2 H = x_m^2 H, \\ x_i x_m^2 H &= x_i x_m^2 x_i^2 H = x_i^2 x_m H, \\ x_m x_i^2 x_m H &= x_m x_i x_m^2 H = x_i^2 x_m^4 H = x_i^2 x_m H, \\ x_i x_j^2 x_m H &= x_i x_j x_m^2 H = x_j^2 x_i^2 x_m^2 H = x_j^2 x_m H. \end{aligned}$$

Dies zeigt, dass G durch Linksmultiplikation auf L operiert. Man erhält $|G| \leq n|H| \leq n!/2$.

Umgekehrt erfüllen die Elemente $x_i := (1, 2, i+2)$ für $i = 1, \ldots, n-2$ in A_n die angegebenen Relationen, denn $x_i x_j = (1, i+2)(2, j+2)$ für $i \neq j$. Nach Satz 8.10 existiert ein Isomorphismus $G \to A_n$. □

Satz 8.14 (Gauss)**.** *Für jede Primzahl p und $n \geq 1$ gilt*

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

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

Sei zunächst $p > 2$. Wir müssen zeigen, dass G zyklisch ist. Im Fall $n = 1$ ist $G = \mathbb{F}_p^\times$ und die Behauptung gilt (Algebra oder Satz 9.8). Sei nun $n \geq 2$. Dann ist $|G| = \varphi(p^n) = p^{n-1}(p-1)$. Die kanonische Abbildung $\Psi \colon G \to (\mathbb{Z}/p\mathbb{Z})^\times$, $a + p^n\mathbb{Z} \mapsto a + p\mathbb{Z}$ ist offenbar ein Epimorphismus. Insbesondere ist $P := \operatorname{Ker}(\Psi) \in \operatorname{Syl}_p(G)$ und $G/P \cong C_{p-1}$. Nach Satz 2.11 genügt es zu zeigen, dass P zyklisch ist. Wir zeigen genauer, dass P von $1 + p + p^n\mathbb{Z} \in P$ erzeugt wird. Dafür berechnet man

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

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

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

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

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

und

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

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

Satz 8.15. *Sei P eine p-Gruppe der Ordnung p^n mit einer zyklischen Untergruppe der Ordnung p^{n-1}. Dann gilt eine der folgenden Aussagen:*

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

(ii) $n \geq 3$ *und* $P \cong M_{p^n} := \langle x, y \mid x^{p^{n-1}} = y^p = 1,\ yxy^{-1} = x^{1+p^{n-2}} \rangle$ (modulare Gruppe[19]).

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

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

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

Beweis. Ist P abelsch, so gilt offenbar (i) nach Satz 2.11. Sei nun P nichtabelsch. Dann ist $n \geq 3$. Sei $x \in P$ mit $|\langle x \rangle| = p^{n-1}$. Dann ist $\langle x \rangle \trianglelefteq P$ nach Satz 4.10. Nehmen wir zunächst an, dass $\langle x \rangle$ ein Komplement in P besitzt, d. h. es gilt $P = \langle x \rangle \rtimes \langle y \rangle$ für ein $y \in P$ mit $y^p = 1$. Ist $p > 2$, so ist $\mathrm{Aut}(\langle x \rangle)$ zyklisch nach Satz 8.14. Indem man y notfalls durch eine Potenz ersetzt, erreicht man $yxy^{-1} = x^{1+p^{n-2}}$, denn $(1 + p^{n-2})^p \equiv 1 \pmod{p^{n-1}}$. Nach Satz 8.10 existiert ein Epimorphismus $M_{p^n} \to P$. Offenbar gilt $|M_{p^n}| \leq p^n$ und es folgt $P \cong M_{p^n}$.

Sei nun $p = 2$. Im Fall $n = 3$ ist $\mathrm{Aut}(\langle x \rangle)$ immer noch zyklisch und man erhält wieder $P \cong M_8 \cong D_8$. Sei also $n \geq 4$. Nach Satz 8.14 besitzt $\mathrm{Aut}(\langle x \rangle)$ genau drei Involutionen (=Elemente der Ordnung 2): $x \mapsto x^{-1}$, $x \mapsto x^{1+2^{n-2}}$ und $x \mapsto x^{-1+2^{n-2}}$. Der erste Fall führt zu $P \cong D_{2^n}$, der zweite zu $P \cong M_{2^n}$ und der dritte zu $P \cong SD_{2^n}$.

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

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

Im Fall $yxy^{-1} = x^{1+p^{n-2}}$ ist $[y, x] = x^{1+p^{n-2}}x^{-1} = x^{p^{n-2}} \in \mathrm{Z}(P)$ und Aufgabe 16(b) liefert

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

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

Satz 8.16. *Die Gruppen M_{p^n}, D_{2^n}, Q_{2^n} und SD_{2^n} haben die Ordnung p^n (bzw. 2^n) und sind paarweise nicht isomorph.*

[19] *Modular* bedeutet, dass eine Verallgemeinerung der Dedekind-Identität gilt: $U \leq W \Rightarrow \langle U, V \rangle \cap W = \langle U, V \cap W \rangle$ für alle $U, V, W \leq G$. Für $G = M_{p^n}$ gilt sogar $\langle U, V \rangle = UV$, d. h. $UV = VU$ für alle $U, V \leq M_{p^n}$ (Aufgabe 63)

Beweis. Es ist klar, dass man semidirekte Produkte $C_{p^{n-1}} \rtimes C_p$ mit geeigneten Operationen konstruieren kann. Somit zeigt Satz 8.15, dass M_{p^n}, D_{2^n} und SD_{2^n} die „richtige“ Ordnung haben. Sei nun $\zeta := e^{2\pi \mathrm{i}/2^{n-1}} \in \mathbb{C}$ und $Q = \langle x, y \rangle \leq \mathrm{GL}(2, \mathbb{C})$ mit

$$x := \begin{pmatrix} \zeta & 0 \\ 0 & \zeta^{-1} \end{pmatrix}, \qquad y := \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

Offenbar gilt $x^{2^{n-1}} = 1$, $y^2 = x^{2^{n-2}}$ und $yxy^{-1} = x^{-1}$. Also hat jedes Element in Q die Form $x^i y^j$ mit $i \in \{0, \ldots, 2^{n-1} - 1\}$ und $j \in \{0, 1\}$. Wegen $y \notin \langle x \rangle$ ist $|Q| = 2^n$. Nach Satz 8.15 gilt $Q \cong Q_{2^n}$.

Es verbleibt zu zeigen, dass die Gruppen M_{2^n}, D_{2^n}, Q_{2^n} und SD_{2^n} paarweise nicht isomorph sind (mit der Ausnahme $M_8 \cong D_8$). Die semidirekten Produkte M_{2^n}, D_{2^n} und SD_{2^n} besitzen mindestens zwei Involutionen. In Q_{2^n} ist andererseits $(x^i y)^2 = x^i y x^i y^{-1} y^2 = y^2 \neq 1$ für $i \in \mathbb{Z}$. Daher besitzt Q_{2^n} nur eine Involution und es gilt $Q_{2^n} \ncong M_{2^n}$, $Q_{2^n} \ncong D_{2^n}$ und $Q_{2^n} \ncong SD_{2^n}$. Wir können nun $n \geq 4$ annehmen. In der Gruppe M_{2^n} gilt $\langle [x, y] \rangle = \langle x(yx^{-1}y^{-1}) \rangle = \langle x^{2^{n-2}} \rangle \trianglelefteq M_{2^n}$. Da $M_{2^n}/\langle [x, y] \rangle$ abelsch ist, gilt $M'_{2^n} = \langle [x, y] \rangle \cong C_2$. In D_{2^n} gilt andererseits $[x, y] = x^2$ und damit $|D'_{2^n}| \geq 2^{n-2}$. In SD_{2^n} ist analog $[x, y] = x^{2+2^{n-2}}$ und $|SD'_{2^n}| \geq 2^{n-2}$. Dies zeigt $M_{2^n} \ncong D_{2^n}$ und $M_{2^n} \ncong SD_{2^n}$. Schließlich müssen wir noch D_{2^n} von SD_{2^n} unterscheiden. Nach Burnsides Basissatz ist

$$D_{2^n}/\Phi(D_{2^n}) \cong C_2^2 \cong SD_{2^n}/\Phi(SD_{2^n}).$$

Die maximalen Untergruppen von D_{2^n} sind daher $\langle x \rangle \cong C_{2^{n-1}}$, $\langle x^2, y \rangle \cong D_{2^{n-1}}$ und $\langle x^2, xy \rangle \cong D_{2^{n-1}}$. Die maximalen Untergruppen von SD_{2^n} sind andererseits $\langle x \rangle \cong C_{2^{n-1}}$, $\langle x^2, y \rangle \cong D_{2^{n-1}}$ und $\langle x^2, xy \rangle \cong Q_{2^{n-1}} \ncong D_{2^{n-1}}$. Also ist $D_{2^n} \ncong SD_{2^n}$. □

9 Zentralprodukte und die verallgemeinerte Fittinggruppe

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

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

Beweis. Induktion nach n: Für $n = 3$ folgt die Behauptung aus Beispiel 4.22. Sei also $n \geq 4$ und $N \neq 1$. Da auch $P/\mathrm{Z}(P)$ maximale Klasse hat, gilt $|\mathrm{Z}(P)| = p$. Nach Satz 3.14 ist $\mathrm{Z}(P) \leq N$. Induktion impliziert daher $N/\mathrm{Z}(P) = \mathrm{Z}_{k-1}(P/\mathrm{Z}(P)) = \mathrm{Z}_k(P)/\mathrm{Z}(P)$ und $N = \mathrm{Z}_k(P)$. Nach Bemerkung 9.1 ist auch $P^{[n-k]}$ ein Normalteiler der Ordnung p^k. Also ist $P^{[n-k]} = \mathrm{Z}_k(P) = N$. □

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

(1) P hat maximale Klasse.

(2) $|P : P'| = 4$.

(3) P ist eine Diedergruppe, eine Quaternionengruppe oder eine Semidiedergruppe.

Beweis. Die Implikation (1)⇒(2) folgt aus Bemerkung 9.1. Sei nun $|P : P'| = 4$. Sei $2^n := |P|$ minimal, sodass (3) nicht erfüllt ist. Wir haben in Satz 8.16 bereits gesehen, dass $|M'_{2^n}| = 2$ gilt. Nach Satz 8.15 ist daher $\exp(P) \leq 2^{n-2}$. Sei $Z \leq \mathrm{Z}(P) \cap P'$ mit $|Z| = 2$ (Satz 3.14). Dann ist $|P/Z : (P/Z)'| = |P/P'| = 4$. Nach Wahl von P ist $P/Z \in \{D_{2^{n-1}}, Q_{2^{n-1}}, SD_{2^{n-1}}\}$. Sei also $x \in P$ mit $|P : \langle x\rangle Z| = 2$. Wegen $Z \leq \mathrm{Z}(P)$ und $\exp(P) \leq 2^{n-2}$ ist $\langle x\rangle Z \cong C_{2^{n-2}} \times C_2$. Aus Aufgabe 26 folgt $\mathrm{Z}(P) = Z$. Für $y \in P \setminus \langle x\rangle Z$ gilt $yxy^{-1} \in x^{-1}Z \cup x^{-1+2^{n-3}}Z$ und $yx^2y^{-1} = x^{-2}$. Dies liefert den Widerspruch $x^{2^{n-3}} \in \mathrm{Z}(P) = Z$. Also muss (3) gelten.

Sei nun $P \in \{D_{2^n}, Q_{2^n}, SD_{2^n}\}$. Wir zeigen (1) durch Induktion nach n (vgl. Aufgabe 17). Im Fall $n = 3$ sind D_8 und Q_8 nichtabelsch und daher von maximaler Klasse. Sei nun $n \geq 4$. Dann ist $[x, y] \in \{x^2, x^{2+2^{n-2}}\}$ und $P' = \langle x^2\rangle$. Aus Aufgabe 26 folgt $\mathrm{Z}(P) = \langle x^{2^{n-2}}\rangle$. Nach Induktion hat $P/\mathrm{Z}(P) \cong D_{2^{n-1}}$ maximale Klasse und daher auch P. □

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

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

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

Nehmen wir $A < C$ an. Wie üblich existiert ein $N \trianglelefteq P$ mit $A < N \leq C$ und $|N : A| = p$. Nach Wahl von A ist N nichtabelsch und wir können Satz 8.15 anwenden. Wegen $B \leq \mathrm{Z}(N)$ kommt nach Taussky nur $N \cong M_{p^n}$ in Frage. Es gilt $M'_{p^n} = \langle x^{p^{n-2}}\rangle \cong C_p$ und $M_{p^n}/M'_{p^n} \cong C_{p^{n-2}} \times C_p$. Jedes Element der Ordnung p in M_{p^n} liegt also in $\langle x^{p^{n-3}}, y\rangle$. Da $x^{p^{n-3}}$ Ordnung p^2 hat, bilden die Elemente der Ordnung p in M_{p^n} die charakteristische Untergruppe $E := \langle x^{p^{n-2}}, y\rangle \cong C_p \times C_p$. Dann ist E aber ein nicht-zyklischer, abelscher Normalteiler von P. Dieser Widerspruch zeigt $A = C$.

Also ist $|P : A| = p$. Wieder lässt sich Satz 8.15 anwenden. Der Fall $P \cong M_{p^n}$ ist wie eben ausgeschlossen. Dies zeigt die Behauptung. □

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

(1) P besitzt nur eine Untergruppe der Ordnung p.

(2) Jede abelsche Untergruppe von P ist zyklisch.

(3) P ist zyklisch oder eine Quaternionengruppe.

Beweis. Die Implikation (1)⇒(2) folgt aus Satz 2.11. Gilt (2), so ist P zyklisch, eine Diedergruppe, eine Quaternionengruppe oder eine Semidiedergruppe nach Satz 9.5. In (Semi)diedergruppen ist die abelsche Untergruppe $\langle x^{2^{n-2}}, y\rangle$ nicht zyklisch. Dies zeigt (3). Nehmen wir nun (3) an. Ist P zyklisch, so folgt (1) aus Satz 2.4. Für Quaternionengruppen hatten wir in Satz 8.16 bereits gesehen, dass nur eine Involution existiert. □

Lemma 9.7. *Für jede Primzahl p existieren $\lambda, \mu \in \mathbb{F}_p$ mit $\lambda^2 + \mu^2 = -1$.*

Beweis. Für $p = 2$ wähle man $\lambda = 1$ und $\mu = 0$. Sei daher $p > 2$. Aus $\lambda^2 = \mu^2$ folgt $(\lambda+\mu)(\lambda-\mu) = 0$ und $\lambda = \pm\mu$. Dies zeigt $|\{\lambda^2 + 1 : \lambda \in \mathbb{F}_p\}| = |\{-\mu^2 : \mu \in \mathbb{F}_p\}| \geq \lceil p/2 \rceil > p/2$. Nach dem Schubfachprinzip ist

$$\{\lambda^2 + 1 : \lambda \in \mathbb{F}_p\} \cap \{-\mu^2 : \mu \in \mathbb{F}_p\} \neq \varnothing. \qquad \square$$

Satz 9.8 (Wedderburn)**.** *Jeder endliche Schiefkörper ist ein Körper mit zyklischer Einheitengruppe.*

Beweis (Kaczynski). Sei K ein endlicher Schiefkörper und $p \in \mathbb{N}$ die Ordnung von 1 in $(K, +)$. Angenommen p ist keine Primzahl, etwa $p = ab$ mit $a, b > 1$. Dann ist

$$\sum_{i=1}^{a} 1 \cdot \sum_{i=1}^{b} 1 = \sum_{i=1}^{p} 1 = 0.$$

Da K ein Schiefkörper ist, erhält man den Widerspruch $\sum_{i=1}^{a} 1 = 0$ oder $\sum_{i=1}^{b} 1 = 0$. Daher ist p eine Primzahl und K ist ein $\mathbb{F}_p$-Vektorraum. Für eine Untergruppe $H \leq G := K^\times$ sei

$$L(H) := \operatorname{span}_{\mathbb{F}_p} H \subseteq K.$$

Nach dem Distributivgesetz ist $L(H)$ unter Multiplikation abgeschlossen. Da jedes Element in G endliche Ordnung hat, ist $L(H)$ auch unter Division abgeschlossen, d. h. $L(H)$ ist selbst ein Schiefkörper. Nehmen wir an, dass H eine elementarabelsche q-Gruppe vom Rang 2 ist. Dann ist $L(H)$ ein Körper, in dem das Polynom $X^q - 1$ mehr als q Nullstellen besitzt. Dieser Widerspruch zeigt, dass jede abelsche Untergruppe von G zyklisch ist. Nach Satz 9.6 ist jede Sylowgruppe von G zyklisch oder eine Quaternionengruppe.

Nehmen wir an, dass eine 2-Sylowgruppe P von G tatsächlich eine Quaternionengruppe ist. Wegen $|G| = |K| - 1$ ist dann $p > 2$. Seien $x, y \in P$ der Ordnung 4 mit $xy = yx^{-1}$. Im Körper $L(\langle x \rangle)$ ist $x^2 \neq 1$ eine Nullstelle von $X^2 - 1$, also $x^2 = -1$ und $xy = -yx$. Analog gilt $y^2 = -1$. Seien $\lambda, \mu \in \mathbb{F}_p$ wie in Lemma 9.7. Dann gilt

$$(\lambda x + y + \mu)(\lambda x + y - \mu) = (\lambda x + y)^2 - \mu^2 = -\lambda^2 - 1 - \mu^2 = 0.$$

Also ist $y = -\lambda x \pm \mu$ und man hat den Widerspruch $xy = yx = -xy$. Nun sind alle Sylowgruppen von G zyklisch. Es genügt zu zeigen, dass G abelsch ist.

Nach Satz 7.24 ist G zumindest auflösbar. Nehmen wir $G \neq \mathrm{Z}(G)$ an. Sei $A/\mathrm{Z}(G)$ ein minimaler Normalteiler von $G/\mathrm{Z}(G)$. Dann ist $A/\mathrm{Z}(G)$ eine elementarabelsche q-Gruppe. Da die q-Sylowgruppen von G und $G/\mathrm{Z}(G)$ zyklisch sind, gilt $|A/\mathrm{Z}(G)| = q$. Nach Aufgabe 8 ist A abelsch. Seien $g \in G$ und $x \in A$ beliebig. Wegen $A \trianglelefteq G$ existiert $y \in A$ mit $(1 + g)x = y(1 + g)$ (auch wenn $1 + g = 0$). Es folgt

$$x - y = yg - gx = (y - gxg^{-1})g.$$

Im Fall $x - y = y - gxg^{-1} = 0$ ist $x = y = gxg^{-1}$, d. h. $g \in \mathrm{C}_G(x)$. Anderenfalls ergibt sich $g = (y - gxg^{-1})^{-1}(x - y) \in \mathrm{C}_G(x)$, da A abelsch ist. Da $g \in G$ und $x \in A$ beliebig waren, folgt der Widerspruch $A \leq \mathrm{Z}(G)$. Also ist $K^\times = G = \mathrm{Z}(G)$ abelsch und zyklisch. $\square$

Satz 9.9. *Für eine Primzahl p gibt es bis auf Isomorphie genau fünf Gruppen der Ordnung p^3. Diese sind gegeben durch:*

(i) C_{p^3}.

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

(iii) C_p^3.

(iv) M_{p^3}.

(v) Q_8 *für* $p = 2$.

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

Beweis. Sei $|P| = p^3$. Wir können sicher annehmen, dass P nichtabelsch ist. Nach Satz 8.15 dürfen wir auch $\exp(P) = p$ voraussetzen. Dann ist $p > 2$, denn anderenfalls wäre $xy = (xy)^{-1} = y^{-1}x^{-1} = yx$ für $x, y \in P$. Wegen $|P : \Phi(P)| = p^2$ lässt sich P durch zwei Elemente x, y erzeugen. Sicher ist dann $x^p = y^p = 1$ und $[x, x, y], [y, x, y] \in P^{[3]} = 1$. Nach Satz 8.10 gibt es einen Epimorphismus $p_+^{1+2} \to P$. Wir müssen nun zeigen, dass $|p_+^{1+2}| \leq p^3$ gilt. Sei dafür $z := [x, y]$. Nach Aufgabe 16 ist $z^p = [x^p, y] = 1$. Wegen $xy = [x, y]yx = zyx = yxz$ lässt sich jedes Element in p_+^{1+2} in der Form $x^i y^j z^k$ mit $i, j, k \in \{0, \ldots, p-1\}$ schreiben. Dies zeigt $P \cong p_+^{1+2}$.

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

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

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

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

Dies zeigt $\exp(P) = p$. □

Definition 9.10. Eine p-Gruppe P heißt *extraspeziell*, falls $P' = \Phi(P) = \mathrm{Z}(P) \cong C_p$ gilt.

Beispiel 9.11. Nach Beispiel 4.22 ist jede nichtabelsche Gruppe der Ordnung p^3 extraspeziell.

Lemma 9.12. *Sei P extraspeziell und $\alpha \in \mathrm{Aut}(P)$ mit $\alpha(x)\mathrm{Z}(P) = x\mathrm{Z}(P)$ für alle $x \in P$. Dann ist $\alpha \in \mathrm{Inn}(P)$.*

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

Lemma 9.13. *Sei P eine extraspezielle Untergruppe einer Gruppe G mit $[G, P] \leq \mathrm{Z}(P)$. Dann ist $G = P\mathrm{C}_G(P)$.*

Beweis. Wegen $[G, P] \leq \mathrm{Z}(P) \leq P$ ist $P \trianglelefteq G$. Für $g \in G$ definiert $\alpha(x) := gxg^{-1}$ $(x \in P)$ einen Automorphismus auf P. Dabei gilt $\alpha(x)\mathrm{Z}(P) = gxg^{-1}x^{-1}x\mathrm{Z}(P) = [g, x]x\mathrm{Z}(P) = x\mathrm{Z}(P)$. Nach Lemma 9.12 ist α ein innerer Automorphismus auf P. Daher existiert ein $x \in P$ mit $gyg^{-1} = \alpha(y) = xyx^{-1}$ für alle $y \in P$. Es folgt $g = xx^{-1}g \in P\mathrm{C}_G(P)$. □

Definition 9.14. Eine Gruppe G heißt *Zentralprodukt* von Untergruppen $N_1, \ldots, N_k \leq G$, falls:

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

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

Bemerkung 9.15. Wegen $[N_i, N_j] = 1$ ist $N_i \trianglelefteq G = N_1 * \ldots * N_k$ für $i = 1, \ldots, k$. Somit ist die direkte Summe $N_1 \oplus \ldots \oplus N_k$ auch ein Zentralprodukt. Wie bei der direkten Summe gilt $N * M = M * N$ und $(N_1 * N_2) * N_3 = N_1 * (N_2 * N_3)$ (vgl. Bemerkung 2.8).

Beispiel 9.16. Es gilt $C_2 \cong C_2 * C_2$, aber auch $C_2^2 \cong C_2 * C_2$. Die Schreibweise $N_1 * \ldots * N_k$ ist also in der Regel nicht eindeutig.

Satz 9.17. *Sei $G = N_1 * \ldots * N_k$ mit $k \geq 2$. Dann ist $\bigcap_{i=1}^k N_i \leq \mathrm{Z}(G)$ und*

$$G/\mathrm{Z}(G) \cong N_1/\mathrm{Z}(N_1) \times \ldots \times N_k/\mathrm{Z}(N_k).$$

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

Bemerkung 9.18. Analog zum direkten Produkt (vs. direkte Summe) konstruieren wir nun ein „äußeres“ Zentralprodukt.

Satz 9.19. *Seien $G_1, \ldots, G_k$ Gruppen mit $Z_i \leq \mathrm{Z}(G_i)$ und $Z_1 \cong \ldots \cong Z_k$ mit $k \geq 2$. Dann existiert ein Zentralprodukt der Form $G = N_1 * \ldots * N_k$ mit $N_i \cong G_i$ $(i = 1, \ldots, k)$ und $\bigcap_{i=1}^k N_i \cong Z_1$.*

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

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

Sei $G := (G_1 \times \ldots \times G_k)/Z$. Dann wird G von den Normalteilern

$$N_i := G_iZ/Z \cong G_i/G_i \cap Z \cong G_i$$

erzeugt. Dabei gilt $[N_i, N_j] = [G_iZ/Z, G_jZ/Z] = [G_i, G_j]Z/Z = 1$ für $i \neq j$. Also ist $G = N_1 * \ldots * N_k$. Für $z_1 \in Z_1$ und $i \in \{1, \ldots, k\}$ ist $z_1Z = z_1z_1^{-1}\varphi_i(z_1)Z = \varphi_i(z_1)Z$. Dies zeigt

$$Z_1 \cong Z_1Z/Z = Z_iZ/Z \leq \bigcap_{i=1}^k N_i.$$

Sei nun $g_1Z = \ldots = g_kZ \in \bigcap_{i=1}^k N_i$ mit $g_i \in G_i$. Dann ist $g_1^{-1}g_i \in Z \leq Z_1 \times \ldots \times Z_k$ und es folgt $g_i \in Z_i$ für $i = 1, \ldots, k$. Also ist $\bigcap_{i=1}^k N_i = Z_1Z/Z \cong Z_1$. □

Satz 9.20. *Jede extraspezielle p-Gruppe P hat die Form $P = E_1 * \ldots * E_k$ mit $E_i \in \{D_8, Q_8\}$ (falls $p = 2$) bzw. $E_i \in \{M_{p^3}, p_+^{1+2}\}$ (falls $p > 2$) für $i = 1, \ldots, k$. Dabei ist $\bigcap_{i=1}^k E_i = \mathrm{Z}(P)$, falls $k \geq 2$. Insbesondere gilt $|P| = p^{2k+1}$.*

Beweis. Sei P extraspeziell der Ordnung p^n. Wir argumentieren durch Induktion nach n. Seien $x_1, y_1 \in P$ mit $[x_1, y_1] \neq 1$. Dann ist $P' = \langle [x_1, y_1] \rangle \leq \langle x_1, y_1 \rangle =: E_1 \trianglelefteq P$. Nach Lemma 4.15 ist $\Phi(E_1) \leq \Phi(P) = P'$. Aus Burnsides Basissatz folgt daher $|E_1| = p^3$ und $E_1 \in \{D_8, Q_8\}$ (bzw. $E_1 \in \{M_{p^3}, p_+^{1+2}\}$). Im Fall $P = E_1$ sind wir fertig. Sei also $E_1 < P$.

Nach Lemma 9.13 ist $P = E_1 Q$ mit $Q := \mathrm{C}_P(E_1)$. Es gilt $\mathrm{Z}(Q) \leq \mathrm{C}_P(E_1 Q) = \mathrm{Z}(P) = \mathrm{Z}(E_1)$. Insbesondere ist Q nichtabelsch und daher $1 \neq \Phi(Q) \leq Q' \leq P'$ und $\Phi(Q) = Q' = \mathrm{Z}(Q) = P' \cong C_p$. Dies zeigt, dass Q extraspeziell ist. Nach Induktion hat $Q = E_2 * \ldots * E_k$ die gewünschte Form mit $\mathrm{Z}(Q) \leq \bigcap_{i=2}^k E_i$. Also ist auch $P = E_1 * Q = E_1 * \ldots * E_k$ mit $\bigcap_{i=1}^k E_i = E_1 \cap Q = \mathrm{Z}(E_1) = \mathrm{Z}(P)$. Aus Satz 9.17 folgt

$$|P| = |\mathrm{Z}(P)||E_1/\mathrm{Z}(E_1)| \ldots |E_k/\mathrm{Z}(E_k)| = p^{2k+1}. \qquad \square$$

Bemerkung 9.21. Wir beschäftigen uns nun mit der Eindeutigkeit in Satz 9.20.

Lemma 9.22. *Sei P nichtabelsch der Ordnung p^3 und $a, b \in P' \setminus \{1\}$. Dann existiert ein $\alpha \in \mathrm{Aut}(P)$ mit $\alpha(a) = b$.*

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

Sei nun $P = \langle x, y \rangle \cong p_+^{1+2}$. Dann ist $a = [x, y]^i$ und $b = [x, y]^j$ für $i, j \in \mathbb{Z} \setminus p\mathbb{Z}$. Wie eben existiert ein $\alpha \in \mathrm{Aut}(P)$ mit $\alpha(x^i) = x^j$ und $\alpha(y) = y$. Nach Aufgabe 16 gilt

$$\alpha(a) = \alpha([x, y]^i) = \alpha([x^i, y]) = [x^j, y] = [x, y]^j = b. \qquad \square$$

Satz 9.23. *Für $k \geq 1$ gibt es bis auf Isomorphie genau zwei extraspezielle Gruppen der Ordnung p^{2k+1}:*

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

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

Beweis. Sei $P = E_1 * \ldots * E_k$ extraspeziell wie in Satz 9.20. Wir zeigen zunächst, dass der Isomorphietyp von P durch die E_i eindeutig bestimmt ist. Sei also $Q = F_1 * \ldots * F_k$ mit $E_i \cong F_i$ für $i = 1, \ldots, k$. Sei außerdem $\bigcap_{i=1}^k E_i \neq 1 \neq \bigcap_{i=1}^k F_i$ und damit $|P| = |Q|$ nach Satz 9.17. Wir wählen Isomorphismen $\varphi_i \colon E_i \to F_i$. Nach Lemma 9.22 können wir $\varphi_i(z) = \varphi_1(z)$ für $i = 2, \ldots, k$ und $z \in \mathrm{Z}(E_i) = \mathrm{Z}(P)$ annehmen. Jedes Element in P hat die Form $x_1 \ldots x_k$ mit $x_i \in E_i$ für $i = 1, \ldots, k$. Im Fall $x_1 \ldots x_k = 1$ gilt $x_i = (x_1 \ldots x_{i-1} x_{i+1} \ldots x_k)^{-1} \in \mathrm{Z}(E_i)$. Also ist

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

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

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

$(xa^{-1})^p = x^p a^{-p} = 1$, $[xa^{-1}, b]^p = [a^{-1}, b]^p = 1$ und $[xa^{-1}, xa^{-1}, b] = 1 = [b, xa^{-1}, b]$ ist $P_2 \cong p_+^{1+2}$. Schließlich ist $[x, xa^{-1}] = 1 = [x, b]$ und

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

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

Im Folgenden können wir $p = 2$ annehmen. Sei $P := D_8 * D_8 = \langle x, y\rangle * \langle a, b\rangle$ mit $x^2 = a^2 \neq 1$. Dann ist $P_1 := \langle x, ya\rangle \cong Q_8$ und $P_2 := \langle a, bx\rangle \cong Q_8$. Wegen $[ya, bx] = [y, x][a, b] = x^2a^2 = 1$ ist $P \cong P_1 * P_2 \cong Q_8 * Q_8$. Es gibt also auch hier höchstens zwei extraspezielle Gruppen der Ordnung 2^{2k+1}. Der Nachweis $2_-^{1+2k} \ncong 2_+^{1+2k}$ gestaltet sich schwieriger, da beide Gruppen Exponent 4 haben. Sei

$$\begin{aligned} f_2(k) &:= |\{x \in 2_+^{1+2k} : x^2 = 1\}|, \\ f_4(k) &:= |\{x \in 2_+^{1+2k} : |\langle x\rangle| = 4\}| = 2^{2k+1} - f_2(k). \end{aligned}$$

Wir zeigen $f_4(k) = 2^{2k} - 2^k$ durch Induktion nach $k \in \mathbb{N}$. Für $k = 1$ ist $2_+^{1+2} = D_8$ und $f_4(1) = 2$. Für $k \geq 1$ ist $2_+^{1+2(k+1)} = 2_+^{1+2k} * D_8 \cong (2_+^{1+2k} \times D_8)/Z$, wobei $Z := \langle (z, z)\rangle \leq \mathrm{Z}(2_+^{1+2k}) \times \mathrm{Z}(D_8)$ (siehe Beweis von Satz 9.19). Sei $(x, y) \in 2_+^{1+2k} \times D_8$ der Ordnung 4. Dann hat x oder y Ordnung 4. Haben x und y Ordnung 4, so ist $x^4 = y^4 = z$ und die Nebenklasse $(x, y)Z$ hat Ordnung 2. Daher gilt

$$f_4(k+1) = \frac{f_4(k)f_2(1) + f_2(k)f_4(1)}{2} = 3f_4(k) + f_2(k) = 3(2^{2k} - 2^k) + 2^{2k} + 2^k = 2^{2(k+1)} - 2^{k+1}.$$

Sei nun $g_2(k) := |\{x \in 2_-^{1+2k} : x^2 = 1\}|$ und $g_4(k) = 2^{2k+1} - g_2(k)$. Dann ist $g_2(1) = 2 = f_4(1)$ und $g_4(1) = 6 = f_2(1)$. Wegen $2_+^{1+2(k+1)} = 2_+^{1+2k} * Q_8$ folgt

$$g_4(k+1) = \frac{f_4(k)g_2(1) + f_2(k)g_4(1)}{2} = f_4(k) + 3f_2(k) = 2^{2(k+1)} + 2^{k+1} = f_2(k+1)$$

für $k \geq 0$. Insbesondere ist $f_4(k) \neq g_4(k)$. □

Definition 9.24. Eine Untergruppe $H \leq G$ heißt *subnormal*, falls eine Folge $H = H_0 \trianglelefteq H_1 \trianglelefteq \ldots \trianglelefteq H_k = G$ existiert. Wir schreiben $H \trianglelefteq\trianglelefteq G$. Subnormalität ist also der transitive Abschluss der Normalteilerrelation.

Beispiel 9.25. Jede Untergruppe einer nilpotenten Gruppe ist subnormal nach Satz 4.10.

Bemerkung 9.26. Für $H \trianglelefteq\trianglelefteq G$ muss die Folge $H \trianglelefteq \mathrm{N}_G(H) \trianglelefteq \mathrm{N}_G(\mathrm{N}_G(H)) \trianglelefteq \ldots$ nicht unbedingt bei G enden. Zum Beispiel ist $\langle (1,2)(3,4)\rangle \trianglelefteq \langle (1,3,2,4), (1,2)\rangle =: P \in \mathrm{Syl}_2(S_4)$, aber $P = \mathrm{N}_{S_4}(P)$. Andererseits ist $\langle (1,2)(3,4)\rangle \trianglelefteq V_4 \trianglelefteq S_4$.

Lemma 9.27. *Sei $H \trianglelefteq\trianglelefteq G$ und M ein minimaler Normalteiler von G. Dann gilt $M \leq \mathrm{N}_G(H)$.*

Beweis. O. B. d. A. sei $H < G$ und $H \trianglelefteq\trianglelefteq N \lhd G$. Die Minimalität von M zeigt $N \cap M \in \{1, M\}$. Im Fall $N \cap M = 1$ gilt $M \leq \mathrm{C}_G(N) \leq \mathrm{C}_G(H) \leq \mathrm{N}_G(H)$. Sei also $M \leq N$. Sei $K \leq M$ ein minimaler Normalteiler von N. Durch Induktion nach $|G|$ können wir $K \leq \mathrm{N}_N(H)$ annehmen. Für $g \in G$ ist auch gKg^{-1} ein minimaler Normalteiler von N. Dies zeigt

$$M = K^G = \langle gKg^{-1} : g \in G\rangle \leq \mathrm{N}_N(H) \leq \mathrm{N}_G(H).$$ □

Satz 9.28 (Wielandt). *Für $H, K \trianglelefteq\trianglelefteq G$ gilt $\langle H, K\rangle \trianglelefteq\trianglelefteq G$.*

Beweis. Sei M ein minimaler Normalteiler von G und $\overline{G} := G/M$. Offenbar ist $\overline{H}, \overline{K} \trianglelefteq\trianglelefteq \overline{G}$. Durch Induktion nach $|G|$ können wir $\langle \overline{H}, \overline{K}\rangle \trianglelefteq\trianglelefteq \overline{G}$ annehmen. Dies zeigt $\langle H, K\rangle M \trianglelefteq\trianglelefteq G$. Nach Lemma 9.27 gilt $\langle H, K\rangle \trianglelefteq \langle H, K\rangle M$ und die Behauptung folgt. □

Lemma 9.29. *Sei $H \leq G$ nicht subnormal in G. Für alle $H \leq K < G$ gelte $H \trianglelefteq\trianglelefteq K$. Dann ist H in genau einer maximalen Untergruppe von G enthalten.*

Beweis. Induktion nach $|G : H|$. Nach Voraussetzung existiert eine maximale Untergruppe $M < G$ mit $\mathrm{N}_G(H) \leq M$. Sei auch $K < G$ maximal mit $H \leq K$. Nach Voraussetzung ist $H \trianglelefteq\trianglelefteq K$. Gilt sogar $H \trianglelefteq K$, so ist $K \leq \mathrm{N}_G(H) \leq M$ und $K = M$ wie gewünscht. Sei also $H \not\trianglelefteq K$. Sei $H = H_0 \trianglelefteq \ldots \trianglelefteq H_s = K$ mit $s \geq 2$ minimal. Dann existiert $g \in H_2$ mit $gHg^{-1} \neq H$. Es gilt nun $\tilde{H} := \langle H, gHg^{-1}\rangle \leq K$ und $gHg^{-1} \leq gH_1g^{-1} = H_1 \leq \mathrm{N}_G(H)$. Dies zeigt $\tilde{H} \leq \mathrm{N}_G(H) \leq M$ und $H \trianglelefteq \tilde{H} < G$.

Sei $\tilde{H} \leq L < G$. Dann ist $H \trianglelefteq\trianglelefteq L$ und aus Symmetriegründen auch $gHg^{-1} \trianglelefteq\trianglelefteq L$. Aus Satz 9.28 folgt $\tilde{H} \trianglelefteq\trianglelefteq L$. Da H nicht subnormal in G ist, kann auch $\tilde{H}$ nicht subnormal in G sein. Somit erfüllt auch $\tilde{H}$ die Voraussetzung. Nach Induktion ist M die einzige maximale Untergruppe, die $\tilde{H}$ enthält. Wegen $\tilde{H} \leq K$ muss $M = K$ gelten. □

Satz 9.30 (Baer-Suzuki). *Für $H \leq G$ gilt $H \leq \mathrm{F}(G)$ genau dann, wenn $\langle H, gHg^{-1}\rangle$ für alle $g \in G$ nilpotent ist.*

Beweis. Ist $H \leq \mathrm{F}(G) \trianglelefteq G$, so ist $\langle H, gHg^{-1}\rangle \leq \mathrm{F}(G)$ nilpotent. Nehmen wir umgekehrt an, dass $\langle H, gHg^{-1}\rangle$ für alle $g \in G$ nilpotent ist. Dann ist H nilpotent und es genügt $H \trianglelefteq\trianglelefteq G$ zu zeigen (Aufgabe 69). Neben wir das Gegenteil an. Sei $H \leq K < G$. Durch Induktion nach $|G|$ ist $H \trianglelefteq\trianglelefteq K$. Nach Lemma 9.29 liegt H in genau einer maximalen Untergruppe $M < G$. Für $g \in G$ ist $H \leq \langle H, gHg^{-1}\rangle < G$ (anderenfalls wäre $\mathrm{F}(G) = G$) und daher $\langle H, gHg^{-1}\rangle \leq M$. Es folgt $H^G \leq M$ und $H \trianglelefteq\trianglelefteq H^G \trianglelefteq G$. Widerspruch. □

Folgerung 9.31. *Sei $x \in G$ und $\langle x, gxg^{-1}\rangle$ für alle $g \in G$ eine p-Gruppe. Dann ist $x \in \mathrm{O}_p(G)$.*

Beweis. Für $H := \langle x\rangle$ gilt $\langle H, gHg^{-1}\rangle = \langle x, gxg^{-1}\rangle$. Baer-Suzuki zeigt daher $H \leq \mathrm{F}(G)$. Als p-Gruppe liegt H in der einzigen p-Sylowgruppe $\mathrm{O}_p(G)$ von $\mathrm{F}(G)$ (Satz 4.11). □

Folgerung 9.32. *Sei $x \in G \setminus \mathrm{O}_2(G)$ eine Involution. Dann existiert ein Element $y \in G \setminus \{1\}$ mit ungerader Ordnung und $xyx^{-1} = y^{-1}$.*

Beweis. Nach Folgerung 9.31 existiert $g \in G$, sodass $D := \langle x, gxg^{-1}\rangle$ keine 2-Gruppe ist. Da auch gxg^{-1} eine Involution ist, ist D eine Diedergruppe nach Aufgabe 30. Insbesondere ist die Ordnung von $y := xgxg^{-1}$ keine 2-Potenz. Zudem gilt $xyx^{-1} = gxg^{-1}x^{-1} = y^{-1}$. Indem wir y durch eine Potenz ersetzen, können wir erreichen, dass $|\langle y\rangle| > 1$ ungerade ist. □

Beispiel 9.33. Folgerung 9.31 wurde in viele Richtungen verallgemeinert (ohne Beweis):

- (Revin) Sei π eine Menge ungerader Primzahlen. Sei $x \in G$ und $\langle x, gxg^{-1}\rangle$ für alle $g \in G$ eine π-Gruppe. Dann ist $x \in \mathrm{O}_\pi(G)$.

- (Guralnick, Tong-Viet, Tracey) Sei $x \in G$ ein p-Element und $[x, g]$ ein p-Element für alle p'-Elemente $g \in G$. Dann ist $x \in \mathrm{O}_p(G)$.
- (Guest) Sei $x \in G$ ein Element mit Primzahlordnung $p \geq 5$. Ist $\langle x, gxg^{-1} \rangle$ für alle $g \in G$ auflösbar, so ist $\langle gxg^{-1} : g \in G \rangle$ auflösbar.
- (Thompson) Genau dann ist G auflösbar, wenn $\langle x, y \rangle$ für alle $x, y \in G$ auflösbar ist.

Bemerkung 9.34. Für Induktionsbeweise benutzen wir oft minimale Normalteiler N aufgrund ihrer einfachen Struktur (Satz 2.27). Allerdings hat man keinerlei Kontrolle über G/N. Für auflösbare Gruppen ist $F(G)$ ein guter Ersatz für N nach Bemerkung 3.20. Wir konstruieren nun eine Verallgemeinerung der Fittinggruppe für nicht-auflösbare Gruppen mit ähnlich guten Eigenschaften.

Definition 9.35.

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

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

Beispiel 9.36. Jede nichtabelsche einfache Gruppe ist quasieinfach.

Lemma 9.37. *Sei K eine Komponente von G. Dann gilt:*

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

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

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

Beweis.

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

(ii) Es gilt $N\mathrm{Z}(K)/\mathrm{Z}(K) \trianglelefteq K/\mathrm{Z}(K)$. Da $K/\mathrm{Z}(K)$ einfach ist, gilt $N \leq \mathrm{Z}(K)$ oder $K = N\mathrm{Z}(K)$. Im zweiten Fall wäre $K = K' = (N\mathrm{Z}(K))' = N' \leq N$.

(iii) Hier ist $N \cap K \lhd K$ und $N \cap K \leq \mathrm{Z}(K)$ nach (ii). Dies zeigt $(K/K \cap N)/(\mathrm{Z}(K)/K \cap N) \cong K/\mathrm{Z}(K)$. Wegen

$$\mathrm{Z}(K)/K \cap N \leq \mathrm{Z}(K/K \cap N) \trianglelefteq K/K \cap N$$

folgt $\mathrm{Z}(K/K \cap N) = \mathrm{Z}(K)/K \cap N$, da $K/\mathrm{Z}(K)$ einfach ist. Insbesondere ist $(K/K \cap N)/\mathrm{Z}(K/K \cap N)$ einfach. Außerdem ist $(KN/N)' = K'N/N = KN/N$. Somit ist $KN/N \cong K/K \cap N$ quasieinfach. Schließlich ist $KN/N = K_0N/N \trianglelefteq \ldots \trianglelefteq K_nN/N = G/N$. □

Lemma 9.38. *Sei K eine Komponente von G und $H \trianglelefteq\trianglelefteq G$. Dann ist $K \leq H$ oder $[K, H] = 1$.*

Beweis. Wir können $H < G$ annehmen. Sei also $H \leq N \lhd G$. Im Fall $G = K$ erhält man $H \leq N \leq \mathrm{Z}(G)$ aus Lemma 9.37. Dann gilt $[K, H] = 1$. Wir können daher $K < G$ annehmen. Sei $K \leq M \lhd G$. Dann ist $H_1 := [H, K] \leq [N, M] \leq N \cap M$ und $K \leq \mathrm{N}_M(H_1) =: G_1 \leq M < G$ nach Lemma 3.3. Nach Lemma 9.37 ist K eine Komponente von G_1 und $H_1 \trianglelefteq G_1$. Durch Induktion nach $|G|$ können wir $[K, H_1] = 1$ oder $K \leq H_1$ annehmen. Im ersten Fall ist $1 = [K, H, K] = [K, K, H]$. Aus Lemma 3.6 folgt $[H, K] = [H, K'] = [H, K, K] = 1$. Sei also $K \leq H_1 \leq N$. Dann ist K eine Komponente von N und $H \trianglelefteq\trianglelefteq N$. Per Induktion gilt die Behauptung für N und wir sind fertig. □

Satz 9.39. *Seien $K_1, \ldots, K_n$ die Komponenten von G. Dann ist*

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

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

Beweis. Für $i \neq j$ gilt $[K_i, K_j] = 1$, denn anderenfalls wäre $K_i \leq K_j \leq K_i$ nach Lemma 9.38. Dies zeigt $\mathrm{E}(G) = K_1 * \ldots * K_n$. Da $\mathrm{F}(G)$ nilpotent ist, kann $\mathrm{F}(G)$ keine Komponente von G enthalten. Lemma 9.38 liefert also $[\mathrm{F}(G), K_i] = 1$ und $[\mathrm{F}(G), \mathrm{E}(G)] = 1$. □

Definition 9.40. Man nennt

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

die *verallgemeinerte Fittinggruppe* von G.

Beispiel 9.41. Für $n \geq 5$ ist $\mathrm{F}^*(S_n) = \mathrm{E}(S_n) = A_n$, denn A_n ist eine Komponente von S_n.

Bemerkung 9.42. Der nächste Satz verallgemeinert Satz 3.19.

Satz 9.43. *Es gilt* $\mathrm{C}_G(\mathrm{F}^*(G)) \leq \mathrm{F}^*(G)$.

Beweis. Sei $G \neq 1$. Wir zeigen zunächst $\mathrm{F}^*(G) \neq 1$. Sei dafür N ein minimaler Normalteiler von G. Ist N abelsch, so gilt $1 \neq N \leq \mathrm{F}(G) \leq \mathrm{F}^*(G)$. Anderenfalls ist $N = T_1 \oplus \ldots \oplus T_n$ mit nichtabelschen einfachen Gruppen $T_1, \ldots, T_n$ nach Satz 2.27. Wegen $T_i \trianglelefteq N \trianglelefteq G$ sind die T_i Komponenten und es folgt $1 \neq N \leq \mathrm{E}(G) \leq \mathrm{F}^*(G)$.

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

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

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

und $K = K''\mathrm{Z}(C)$. Insbesondere ist $K/K'' \cong \mathrm{Z}(C)/\mathrm{Z}(C) \cap K''$ abelsch und $K' = K''$. Aus $K \trianglelefteq\trianglelefteq C$ folgt $K' \trianglelefteq\trianglelefteq C$. Um zu zeigen, dass $K'/\mathrm{Z}(K')$ einfach ist, nehmen wir $\mathrm{Z}(K') < N \trianglelefteq K'$ an. Dann ist $N\mathrm{Z}(C)/\mathrm{Z}(C) \trianglelefteq\trianglelefteq C/\mathrm{Z}(C)$ und Lemma 9.38 zeigt $K \leq N\mathrm{Z}(C)$ oder $[K, N] \leq \mathrm{Z}(C)$. Im ersten Fall ist $K' \leq (N\mathrm{Z}(C))' \leq N' \leq N \leq K'$. Im zweiten Fall ist $[K, K, N] = [K, N, K] = 1$ und Lemma 3.6 liefert den Widerspruch $[N, K'] = [N, K, K] = 1$. Also ist $K'/\mathrm{Z}(K')$ einfach und K' ist eine Komponente von $C \trianglelefteq G$. Dann ist K' auch eine Komponente von G und wir erhalten den Widerspruch $K' \leq \mathrm{F}^*(G) \cap C \leq \mathrm{Z}(C)$. Somit besitzt $C/\mathrm{Z}(C)$ keine Komponenten und $\mathrm{F}^*(C/\mathrm{Z}(C)) = 1$. □

Beispiel 9.44. Sei $\mathrm{F}^*(G) = \mathrm{E}(G) = K$ quasieinfach. Nach Satz 9.43 ist

$$G/K \cong (G/\mathrm{C}_G(K))/(K/\mathrm{Z}(K)) \leq \mathrm{Out}(K) \overset{\text{Aufgabe 70}}{\leq} \mathrm{Out}(K/\mathrm{Z}(K)).$$

Eine Vermutung von Schreier (die bislang nur mit der Klassifikation der einfachen Gruppen bewiesen werden konnte) besagt, dass $\mathrm{Out}(S)$ für jede einfache Gruppe S auflösbar ist. Daher ist $K/\mathrm{Z}(K)$ der einzige nichtabelsche Kompositionsfaktor von G. Ein Satz von Hölder besagt

$$\mathrm{Out}(A_n) = \begin{cases} C_2^2 & \text{falls } n = 6, \\ C_2 & \text{falls } n \in \{5, 7, 8, \ldots\}. \end{cases}$$

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

Bemerkung 10.1.

(i) Im Folgenden sei $n \in \mathbb{N}$ und $q \neq 1$ eine Primzahlpotenz. Sei $\mathbb{F}_q$ der Körper mit q Elementen (Algebra) und $\mathrm{GL}(n,q) := \mathrm{GL}(n,\mathbb{F}_q)$ sowie $\mathrm{SL}(n,q) := \mathrm{SL}(n,\mathbb{F}_q)$.

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

Lemma 10.2. *Es gilt* $\mathrm{Z}(\mathrm{GL}(n,q)) = \mathbb{F}_q^\times 1_n$ *und* $\mathrm{Z}(\mathrm{SL}(n,q)) = \mathrm{Z}(\mathrm{GL}(n,q)) \cap \mathrm{SL}(n,q)$.

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

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

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

Definition 10.3. Man nennt

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

die *projektive* (*spezielle*) *lineare Gruppe* vom Grad n über $\mathbb{F}_q$.

Satz 10.4.

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

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

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

und die erste Behauptung folgt aus Lemma 10.2.

Für die zweite Behauptung beobachten wir, dass der Homomorphismus $\det\colon \mathrm{GL}(n,q) \to \mathbb{F}_q^\times$ surjektiv ist. Daher ist $|\mathrm{SL}(n,q)| = \frac{|\mathrm{GL}(n,q)|}{q-1} = |\mathrm{PGL}(n,q)|$. Sei nun $\lambda 1_n \in \mathbb{F}_q^\times 1_n \cap \mathrm{SL}(n,q) = \mathrm{Z}(\mathrm{SL}(n,q))$. Dann

ist $1 = \det(\lambda 1_n) = \lambda^n$ und $|\langle\lambda\rangle| \mid \mathrm{ggT}(n, q-1)$. Da $\mathbb{F}_q^\times$ zyklisch ist (Algebra oder Satz 9.8), gibt es genau eine Untergruppe $L \leq \mathbb{F}_q^\times$ mit $|L| = \mathrm{ggT}(n, q-1)$ (Satz 2.4). Es gilt dann $\lambda \in L$. Umgekehrt erfüllt jedes Element $\gamma \in L$ die Bedingung $\gamma^n = 1$. Also ist $|\mathrm{Z}(\mathrm{SL}(n,q))| = |L| = \mathrm{ggT}(n, q-1)$. □

Beispiel 10.5.

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

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

Lemma 10.6 (Iwasawa)**.** *Sei $G \leq \mathrm{Sym}(\Omega)$ primitiv und perfekt. Existiert ein auflösbarer Normalteiler $A \trianglelefteq G_\omega$ $(\omega \in \Omega)$ mit $\langle gAg^{-1} : g \in G\rangle = G$, so ist G einfach.*

Beweis. Sei $1 \neq N \trianglelefteq G$. Nach Lemma 6.20 und Satz 1.24 ist $G = G_\omega N \leq \mathrm{N}_G(NA)$, d. h. $NA \trianglelefteq G$. Nach Voraussetzung ist $G = \langle gAg^{-1} : g \in G\rangle \leq NA$ und $G/N \cong A/A \cap N$ ist auflösbar. Im Fall $N < G$ erhält man den Widerspruch $G/N = G'/N = (G/N)' < G/N$. Also ist $N = G$ und G ist einfach. □

Lemma 10.7. *Für $n \geq 2$ operiert $\mathrm{PSL}(n,q)$ treu und primitiv auf der Menge Ω der 1-dimensionalen Untervektorräume von $\mathbb{F}_q^n$.*

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

Für die Primitivität genügt es nach Satz 6.35 zu zeigen, dass $\mathrm{PSL}(n,q)$ 2-transitiv auf Ω operiert. Seien also $\langle v_1\rangle \neq \langle v_2\rangle$ und $\langle w_1\rangle \neq \langle w_2\rangle$ in Ω. Man kann v_1, v_2 (bzw. w_1, w_2) zu einer Basis $v_1, \ldots, v_n$ (bzw. $w_1, \ldots, w_n$) von $\mathbb{F}_q^n$ fortsetzen. Dann existiert $A \in \mathrm{GL}(n,q)$ mit $Av_i = w_i$ für $i = 1, \ldots, n$. Sei $\lambda := \det(A)$ und $B \in \mathrm{GL}(n,q)$ mit $Bv_1 = \lambda^{-1} w_1$ und $Bv_i = w_i$ für $i = 2, \ldots, n$. Dann ist $B \in \mathrm{SL}(n,q)$ und das entsprechende Element $\overline{B} \in \mathrm{PSL}(n,q)$ bildet $(\langle v_1\rangle, \langle v_2\rangle)$ auf $(\langle w_1\rangle, \langle w_2\rangle)$ ab. □

Lemma 10.8. $\mathrm{SL}(n,q) = \langle 1_n + \lambda e_{ij} : \lambda \in \mathbb{F}_q,\ i \neq j\rangle$.

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

Lemma 10.9. *Für $n \geq 2$ und $(n,q) \notin \{(2,2), (2,3)\}$ ist $\mathrm{SL}(n,q)$ perfekt.*

Beweis. Nach Lemma 10.8 genügt es zu zeigen, dass die Matrizen $1_n + \lambda e_{ij}$ Kommutatoren sind. Es gilt $(1_n + \lambda e_{ij})(1_n - \lambda e_{ij}) = 1_n + \lambda e_{ij} - \lambda e_{ij} - \lambda^2 e_{ij}^2 = 1_n$ und $(1_n + \lambda e_{ij})^{-1} = 1_n - \lambda e_{ij}$. Sei zunächst $n \geq 3$, $\lambda \in \mathbb{F}_q$ und $i, j, k \in \{1, \ldots, n\}$ paarweise verschieden. Dann ist

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

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

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

Dann ist

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

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

Beispiel 10.10. Wegen $|\mathrm{SL}(2, 2)| = 6$ und $|\mathrm{SL}(2, 3)| = 24$ sind $\mathrm{SL}(2, 2)$ und $\mathrm{SL}(2, 3)$ nicht perfekt.

Satz 10.11 (Jordan-Moore-Dickson)**.** *Für $n \geq 2$ und $(n, q) \notin \{(2, 2), (2, 3)\}$ ist $\mathrm{PSL}(n, q)$ einfach.*

Beweis. Wir benutzen Iwasawas Lemma. Sei $G := \mathrm{SL}(n, q)$, $Z := \mathrm{Z}(G)$ und $\overline{H} := HZ/Z$ für $H \leq G$. Nach Lemma 10.7 ist $\overline{G}$ eine primitive Permutationsgruppe. Nach Lemma 10.9 ist $\overline{G}' = \overline{G'} = \overline{G}$, d. h. $\overline{G}$ ist perfekt. Sei $e_i := (\delta_{ij})_{j=1}^n \in \mathbb{F}_q^n$ und sei $H \leq G$ der Stabilisator von $U := \langle e_1 \rangle$. Sei

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

Wegen

$$\left(1_n + \sum_{i=2}^n \lambda_i e_{1i}\right)\left(1_n + \sum_{i=2}^n \mu_i e_{1i}\right) = 1_n + \sum_{i=2}^n (\lambda_i + \mu_i) e_{1i} \in A$$

ist A eine abelsche Untergruppe von H. Für $h \in H$ und $v, w \in \mathbb{F}_q^n$ mit $v + U = w + U$ gilt $h(v - w) \in hU = U$ und daher $hv + U = hw + U$. Also operiert H auf $\mathbb{F}_q^n/U$. Sei $h = (h_{ij}) \in H$ im Kern dieser Operation. Dann gilt $he_i \in e_i + U$ für $i = 2, \ldots, n$. Dies zeigt $h_{ij} = \delta_{ij}$ für $i \geq 2$. Wegen $\det h = 1$ gilt auch $h_{11} = 1$ und somit $h \in A$. Umgekehrt operiert jedes Element aus A trivial auf $\mathbb{F}_q^n/U$. Also ist A der Kern und daher $A \trianglelefteq H$. Sicher ist dann auch $\overline{A}$ ein abelscher Normalteiler von $\overline{H}$. Es verbleibt zu zeigen, dass $\overline{G} = \langle \overline{gAg^{-1}} : g \in G \rangle$ gilt. Nach Lemma 10.8 genügt es, $1_n + \lambda e_{ij} \in \bigcup_{g \in G} gAg^{-1}$ zu zeigen ($\lambda \in \mathbb{F}_q$, $i \neq j$). Nach Definition gilt bereits $1_n + \lambda e_{1j} \in A$. Für $j \neq i \geq 2$ sei $g_i \in G$ mit

$$g_i e_k := \begin{cases} e_i & \text{falls } k = 1, \\ -e_1 & \text{falls } k = i, \\ e_k & \text{sonst.} \end{cases}$$

Dann gilt $(g_i e_{1j} g_i^{-1})e_j = e_i$ und $(g_i e_{1j} g_i^{-1})e_k = 0$ für $k \neq j$. Dies zeigt $g_i(1_n + \lambda e_{1j})g_i^{-1} = 1_n + \lambda g_i e_{1j} g_i^{-1} = 1_n + \lambda e_{ij}$. Die Behauptung folgt. □

Bemerkung 10.12.

(i) Nach Satz 10.4 ist $|\mathrm{PSL}(2,4)| = |\mathrm{PSL}(2,5)| = 60$. Aus Satz 6.40 folgt daher $\mathrm{PSL}(2,4) \cong \mathrm{PSL}(2,5) \cong A_5$. Man kann weiter $\mathrm{PSL}(2,7) \cong \mathrm{PSL}(3,2) \cong \mathrm{GL}(3,2)$, $\mathrm{PSL}(2,9) \cong A_6$ und $\mathrm{PSL}(4,2) \cong \mathrm{GL}(4,2) \cong A_8$ zeigen.

(ii) Die kleinste einfache Gruppe, die nicht zu C_p, A_n oder $\mathrm{PSL}(n,q)$ isomorph ist, ist die *spezielle unitäre* Gruppe $\mathrm{SU}(3,3)$ der Ordnung 6048. Für $A = (a_{ij}) \in \mathrm{GL}(n,q^2)$ definiert man $\overline{A} := (a_{ij}^q)$ (Frobenius-Automorphismus) und

$$\begin{aligned} \mathrm{GU}(n,q) &:= \{A \in \mathrm{GL}(n,q^2) : \overline{A}A^{\mathrm{t}} = 1_n\}, \\ \mathrm{SU}(n,q) &:= \{A \in \mathrm{GU}(n,q) : \det(A) = 1\}, \\ \mathrm{PSU}(n,q) &:= \mathrm{SU}(n,q)/\mathrm{Z}(\mathrm{SU}(n,q)). \end{aligned}$$

Es gilt $\mathrm{PSU}(2,q) \cong \mathrm{PSL}(2,q)$. Für $n \geq 3$ und $(n,q) \neq (3,2)$ ist $\mathrm{PSU}(n,q)$ einfach.[20]

(iii) Sei $G := \mathrm{GL}(n,q)$ mit $n \geq 2$ und $(n,q) \notin \{(2,2),(2,3)\}$. Da $\mathrm{SL}(n,q)$ quasieinfach ist, gilt $\mathrm{SL}(n,q) \leq \mathrm{E}(G)$. Wegen $\mathrm{C}_G(\mathrm{SL}(n,q)) \leq \mathrm{Z}(G)$ (Beweis von Lemma 10.2) kann es nach Satz 9.39 keine weiteren Komponenten geben, d. h. $\mathrm{E}(G) = \mathrm{SL}(n,q)$. Aus Satz 9.39 folgt auch $\mathrm{Z}(G) \leq \mathrm{F}(G) \leq \mathrm{C}_G(\mathrm{E}(G)) \leq \mathrm{Z}(G)$, also $\mathrm{F}(G) = \mathrm{Z}(G) = \mathbb{F}_q^\times 1_n$ und $\mathrm{F}^*(G) = \mathbb{F}_q^\times \mathrm{SL}(n,q)$. Dabei gilt

$$|G : \mathrm{F}^*(G)| = \frac{|G||\mathrm{Z}(\mathrm{E}(G))|}{|\mathrm{E}(G)||\mathrm{Z}(G)|} = |\mathrm{Z}(\mathrm{E}(G))| = \mathrm{ggT}(n, q-1).$$

Satz 10.13. *Sei P eine p-Sylowgruppe von $\mathrm{SL}(2,q)$. Dann gilt:*

(i) Für $p \mid q$ ist P elementarabelsch der Ordnung q.

(ii) Für $p = 2 \nmid q$ ist P eine (verallgemeinerte) Quaternionengruppe.

(iii) Für $2 < p \nmid q$ ist P zyklisch.

Beweis. Sei $G := \mathrm{SL}(2,q)$. Bekanntlich ist $|G| = (q+1)q(q-1)$. Für $p \mid q$ ist $P = \{1_2 + \lambda e_{12} : \lambda \in \mathbb{F}_q\}$ offenbar eine elementarabelsche p-Sylowgruppe von G. Sei nun $p = 2 \nmid q$ und sei $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in P$ eine Involution. Dann ist $A = A^{-1} = \left(\begin{smallmatrix} d & -b \\ -c & a \end{smallmatrix}\right)$ (beachte $\det(A) = 1$) und es folgt $A = -1_2$ (beachte $1 \neq -1$ in $\mathbb{F}_q$). Also besitzt P nur eine Involution. Nach Satz 9.6 ist P zyklisch oder eine Quaternionengruppe. Im ersten Fall ist G 2-nilpotent nach Satz 7.22. Aus Lemma 10.9 folgt $q = 3$. Die Operation auf den vier 1-dimensionalen Unterräumen liefert einen Homomorphismus $G \to S_4$ mit Bild A_4. Da A_4 nicht 2-nilpotent ist, ist dies ausgeschlossen. Also ist P eine Quaternionengruppe.

Sei schließlich $2 < p \nmid q$. Wegen $\mathrm{ggT}(q+1, q-1) \leq 2$ ist $|P|$ ein Teiler von $q+1$ oder ein Teiler von $q-1$. Sei $\mathbb{F}_q^\times = \langle\zeta\rangle$ (Algebra oder Satz 9.8). Dann erzeugt $\left(\begin{smallmatrix} \zeta & 0 \\ 0 & \zeta^{-1} \end{smallmatrix}\right)$ eine zyklische Untergruppe der Ordnung $q-1$ in G. Ist $|P|$ ein Teiler von $q-1$, so ist P also zyklisch. In Beispiel 6.23 haben wir eine zyklische Gruppe $S \leq \mathrm{GL}(2,q)$ der Ordnung q^2-1 konstruiert (Singer-Zyklus). Wegen

$$S/S \cap \mathrm{SL}(2,q) \cong S\mathrm{SL}(2,q)/\mathrm{SL}(2,q) \leq \mathrm{GL}(2,q)/\mathrm{SL}(2,q) \cong C_{q-1}$$

ist $|S \cap \mathrm{SL}(2,q)|$ durch $q+1$ teilbar. Somit ist P auch im Fall $|P| \mid q+1$ zyklisch. □

[20] Siehe Skript zur kombinatorischen Gruppentheorie

Bemerkung 10.14. Wegen $\mathrm{PSL}(2,q) = \mathrm{SL}(2,q)/\langle \pm 1_2 \rangle$ erhält man aus Satz 10.13 auch die p-Sylowgruppen von $\mathrm{PSL}(2,q)$. Ist q ungerade, so ist eine 2-Sylowgruppe von $\mathrm{PSL}(2,q)$ eine Diedergruppe, denn $Q_{2^n}/\mathrm{Z}(Q_{2^n}) \cong D_{2^{n-1}}$, wobei $D_4 := C_2^2$. Gorenstein und Walter haben umgekehrt gezeigt, dass A_7 und $\mathrm{PSL}(2,q)$ mit q ungerade die einzigen einfachen Gruppen mit einer Diedergruppe (oder C_2^2) als 2-Sylowgruppe sind (beachte $A_6 \cong \mathrm{PSL}(2,9)$). Brauer und Suzuki haben gezeigt, dass keine einfache Gruppe eine Quaternionengruppe als Sylowgruppe besitzt.

11 Schur-Erweiterungen

Bemerkung 11.1. Nach Satz 9.43 wird die Struktur von G durch $\mathrm{F}^*(G)$ beeinflusst. Die Struktur der nilpotenten Gruppe $\mathrm{F}(G)$ folgt aus Satz 4.10, während $\mathrm{E}(G)$ ein Zentralprodukt von quasieinfachen Komponenten K ist. Nach der Klassifikation der einfachen Gruppen kennt man die Möglichkeiten für $K/\mathrm{Z}(K)$. Wir werden sehen, wie man daraus die Möglichkeiten von K ableiten kann.

Beispiel 11.2. Sei G eine Gruppe mit 2-Sylowgruppe $P = \langle x, y \rangle \cong D_{2^n}$. Nehmen wir zunächst $Z := \mathrm{Z}(G) \cap P \neq 1$ an. Wegen $|\mathrm{Z}(P)| = 2$ ist dann $Z = \mathrm{Z}(P)$. Wir zeigen $\mathrm{Foc}_G(P) \leq \langle x \rangle$. Seien dafür $g \in G$, $h, ghg^{-1} \in P$. Im Fall $h^2 \neq 1$ gilt $h, ghg^{-1} \in \langle x \rangle$, denn $P \setminus \langle x \rangle$ besteht aus Involutionen. Dann ist also $[g,h] \in \langle x \rangle$. Nehmen wir nun $h^2 = 1$ an. Im Fall $h \in \langle x \rangle$ gilt $h \in Z$ und $ghg^{-1} \in Z$ folgt aus $Z \trianglelefteq G$. Wieder ist $[g,h] \in \langle x \rangle$. Im letzten Fall $h, ghg^{-1} \in P \setminus \langle x \rangle$ gilt ebenfalls $[g,h] \in \langle x \rangle$. Also ist $\mathrm{Foc}_G(P) \leq \langle x \rangle$. Nach Higman hat G' die zyklische 2-Sylowgruppe $\mathrm{Foc}_G(P) = P \cap G'$. Nach Satz 7.22 ist G' 2-nilpotent. Nach Feit-Thompson sind G' und G auflösbar.

Sei nun $Z = 1$ und $\mathrm{E}(G) = K_1 * \ldots * K_n$ mit Komponenten $K_1, \ldots, K_n$. Sei $P_i \in \mathrm{Syl}_2(K_i)$. Nach Sylow ist P_i zu einer Untergruppe von P isomorph. Nach Feit-Thompson und Satz 7.22 kann P_i nicht zyklisch sein. Also hat $P_i \cap \langle x \rangle$ Index 2 in P_i. Es folgt leicht, dass P_i selbst eine Diedergruppe ist oder $P_i \cong C_2^2$. Wie oben ist nun $|\mathrm{Z}(K_i)|$ ungerade. Nach Satz 9.17 ist $P_1 \times \ldots \times P_n \in \mathrm{Syl}_2(\mathrm{E}(G))$ zu einer Untergruppe von P isomorph. Andererseits lässt sich jede Untergruppe $Q \leq P$ mit zwei Elementen erzeugen, denn $|Q : Q \cap \langle x \rangle| = |\langle x \rangle Q : \langle x \rangle| \leq 2$. Dies zeigt $n = 1$ und $\mathrm{E}(G) = K$ ist quasieinfach. Wegen $P_1 \cong P_1\mathrm{Z}(K)/\mathrm{Z}(K) \in \mathrm{Syl}_2(K/\mathrm{Z}(K))$ ist $K/\mathrm{Z}(K) \cong A_7$ oder $K/\mathrm{Z}(K) \cong \mathrm{PSL}(2,q)$ (Bemerkung 10.14). Wir werden zeigen, dass $\mathrm{Z}(K) = 1$ oder $K/\mathrm{Z}(K) \in \{A_6, A_7\}$ und $\mathrm{Z}(K) \cong C_3$ gilt (Beispiel 11.38).

Definition 11.3. Eine *Schur-Erweiterung* einer endlichen Gruppe G ist eine Gruppe $\widehat{G}$, sodass ein $Z \leq \mathrm{Z}(\widehat{G}) \cap \widehat{G}'$ mit $\widehat{G}/Z \cong G$ existiert.

Beispiel 11.4.

(i) Jede extraspezielle Gruppe ist eine Schur-Erweiterung einer elementarabelschen Gruppe. Insbesondere sind D_8 und Q_8 Schur-Erweiterungen von C_2^2.

(ii) Jede quasieinfache Gruppe G ist eine Schur-Erweiterung der einfachen Gruppe $G/\mathrm{Z}(G)$. Insbesondere ist $\mathrm{SL}(2,5)$ eine Schur-Erweiterung von A_5 (Bemerkung 10.12).

(iii) Sei $\widehat{G}$ eine Schur-Erweiterung einer zyklischen Gruppe $G \cong \widehat{G}/Z$. Nach Aufgabe 8(a) ist $\widehat{G}$ abelsch, denn $\widehat{G}/\mathrm{Z}(\widehat{G}) \cong (\widehat{G}/Z)/(\mathrm{Z}(\widehat{G})/Z)$ ist zyklisch. Dies zeigt $Z \leq \widehat{G}' = 1$ und $\widehat{G} \cong G$.

(iv) Satz 7.15 zeigt, dass die p-Sylowgruppen einer Schur-Erweiterung $\widehat{G}$ nichtabelsch sind, falls p ein Teiler von $|Z|$ ist (wobei $Z \leq \widehat{G}' \cap \mathrm{Z}(\widehat{G})$).

Satz 11.5. *Hat $\mathrm{Z}(G)$ endlichen Index in G, so ist G' endlich. Insbesondere ist jede Schur-Erweiterung einer endlichen Gruppe endlich.*

Beweis. Sei $Z := \mathrm{Z}(G)$ und $n := |G : Z| < \infty$. Sei R ein Repräsentantensystem für G/Z. Für $\Gamma := \big\{[r,s] : r,s \in R\big\}$ gilt $|\Gamma| \le |R|^2 = |G/Z|^2 = n^2$. Für $r,s \in R$ und $z \in Z$ gilt $[rz,s] = [r,s] = [r,sz]$. Jedes Element $g \in G'$ hat also die Form $g = c_1 \dots c_m$ mit $c_1, \dots, c_m \in \Gamma$. Es genügt zu zeigen, dass man dabei $m < n^3$ wählen kann (dann folgt $|G'| < n^{2n^3} < \infty$). Nehmen wir $m \ge n^3$ an. Dann existiert ein $\gamma \in \Gamma$ mit $|\{i \in \{1,\dots,m\} : c_i = \gamma\}| \ge n$. Wegen $c_i c_{i+1} = c_{i+1}(c_{i+1}^{-1} c_i c_{i+1}) = c_{i+1}\delta$ mit $\delta \in \Gamma$ können wir $c_1 = \dots = c_n = \gamma$ annehmen. Nach Beispiel 7.9 ist die Verlagerung $V\colon G \to Z$, $g \mapsto g^n$ ein Homomorphismus (für die Definition der Verlagerung $V_{H/K}$ benötigt man nur $|G : H| < \infty$). Da Z abelsch ist, gilt $G' \subseteq \mathrm{Ker}(V)$. Also ist $c_1 \dots c_n = \gamma^n = 1$ und man kann m reduzieren.

Für die zweite Behauptung sei $\widehat{G}$ eine Schur-Erweiterung der endlichen Gruppe G mit $\widehat{G}/Z \cong G$. Dann ist $|\widehat{G} : \mathrm{Z}(\widehat{G})| \le |\widehat{G} : Z| = |G| < \infty$ und daher $|\widehat{G}| = |G||Z| \le |G||\widehat{G}'| < \infty$. □

Definition 11.6. Sei G eine endliche Gruppe und A eine (möglicherweise unendliche) abelsche Gruppe. Die Menge $C^1(G,A)$ aller Abbildungen der Form $G \to A$ wird durch $(\alpha\beta)(g) := \alpha(g)\beta(g)$ für $\alpha, \beta \in C^1(G,A)$ und $g \in G$ zu einer abelschen Gruppe (es gilt $C^1(G,A) \cong A^{|G|}$). Sei $C^2(G,A) := C^1(G \times G, A)$ und

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

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

Lemma 11.7. *Die Abbildung $\partial\colon C^1(G,A) \to Z^2(G,A)$ mit $\partial\alpha(x,y) := \alpha(x)\alpha(y)\alpha(xy)^{-1}$ für $\alpha \in C^1(G,A)$ und $x,y \in G$ ist ein Homomorphismus.*

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

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

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

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

Also ist ∂ ein Homomorphismus. □

Definition 11.8. Sei $B^2(G,A) := \partial(C^1(G,A)) \trianglelefteq Z^2(G,A)$ und $H^2(G,A) := Z^2(G,A)/B^2(G,A)$. Man nennt $H^2(G,A)$ die *zweite Kohomologiegruppe* von G nach A.

Lemma 11.9. *Für $\overline{\alpha} \in H^2(G,A)$ existiert ein $\alpha \in Z^2(G,A)$ mit $\alpha B^2(G,A) = \overline{\alpha}$ und $\alpha(1,x) = \alpha(x,1) = 1$ für $x \in G$.*

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

Definition 11.10. Man nennt $M(G) := H^2(G, \mathbb{C}^\times)$ den *Schur-Multiplikator* von G.

Satz 11.11. *Der Schur-Multiplikator $M(G)$ ist eine endliche abelsche Gruppe mit* $\exp(M(G)) \,\big|\, |G|$.

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

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

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

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

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

Bemerkung 11.12. Es gilt sogar $\exp(G)\exp(M(G)) \mid |G|$ (Aufgabe 77) und $\exp(M(G))^2 \mid |G|$ (ohne Beweis). Die von Schur formulierte Vermutung $\exp(M(G)) \mid \exp(G)$ wurde jedoch 1974 widerlegt.

Lemma 11.13. *Für $\alpha \in Z^2(G, A)$ ist die Abbildung $\Psi_\alpha \colon \mathrm{Hom}(A, \mathbb{C}^\times) \to M(G)$, $\lambda \mapsto (\lambda \circ \alpha)B^2(G, \mathbb{C}^\times)$ ein Homomorphismus.*

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

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

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

Lemma 11.14. *Für eine endliche abelsche Gruppe A ist* $\mathrm{Hom}(A, \mathbb{C}^\times) \cong A$.

Beweis. Sei $A = \langle a_1\rangle \oplus \ldots \oplus \langle a_n\rangle$ und $d_i := |\langle a_i\rangle|$ für $i = 1, \ldots, n$. Sei $\zeta_i \in \mathbb{C}$ eine primitive d_i-te Einheitswurzel. Für jedes $\lambda \in \mathrm{Hom}(A, \mathbb{C}^\times)$ gilt dann $\lambda(a_i) \in \langle\zeta_i\rangle$ (Beispiel 1.6(v)). Umgekehrt definiert jede Wahl $\lambda(a_i) = \zeta_i^{k_i}$ einen Homomorphismus. Dies zeigt $|\mathrm{Hom}(A, \mathbb{C}^\times)| = d_1 \ldots d_n = |A|$. Wir definieren $F \colon A \to \mathrm{Hom}(A, \mathbb{C}^\times)$ mit $F(a_1^{k_1} \ldots a_n^{k_n})(a_i) := \zeta_i^{k_i}$ für $i = 1, \ldots, n$. Man zeigt leicht, dass F ein wohldefinierter Isomorphismus ist. □

Satz 11.15 (Schur)**.** *Sei $\widehat{G}$ eine Schur-Erweiterung von G mit $\widehat{G}/Z \cong G$. Dann ist Z zu einer Untergruppe von $M(G)$ isomorph. Insbesondere ist $|\widehat{G}| \le |G||M(G)|$ und G besitzt nur endlich viele Schur-Erweiterungen bis auf Isomorphie.*

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

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

Dies zeigt $\alpha \in Z^2(G, Z)$. Nach Satz 11.5 und Lemma 11.14 genügt es zu zeigen, dass die Abbildung Ψ_α aus Lemma 11.13 injektiv ist. Sei also $\lambda \in \mathrm{Hom}(Z, \mathbb{C}^\times)$ mit $\lambda \circ \alpha = \partial\gamma$ für ein $\gamma \in C^1(G, \mathbb{C}^\times)$. Dann ist $1 = \lambda(1) = \lambda(\alpha(1,1)) = \partial\gamma(1,1) = \gamma(1)$. Sei $\widehat{\lambda} \colon \widehat{G} \to \mathbb{C}^\times$ mit $\widehat{\lambda}(\widehat{x}a) := \gamma(x)\lambda(a)$ für $x \in G$ und $a \in Z$. Wegen $\gamma(1) = 1$ ist $\widehat{\lambda}$ eine Fortsetzung von λ. Für $x, y \in G$ und $a, b \in Z$ gilt

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

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

Definition 11.16. Eine Schur-Erweiterung $\widehat{G}$ von G heißt *maximal*, falls $|\widehat{G}| = |G||M(G)|$.

Satz 11.17 (SCHUR)**.** *Jede endliche Gruppe G besitzt eine maximale Schur-Erweiterung.*

Beweis. Nach Satz 11.11 ist $M(G) = \langle\overline{\alpha}_1\rangle \oplus \ldots \oplus \langle\overline{\alpha_n}\rangle$. Sei $d_i := |\langle\overline{\alpha_i}\rangle|$ und $A_i \leq \mathbb{C}^\times$ mit $|A_i| = d_i$ für $i = 1, \ldots, n$. Sei $\alpha_i \in Z^2(G, \mathbb{C}^\times)$ mit $\alpha_i B^2(G, \mathbb{C}^\times) = \overline{\alpha_i}$. Dann ist $\alpha_i^{d_i} = \partial\gamma_i$ für ein $\gamma_i \in C^1(G, \mathbb{C}^\times)$. Sei $\delta_i(x) \in \mathbb{C}^\times$ mit $\delta_i(x)^{d_i} = \gamma_i(x)^{-1}$ für $x \in G$. Nachdem wir α_i durch $\alpha_i\partial\delta_i$ ersetzt haben, gilt $\alpha_i^{d_i} = 1$ für $i = 1, \ldots, n$. Insbesondere ist $\alpha_i \in Z^2(G, A_i)$ für $i = 1, \ldots, n$. Nach Lemma 11.9 dürfen wir auch $\alpha_i(x, 1) = \alpha_i(1, x) = 1$ für $x \in G$ annehmen. Sei $A := A_1 \times \ldots \times A_n \cong M(G)$ und $\alpha \in C^2(G, A)$ mit $\alpha(x, y) = (\alpha_1(x, y), \ldots, \alpha_n(x, y))$ für $x, y \in G$. Offenbar ist dann $\alpha \in Z^2(G, A)$ mit $\alpha(1, x) = \alpha(x, 1) = 1$ für $x \in G$.

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

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

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

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

Die Verknüpfung ist also assoziativ. Wegen $(1_G, 1_A) \cdot (x, a) = (x, \alpha(1, x)a) = (x, a)$ ist $(1_G, 1_A)$ ein neutrales Element. Schließlich ist $(x^{-1}, \alpha(x^{-1}, x)^{-1}a^{-1}) \cdot (x, a) = (1_G, 1_A)$. Also ist $\widehat{G}$ eine endliche Gruppe.

Wir identifizieren $g \in G$ mit $(g, 1_A) \in \widehat{G}$ und $a \in A$ mit $(1_G, a) \in \widehat{G}$. Offenbar ist dann A der Kern des Epimorphismus $\widehat{G} \to G$, $(x, a) \mapsto x$. Dies zeigt $A \trianglelefteq \widehat{G}$ und $\widehat{G}/A \cong G$. Für $(x, a) \in \widehat{G}$ und $b \in A$ gilt $(x, a) \cdot b = (x, ab) = (x, ba) = b \cdot (x, a)$. Es folgt $A \leq \mathrm{Z}(\widehat{G})$. Es verbleibt $A \leq \widehat{G}'$ zu zeigen.

Sei $\pi_i \colon A \to A_i \leq \mathbb{C}^\times$ die i-te Projektion. Mit der Abbildung Ψ_α aus Lemma 11.13 gilt dann $\Psi_\alpha(\pi_i) = (\pi_i \circ \alpha)B^2(G, \mathbb{C}^\times) = \overline{\alpha_i}$ für $i = 1, \ldots, n$. Wegen $M(G) = \langle\overline{\alpha_1}, \ldots, \overline{\alpha_n}\rangle$ ist Ψ_α surjektiv. Nach Lemma 11.14 ist $\mathrm{Hom}(A, \mathbb{C}^\times) \cong A \cong M(G)$. Daher ist Ψ_α auch injektiv. Nach Satz 2.11 (angewendet auf $\widehat{G}/\widehat{G}'$) existieren Normalteiler $N_1, \ldots, N_s \trianglelefteq \widehat{G}$ mit $\widehat{G}' = N_1 \cap \ldots \cap N_s$, sodass $\widehat{G}/N_i$ zyklisch ist für $i = 1, \ldots, s$. Nehmen wir $A \not\subseteq \widehat{G}'$ an. Dann existiert ein i mit $A \not\subseteq N_i$. Indem man $\widehat{G}/N_i$ in $\mathbb{C}^\times$ einbettet, erhält man einen Homomorphismus $\varphi \colon \widehat{G} \to \mathbb{C}^\times$ mit $\varphi(A) \neq 1$. Die Einschränkung φ_A ist also ein nicht-triviales Element in $\mathrm{Hom}(A, \mathbb{C}^\times)$. Für $x, y \in G$ gilt

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

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

Satz 11.18. *Für $H \leq G$ existiert ein Homomorphismus $F \colon M(G) \to M(H)$ mit $\overline{\alpha}^{|G:H|} = 1$ für $\overline{\alpha} \in \mathrm{Ker}(F)$.*

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

Repräsentantensystem für G/H. Für $x \in G$ sei $r_x \in R$ und $h_x \in H$ mit $x = r_x h_x$. Sei $\gamma(x) := \alpha(r_x, h_x)$ für $x \in G$ und $\beta := \alpha\partial\gamma$. Für $x \in G$ und $h \in H$ gilt dann

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

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

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

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

Folgerung 11.19. *Sind $H_1, \ldots, H_n \leq G$ mit teilerfremden Indizes $|G : H_i|$, so ist $M(G)$ zu einer Untergruppe von $M(H_1) \times \ldots \times M(H_n)$ isomorph. Insbesondere ist $M(G) = 1$, falls alle Sylowgruppen von G zyklisch sind.*

Beweis. Sei $\Gamma_i \colon M(G) \to M(H_i)$ der Homomorphismus aus Satz 11.18. Dann ist

$$\Gamma \colon M(G) \to M(H_1) \times \ldots \times M(H_n), \qquad \overline{\alpha} \mapsto (\Gamma_1(\overline{\alpha}), \ldots, \Gamma_n(\overline{\alpha}))$$

ein Homomorphismus mit $\operatorname{Ker}(\Gamma) = \bigcap_{i=1}^n \operatorname{Ker}(\Gamma_i)$. Sei $\overline{\alpha} \in \operatorname{Ker}(\Gamma)$. Nach Satz 11.18 gilt $\alpha^{|G:H_i|} = 1$ für $i = 1, \ldots, n$. Da die Indizes $|G : H_i|$ teilerfremd sind, folgt $\overline{\alpha} = 1$. Also ist Γ ein Monomorphismus. Für die zweite Behauptung wählt man für $H_1, \ldots, H_n$ die Sylowgruppen von G (es reicht je eine für jeden Primteiler von $|G|$). Nach Beispiel 11.4(iii) ist dann $M(H_1) = \ldots = M(H_n) = 1$ und die Behauptung folgt. □

Bemerkung 11.20. Das nächste Lemma quantifiziert Satz 11.5 für p-Gruppen.

Lemma 11.21. *Sei H eine beliebige Gruppe und $|H : \mathrm{Z}(H)| = p^n$ eine Primzahlpotenz. Dann gilt $|H'| \leq p^{\binom{n}{2}}$.*

Beweis. Induktion nach n. Für $n = 1$ ist $H' = 1$ nach Aufgabe 8. Sei nun $n \geq 2$. Mit $H/\mathrm{Z}(H)$ ist auch H nilpotent. Daher existiert $x \in \mathrm{Z}_2(H) \setminus \mathrm{Z}(H)$. Für $a, b \in H$ gilt $[x,b] \in \mathrm{Z}(H)$ und $[x, ab] = [x,a] \cdot {}^a[x,b] = [x,a][x,b]$. Somit ist $H \to H$, $a \mapsto [x,a]$ ein Homomorphismus mit Bild

$$N := [x,H] = \big\{[x,a] : a \in H\big\} \leq H' \cap \mathrm{Z}(H).$$

Wegen $\mathrm{Z}(H)/N < \mathrm{Z}(H)\langle x\rangle/N \leq \mathrm{Z}(H/N)$ ist $|H/N : \mathrm{Z}(H/N)| \leq p^{n-1}$. Induktion ergibt $|H'/N| = |(H/N)'| \leq p^{\binom{n-1}{2}}$. Aus

$$[x,a] = [x,b] \iff {}^ax = {}^bx \iff a\mathrm{C}_H(x) = b\mathrm{C}_H(x)$$

folgt $|N| = |H : \mathrm{C}_H(x)| \leq |H : \mathrm{Z}(H)\langle x\rangle| \leq p^{n-1}$. Insgesamt gilt nun

$$|H'| = |H'/N||N| \leq p^{\binom{n-1}{2}+n-1} = p^{\binom{n}{2}}.$$ □

Satz 11.22 (Green). *Ist $|G| = p_1^{a_1} \ldots p_s^{a_s}$ die Primfaktorzerlegung von $|G|$, so gilt*

$$|M(G)| \leq p_1^{\binom{a_1}{2}} \ldots p_s^{\binom{a_s}{2}}.$$

Beweis. Nach Folgerung 11.19 kann man annehmen, dass G eine p-Gruppe ist. Sei $\widehat{G}$ eine maximale Schur-Erweiterung von G mit $|\widehat{G}/\mathrm{Z}(\widehat{G})| \leq |\widehat{G}/Z| = |G| = p^a$. Nach Lemma 11.21 gilt $|M(G)| = |Z| \leq |\widehat{G}'| \leq p^{\binom{a}{2}}$. □

Satz 11.23. *Sei F eine freie Gruppe, $N \trianglelefteq F$ und $G \cong F/N$ (Satz 8.7). Dann gilt*

(i) *$N/[F,N]$ ist eine endlich erzeugte abelsche Gruppe mit Torsionsteil $(F' \cap N)/[F,N]$.*

(ii) *Für $N/[F,N] = (F' \cap N)/[F,N] \oplus K/[F,N]$ ist F/K eine maximale Schur-Erweiterung von G.*

(iii) *Für jede Schur-Erweiterung $\widehat{G}$ von G existiert ein $L \trianglelefteq F$ mit $N = (F' \cap N)L$ und $\widehat{G} \cong F/L$. Insbesondere ist $\widehat{G}$ eine Faktorgruppe einer maximalen Schur-Erweiterung.*

(iv) $\boxed{M(G) \cong (F' \cap N)/[F,N]}$ (Hopf-Formel).

Beweis.

(i) Da G endlich ist, können wir annehmen, dass F endlich erzeugt ist. Nach Satz 1.10 ist auch N endlich erzeugt. Mit $N \trianglelefteq F$ ist $[F,N] \trianglelefteq F$ und $[F,N] \leq F' \cap N$. Wegen $N/[F,N] \leq \mathrm{Z}(F/[F,N])$ hat $\mathrm{Z}(F/[F,N])$ endlichen Index in $F/[F,N]$. Nach Satz 11.5 ist $F'/[F,N]$ endlich. Daher ist auch $(F' \cap N)/[F,N]$ endlich. Wegen $N' \leq [F,N]$ ist $N/[F,N]$ abelsch. Weiter ist

$$(N/[F,N])/\big((F' \cap N)/[F,N]\big) \cong N/(F' \cap N) \cong F'N/F' \leq F/F'.$$

Nach Beispiel 8.11 ist F/F' eine freie abelsche Gruppe mit endlichem Rang. Mit F/F' muss auch $F'N/F'$ torsionsfrei sein. Daher ist $(F' \cap N)/[F,N]$ der Torsionsteil von $N/[F,N]$.

(ii) Wegen $K/[F,N] \leq N/[F,N] \leq \mathrm{Z}(F/[F,N])$ ist $K \trianglelefteq F$. Sei $\widehat{G} := F/K$ und $Z := N/K$. Dann gilt $\widehat{G}/Z \cong F/N \cong G$ und $Z \leq \mathrm{Z}(\widehat{G})$ wegen $[F,N] \leq K$. Aus $N/[F,N] \leq F'K/[F,N]$ folgt

$$Z = N/K \leq F'K/K = (F/K)' = \widehat{G}'.$$

Also ist $\widehat{G}$ eine Schur-Erweiterung mit $Z \cong (F' \cap N)/[F,N]$. Aus Satz 11.15 folgt $|M(G)| \geq |(F' \cap N)/[F,N]|$. Für die umgekehrte Ungleichung zeigen wir erst (iii).

(iii) Seien $\alpha\colon F \to G$ und $\beta\colon \widehat{G} \to G$ die kanonischen Epimorphismen mit $N = \mathrm{Ker}(\alpha)$ und $Z := \mathrm{Ker}(\beta)$. Da F frei ist, existiert ein Homomorphismus $\rho\colon F \to \widehat{G}$ mit $\beta\rho = \alpha$. Es gilt dann $\widehat{G} = \rho(F)Z$ und $Z \leq \widehat{G}' \leq \rho(F)' \leq \rho(F)$, also $\rho(F) = \widehat{G}$. Offenbar ist $L := \mathrm{Ker}(\rho) \leq \mathrm{Ker}(\alpha) = N$. Wegen $\beta\rho(N) = \alpha(N) = 1$ ist $\rho(N) \leq \mathrm{Ker}(\beta) = Z$. Dies zeigt $\rho([F,N]) \leq [\widehat{G}, Z] = 1$ und $[F,N] \leq L$. Aus $\rho(N) = Z \leq \widehat{G}' = \rho(F')$ folgt außerdem $N \leq F'L$ und $(F' \cap N)L = F'L \cap N = N$ nach Dedekind. Nun gilt

$$|Z| = \frac{|\widehat{G}|}{|G|} = |N : L| = |(F' \cap N)L : L| = |F' \cap N : F' \cap L| \leq |(F' \cap N)/[F,N]|.$$

Daher ist die in (ii) konstruierte Schur-Erweiterung tatsächlich maximal.

Nach (i) und dem Hauptsatz über endlich erzeugte abelsche Gruppen gilt

$$L/[F,N] = (L \cap F')/[F,N] \oplus M/[F,N],$$

wobei $(L \cap F')/[F,N]$ der Torsionsteil ist. Wegen $|N : L| = |F' \cap N : F' \cap L|$ ist $M/[F,N]$ der torsionsfreie Teil von $N/[F,N]$. Nach (ii) ist F/M eine maximale Schur-Erweiterung und $\widehat{G} \cong F/L \cong (F/M)/(L/M)$.

(iv) Folgt aus dem Beweis von (ii). □

Satz 11.24 (Jones). *Für jede p-Gruppe P der Ordnung p^n gilt $|M(P)||P'| \leq p^{\binom{n}{2}}$.*

Beweis. Sei $P = F/N$ eine Präsentation, $H = F/[F,N]$ und $\mathrm{Z}(H) := Z/[F,N]$. Wegen $N/[F,N] \leq \mathrm{Z}(H)$ gilt $H/\mathrm{Z}(H) \cong F/Z \cong P/(Z/N)$. Insbesondere ist $H/\mathrm{Z}(H)$ eine p-Gruppe mit Ordnung $\leq p^n$. Aus Lemma 11.21 folgt $|F'/[F,N]| = |H'| \leq p^{\binom{n}{2}}$. Mit der Hopf-Formel erhält man $|M(P)||P'| = |(F' \cap N)/[F,N]||F'/(F' \cap N)| = |F'/[F,N]| \leq p^{\binom{n}{2}}$. □

Satz 11.25. *Seien $\widehat{G}_1$, $\widehat{G}_2$ maximale Schur-Erweiterungen von G mit $\widehat{G}_1/Z_1 \cong G \cong \widehat{G}_2/Z_2$. Dann gilt*

(i) (Schur) $\widehat{G}_1' \cong \widehat{G}_2'$ *und* $\widehat{G}_1/\widehat{G}_1' \cong G/G' \cong \widehat{G}_2/\widehat{G}_2'$.

(ii) (Gaschütz) $\widehat{G}_1/\mathrm{Z}(\widehat{G}_1) \cong \widehat{G}_2/\mathrm{Z}(\widehat{G}_2)$.

(iii) (Read) $\mathrm{Z}(\widehat{G}_1)/Z_1 \cong \mathrm{Z}(\widehat{G}_2)/Z_2$.

Beweis. Sei $G = F/N$, $K_i \trianglelefteq F$ und $\widehat{G}_i \cong F/K_i$ wie in Satz 11.23. Wir zeigen, dass die angegebenen Gruppen nicht von i abhängen.

(i) Es gilt

$$\begin{aligned} \widehat{G}_i' &\cong F'K_i/K_i \cong F'/(F' \cap K_i) = F'/(F' \cap N \cap K_i) = F'/[F,N], \\ \widehat{G}_i/\widehat{G}_i' &\cong (\widehat{G}_i/Z_i)/(\widehat{G}_i'/Z_i) \cong G/G'. \end{aligned}$$

(ii) Für $L/[F,N] := \mathrm{Z}(F/[F,N])$ gilt $[F,L] \leq [F,N] \leq K_i$ und $L/K_i \leq \mathrm{Z}(F/K_i)$. Sei umgekehrt $xK_i \in \mathrm{Z}(F/K_i)$. Dann ist $[x,F] \leq K_i \cap F' = K_i \cap F' \cap N = [F,N]$ und es folgt $x[F,N] \in \mathrm{Z}(F/[F,N]) = L/[F,N]$. Dies zeigt

$$\widehat{G}_i/\mathrm{Z}(\widehat{G}_i) \cong (F/K_i)/\mathrm{Z}(F/K_i) = (F/K_i)/(L/K_i) \cong F/L.$$

(iii) Mit den Bezeichnungen aus (ii) gilt

$$\mathrm{Z}(\widehat{G}_i)/Z_i \cong (L/K_i)/(N/K_i) \cong L/N.$$ □

Bemerkung 11.26. Nach Satz 11.25(i) ist eine maximale Schur-Erweiterung einer perfekten Gruppe G auch perfekt und bis auf Isomorphie eindeutig bestimmt (dies wird in Satz 11.28 verallgemeinert). Man nennt sie *universelle Schur-Erweiterung* von G.[21] Nach Satz 11.23 ist jede Schur-Erweiterung von G zu einer Faktorgruppe der universellen Schur-Erweiterung isomorph.

Satz 11.27. *Die universelle Schur-Erweiterung einer perfekten Gruppe hat trivialen Schur-Multiplikator.*

[21] Schur spricht von *Darstellungsgruppen*.

Beweis. Sei $\widehat{G}$ eine maximale Schur-Erweiterung von G mit $\widehat{G}/Z \cong G$. Sei $\widehat{\widehat{G}}$ eine maximale Schur-Erweiterung von $\widehat{G}$ mit $\widehat{\widehat{G}}/W \cong \widehat{G}$. Mit G sind auch $\widehat{G}$ und $\widehat{\widehat{G}}$ perfekt. Sei $\mathrm{Z}(\widehat{\widehat{G}}/W) = X/W$. Es gilt

$$[\widehat{\widehat{G}}, X, \widehat{\widehat{G}}] = [\widehat{\widehat{G}}, \widehat{\widehat{G}}, X] \leq [\widehat{\widehat{G}}, W] = 1.$$

Aus Lemma 3.6 folgt $[X, \widehat{\widehat{G}}] = [X, \widehat{\widehat{G}}, \widehat{\widehat{G}}] = 1$ und $X \leq \mathrm{Z}(\widehat{\widehat{G}}) \leq X$. Sei L/W das Urbild von Z unter $\widehat{\widehat{G}}/W \cong \widehat{G}$. Dann ist $L/W \leq \mathrm{Z}(\widehat{\widehat{G}}/W) = \mathrm{Z}(\widehat{\widehat{G}})/W$ und $\widehat{\widehat{G}}/L \cong (\widehat{\widehat{G}}/W)/(L/W) \cong \widehat{G}/Z \cong G$. Also ist $\widehat{\widehat{G}}$ eine Schur-Erweiterung von G. Dies zeigt $\widehat{\widehat{G}} \cong \widehat{G}$ und $M(\widehat{G}) = 1$. □

Satz 11.28. *Sind $|G/G'|$ und $|M(G)|$ teilerfremd, so besitzt G bis auf Isomorphie nur eine maximale Schur-Erweiterung.*

Beweis. Wie in Satz 11.25 sei $G = F/N$ und $\widehat{G}_i = F/K_i$ für $i = 1, 2$. Wir wählen $x_1, \ldots, x_n \in F$ mit

$$\langle x_1, \ldots, x_n \rangle F'N/F'N = F/F'N \cong G/G' \cong C_{d_1} \times \ldots \times C_{d_n}$$

und $x_j^{d_j} \in F'N$ für $j = 1, \ldots, n$. Nach Satz 11.23 ist $F'N = F'(F' \cap N)K_i = F'K_i$. Sei $a_j \in K_1$ mit $x_j^{d_j} a_j \in F'$. Als Teiler von $|G/G'|$ ist d_j zu

$$|K_1/(K_1 \cap K_2)| = |K_1K_2/K_2| \leq |N/K_2| = |(N/[F,N])/(K_2/[F,N])| = |M(G)|$$

teilerfremd. Daher existiert ein $b_j \in K_1$ mit $b_j^{d_j} \equiv a_j \pmod{K_1 \cap K_2}$. Es folgt

$$(x_jb_j)^{d_j} \equiv x_j^{d_j} b_j^{d_j} \equiv 1 \pmod{F'(K_1 \cap K_i)}.$$

Indem wir x_j durch x_jb_j ersetzen, können wir $x_j^{d_j} \in F'(K_1 \cap K_2)$ für $j = 1, \ldots, n$ annehmen. Wegen $F' \cap K_1 = [F,N] = F' \cap K_2$ und ist die Abbildung $F'N/K_1 \to F'N/K_2$, $yK_1 \mapsto yK_2$ mit $y \in F'$ ein wohldefinierter Isomorphismus. Dabei wird $x_j^{d_j}K_1$ auf $x_j^{d_j}K_2$ abgebildet.

Jedes Element in $\widehat{G}_i$ hat die Form $x_1^{e_1} \ldots x_n^{e_n} yK_i$ mit $y \in F'$ und eindeutig bestimmten $0 \leq e_j < d_j$. Daher ist die Abbildung

$$\Gamma \colon \widehat{G}_1 \to \widehat{G}_2, \qquad x_1^{e_1} \ldots x_n^{e_n} yK_1 \mapsto x_1^{e_1} \ldots x_n^{e_n} yK_2$$

wohldefiniert und bijektiv. Für $0 \leq f_j < d_j$ und $z \in F'$ gilt

$$x_1^{e_1} \ldots x_n^{e_n} y \cdot x_1^{f_1} \ldots x_n^{f_n} z \equiv x_1^{e_1+f_1} \ldots x_n^{e_n+f_n} \pmod{F'}.$$

Sei $e_j + f_j = g_j + k_jd_j$ mit $0 \leq g_j < d_j$ für $j = 1, \ldots, n$. Dann existiert $c \in F'$ mit

$$x_1^{e_1} \ldots x_n^{e_n} y \cdot x_1^{f_1} \ldots x_n^{f_n} z = x_1^{g_1} \ldots x_n^{g_n} x_1^{k_1d_1} \ldots x_n^{k_nd_n} c.$$

Dies zeigt

$$\Gamma(x_1^{g_1} \ldots x_n^{g_n} x_1^{k_1d_1} \ldots x_n^{k_nd_n} cK_1) = x_1^{g_1} \ldots x_n^{g_n} x_1^{k_1d_1} \ldots x_n^{k_nd_n} cK_2 = \Gamma(x_1^{e_1} \ldots x_n^{e_n} yK_1)\Gamma(x_1^{f_1} \ldots x_n^{f_n} zK_1),$$

d. h. Γ ist ein Isomorphismus. □

Satz 11.29 (Hochschild-Serre-Sequenz)**.** *Sei $N \trianglelefteq G$ und $H = G/N$. Dann existiert eine exakte Folge der Form*

$$M(G) \to M(H) \to N/[G,N] \to G/G' \to H/H' \to 1.$$

Beweis. Nach dem zweiten Isomorphiesatz dürfen wir H/H' durch $G/G'N$ ersetzen. Sicher ist dann

$$\alpha\colon G/G' \to G/G'N, \quad xG' \to xG'N$$

ein Epimorphismus. Wegen $[G,N] \leq G'$ ist

$$\beta\colon N/[G,N] \to G/G', \quad x[G,N] \to xG'$$

ein wohldefinierter Homomorphismus mit Bild $NG'/G' = \mathrm{Ker}(\alpha)$. Sei nun F eine freie Gruppe und $\rho\colon F \to G$ ein Epimorphismus mit Kern $K \trianglelefteq F$. Für $L := \rho^{-1}(N) \trianglelefteq F$ gilt $L/K \cong N$ und $F/L \cong (G/K)/(L/K) \cong H$. Nach der Hopf-Formel dürfen wir $M(G)$ durch $(F' \cap K)/[F,K]$ und $M(H)$ durch $(F' \cap L)[F,L]$ ersetzen. Wegen $\rho([F,L]) = [G,N]$ ist die Abbildung

$$\gamma\colon (F' \cap L)/[F,L] \to N/[G,N], \quad x[F,L] \mapsto \rho(x)[G,N]$$

ein wohldefinierter Homomorphismus mit Bild $\rho(F' \cap L)/[G,N] = (G' \cap N)/[G,N] = \mathrm{Ker}(\beta)$ und $\mathrm{Ker}(\gamma) = (F' \cap K)[F,L]/[F,L]$. Schließlich ist auch

$$\delta\colon (F' \cap K)/[F,K] \to (F' \cap L)/[F,L], \quad x[F,K] \mapsto x[F,L]$$

ein wohldefinierter Homomorphismus mit Bild $(F' \cap K)[F,L]/[F,L] = \mathrm{Ker}(\gamma)$. □

Folgerung 11.30 (Jones)**.** *Sei $N \trianglelefteq G$. Dann ist $|M(G/N)|$ ein Teiler von $|(G' \cap N)/[G,N]||M(G)|$.*

Beweis. Mit den Bezeichnungen aus dem Beweis von Satz 11.29 gilt

$$|M(G)/\mathrm{Ker}(\delta)| = |\delta(M(G))| = |\mathrm{Ker}(\gamma)| = \frac{|M(H)|}{|\mathrm{Ker}(\beta)|} = \frac{|M(H)|}{|(G' \cap N)/[G,N]|}.$$ □

Definition 11.31. Für endliche Gruppen G, H sei

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

Satz 11.32 (Künneth-Formel)**.** *Für endliche Gruppen G und H gilt*

$$\boxed{M(G \times H) \cong M(G) \times M(H) \times P(G,H).}$$

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

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

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

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

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

Surjektivität von $\overline{F}$: Sei $\alpha_1 \in Z^2(G,\mathbb{C}^\times)$, $\alpha_2 \in Z^2(H,\mathbb{C}^\times)$ und $\varphi \in P(G,H)$. Nach Lemma 11.9 dürfen wir $\alpha_1(1,1) = \alpha_2(1,1) = 1$ annehmen. Für $x_1, y_1 \in G$ und $x_2, y_2 \in H$ sei $\alpha(x_1x_2, y_1y_2) := \alpha_1(x_1,y_1)\alpha_2(x_2,y_2)\varphi(x_1,y_2)$. Dann ist

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

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

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

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

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

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

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

Bemerkung 11.33.

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

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

Lemma 11.34. *Für $n,m \in \mathbb{N}$ ist $P(C_n,C_m) \cong C_{\mathrm{ggT}(n,m)}$.*

Beweis. Sei $\langle x\rangle \cong C_n$, $\langle y\rangle \cong C_m$ und $\varphi \in P(\langle x\rangle,\langle y\rangle)$. Dann ist

$$\varphi(x,y)^n = \varphi(x^n,y) = \varphi(1,y) = 1 = \varphi(x,1) = \varphi(x,y^m) = \varphi(x,y)^m,$$

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

Folgerung 11.35. *Sind G und H endliche Gruppen mit* $\mathrm{ggT}(|G/G'|, |H/H'|) = 1$*, so ist* $M(G \times H) \cong M(G) \times M(H)$.

Beweis. Die Behauptung folgt aus Satz 11.32, Bemerkung 11.33 und Lemma 11.34. □

Beispiel 11.36. Sind G und H perfekte Gruppen mit universellen Schur-Erweiterungen $\widehat{G}$ bzw. $\widehat{H}$, so ist $\widehat{G} \times \widehat{H}$ die universelle Schur-Erweiterung von $G \times H$ (Aufgabe 74).

Satz 11.37. *Für $n_1, \ldots, n_k \in \mathbb{N}$ gilt*

$$M(C_{n_1} \times \ldots \times C_{n_k}) \cong \bigtimes_{1 \le i < j \le k} C_{\mathrm{ggT}(n_i, n_j)}.$$

Beweis. Nach Folgerung 11.19, Satz 11.32, Bemerkung 11.33 und Lemma 11.34 ist

$$\begin{aligned} M(C_{n_1} \times \ldots \times C_{n_k}) &\cong M(C_{n_2} \times \ldots \times C_{n_k}) \times P(C_{n_1}, C_{n_2} \times \ldots \times C_{n_k}) \cong \ldots \\ &\cong \bigtimes_{1 \le i < j \le k} P(C_{n_i}, C_{n_j}) \cong \bigtimes_{1 \le i < j \le k} C_{\mathrm{ggT}(n_i, n_j)}. \end{aligned}$$

□

Beispiel 11.38.

(i) Ist $A \cong C_{d_1} \times \ldots \times C_{d_n}$ mit $d_1 \mid \ldots \mid d_n$ wie in Satz 2.11, so vereinfacht sich die Formel zu

$$M(A) \cong C_{d_1}^{n-1} \times C_{d_2}^{n-2} \times \ldots \times C_{d_{n-1}}.$$

(ii) Ist G elementarabelsch vom Rang k, so ist $M(G)$ elementarabelsch von Rang $\binom{k}{2}$. Also ist die Abschätzung in Satz 11.22 optimal. Insbesondere ist $M(C_2^2) \cong C_2$. Die Gruppen D_8 und Q_8 sind daher die einzigen echten Schur-Erweiterungen von C_2^2. Dies zeigt, dass es nicht-isomorphe maximale Schur-Erweiterungen geben kann.

(iii) Sei G eine p-Gruppe der Ordnung p^n mit $|G : \Phi(G)| = p^k$. Nach Satz 11.24 und Folgerung 11.30 (mit $N = \Phi(G)$) ist

$$p^{\binom{k}{2}} = |M(G/\Phi(G))| \le |G'||M(G)| \le p^{\binom{n}{2}}.$$

Wegen $|G'| \le |\Phi(G)| = p^{n-k}$ folgt $|M(G)| \ge p^{\binom{k}{2}-n+k} = p^{\binom{k+1}{2}-n}$. Green hat $M(G) \ne 1$ für $k \ge 4$ bewiesen. Ist G extraspeziell, so erhält man $p^{\binom{n-1}{2}-1} \le |M(G)| \le p^{\binom{n}{2}-1}$. Blackburn und Evens haben bewiesen, dass hier $|M(G)| = p^{\binom{n-1}{2}-1}$ für $n \ge 5$ gilt.

(iv) Sei $\widehat{G}$ eine Schur-Erweiterung von $G \in \{D_{2^n}, Q_{2^n}, SD_{2^n}\}$ mit $\widehat{G}/Z \cong G$. Nach Satz 11.11 ist $\widehat{G}$ eine 2-Gruppe und $4 = |G : G'| = |\widehat{G}/Z : \widehat{G}'/Z| = |\widehat{G} : \widehat{G}'|$. Nach Taussky gilt daher $\widehat{G} \in \{D_{2^m}, Q_{2^m}, SD_{2^m}\}$. Es folgt $|Z| \le |\mathrm{Z}(\widehat{G})| = 2$ und im Fall $|Z| = 2$ ist $Z = \mathrm{Z}(\widehat{G})$ und $G \cong \widehat{G}/Z \cong D_{2^{m-1}}$. Wir haben also gezeigt:

$$M(G) \cong \begin{cases} C_2 & \text{falls } G \cong D_{2^n}, \\ 1 & \text{falls } G \in \{Q_{2^n}, SD_{2^n}\}. \end{cases}$$

(v) Die Sylowgruppen von A_7 sind $\langle (1,2,3,4)(5,6), (1,2)(3,4)\rangle \cong D_8$, $\langle (1,2,3), (4,5,6)\rangle \cong C_3^2$, $\langle (1,\dots,5)\rangle \cong C_5$ und $\langle (1,\dots,7)\rangle \cong C_7$. Nach Folgerung 11.19 existiert ein Monomorphismus $M(A_7) \to M(D_8) \times M(C_3^2) \cong C_6$. Tatsächlich gilt[22]

$$M(A_n) = \begin{cases} C_6 & \text{falls } n \in \{6,7\}, \\ C_2 & \text{falls } n \in \{5,8,9,\dots\}. \end{cases}$$

(vi) Sei $G = \mathrm{PSL}(2,p)$ für eine Primzahl $p > 3$. Nach Bemerkung 10.14 ist jede Sylowgruppe von G zyklisch oder eine Diedergruppe. Aus Beispiel 11.4 und (iv) folgt $M(G) \leq C_2$. Daher ist $\mathrm{SL}(2,p)$ die universelle Schur-Erweiterung von $\mathrm{PSL}(2,p)$. Wenn man von den Ausnahmen $\mathrm{SL}(2,4) \cong \mathrm{PSL}(2,4) \cong A_5$ und $\mathrm{PSL}(2,9) \cong A_6$ absieht, gilt dies auch für $\mathrm{PSL}(2,q)$ für eine Primzahlpotenz $q \geq 5$ (ohne Beweis).

Aufgaben

Aufgabe 1. Sei G eine Gruppe. Zeigen Sie:

(a) Eine nichtleere endliche Teilmenge $H \subseteq G$ ist genau dann eine Untergruppe von G, falls $xy \in H$ für alle $x, y \in H$ gilt.

(b) Jede Untergruppe vom Index 2 ist normal.

(c) Sei $G = \langle X\rangle$ und $H = \langle Y\rangle \leq G$. Genau dann ist $H \trianglelefteq G$, falls $xyx^{-1} \in H$ für alle $x \in X \cup X^{-1}$ und $y \in Y$.

Aufgabe 2. Seien U, V, W Untergruppen einer (möglicherweise unendlichen) Gruppe G. Zeigen Sie:

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

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

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

Aufgabe 3. Zeigen Sie, dass für jede Gruppe G die folgenden Aussagen äquivalent sind:

(1) G ist abelsch.

(2) Die Abbildung $G \to G$, $x \mapsto x^{-1}$ ist ein Automorphismus.

(3) Die Abbildung $G \to G$, $x \mapsto x^2$ ist ein Endomorphismus.

Sei nun $|G| < \infty$. Wann ist $G \to G$, $x \mapsto x^2$ ein Automorphismus?

[22] Siehe Skript zur kombinatorischen Gruppentheorie

Aufgabe 4. Seien $H \leq G$ Gruppen mit $n := |G : H| < \infty$. Zeigen Sie:

(a) G operiert transitiv durch Linksmultiplikation auf G/H, d. h. ${}^x(gH) := xgH$ für $x, g \in G$.

(b) Der Kern dieser Operation ist $H_G = \bigcap_{g \in G} gHg^{-1}$. Insbesondere ist $|G : H_G| \leq n!$.

(c) Ist $|G| < \infty$ und n der kleinste Primteiler von $|G|$, so ist $H \trianglelefteq G$ (dies verallgemeinert Aufgabe 1(b)).

(d) Ist $n > 1$, so ist $\bigcup_{g \in G} gHg^{-1} \neq G$.
Hinweis: Indem man G durch G/H_G ersetzt, kann man $|G| < \infty$ annehmen.

(e) Für $H := \left\{ \left(\begin{smallmatrix} * & * \\ 0 & * \end{smallmatrix}\right) \right\} < G := \mathrm{GL}(2, \mathbb{C})$ gilt $G = \bigcup_{g \in G} gHg^{-1}$.
Hinweis: Ähnlichkeit von Matrizen.

Aufgabe 5. Zeigen Sie:

(a) Eine Gruppe ist genau dann endlich, wenn sie nur endlich viele Untergruppen besitzt.

(b) Eine endlich erzeugte Gruppe besitzt für jedes $n \in \mathrm{N}$ nur endlich viele Untergruppen vom Index n.

(c) Sei G endlich erzeugt und $H \leq G$ mit $|G : H| < \infty$. Dann existiert eine charakteristische Untergruppe K von G mit $K \leq H$ und $|G : K| < \infty$.

Aufgabe 6. Für $3 \leq n \in \mathbb{N}$ sei

$$D_{2n} := \langle \sigma, \tau \rangle \leq \mathrm{Sym}(\mathbb{C})$$

mit $\sigma(z) := e^{\frac{2\pi \mathrm{i}}{n}} z$ und $\tau(z) := \overline{z}$ (komplexe Konjugation) für $z \in \mathbb{C}$. Zeigen Sie:

(a) $\langle \sigma \rangle \trianglelefteq D_{2n}$ und $|D_{2n}| = 2n$.

(b) Ist $\Delta \subseteq \mathbb{C}$ das regelmäßige n-Eck in der komplexen Ebene mit Mittelpunkt 0 und Eckpunkt 1 (also die konvexe Hülle der n-ten Einheitswurzeln), so gilt

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

d. h. D_{2n} ist die *Symmetriegruppe* des regelmäßigen n-Ecks.

Man nennt D_{2n} *Diedergruppe* der Ordnung $2n$.

Aufgabe 7.

(a) Zeigen Sie, dass $(\mathbb{Q}, +)$ *lokal zyklisch* ist, d. h. jede endlich erzeugte Untergruppe von $\mathbb{Q}$ ist zyklisch. Ist $\mathbb{Q}$ selbst zyklisch?

(b) Sei p eine Primzahl und $A := \{ap^b + \mathbb{Z} : a, b \in \mathbb{Z}\} \leq \mathbb{Q}/\mathbb{Z}$. Zeigen Sie, dass jede echte Untergruppe von A endlich und zyklisch ist.

(c) Sei $\mathbb{Z}[X]$ der Ring der Polynome mit ganzzahligen Koeffizienten. Sei $\mathbb{Q}_+ := \{q \in \mathbb{Q} : q > 0\}$. Zeigen Sie $(\mathbb{Z}[X], +) \cong (\mathbb{Q}_+, \cdot)$.
Hinweis: Primfaktorzerlegung.

(d) Entscheiden Sie, ob $(\mathbb{R}, +)$ und $(\mathbb{C}, +)$ isomorph sind.
Hinweis: Auswahlaxiom.

Aufgabe 8. Sei G eine Gruppe. Zeigen Sie:

(a) Ist $G/\mathrm{Z}(G)$ zyklisch, so ist G abelsch (d. h. $G/\mathrm{Z}(G) = 1$).

(b) $\mathrm{C}_{\mathrm{Aut}(G)}(\mathrm{Inn}(G))$ besteht aus allen Automorphismen, die trivial auf $G/\mathrm{Z}(G)$ operieren. Insbesondere ist $\mathrm{Z}(\mathrm{Aut}(G)) = 1$, falls $\mathrm{Z}(G) = 1$.

Aufgabe 9.

(a) Wie viele abelsche Gruppen der Ordnung 72 existieren bis auf Isomorphie?

(b) Bestimmen Sie den Isomorphietyp von $\mathrm{Aut}(C_{24})$.

Aufgabe 10. Sei G eine nichtabelsche Gruppe der Ordnung 8. Zeigen Sie:

(a) G besitzt ein Element x der Ordnung 4.
Hinweis: Aufgabe 3.

(b) Für $y \in G \setminus \langle x \rangle$ gilt $y^4 = 1$ und $yx = x^{-1}y$.

(c) Die Multiplikationstabelle von G ist durch die Ordnung von y eindeutig bestimmt.

(d) Im Fall $y^2 = 1$ ist $G \cong D_8$.

(e) Im Fall $y^2 \neq 1$ ist

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

mit $\mathrm{i} = \sqrt{-1}$. Man nennt Q_8 *Quaternionengruppe* der Ordnung 8.
Hinweis: Es genügt zu zeigen, dass Q_8 die gewünschten Eigenschaften hat.

(f) Konstruieren Sie alle Gruppen der Ordnung 8 bis auf Isomorphie.
Hinweis: Zeigen Sie $D_8 \ncong Q_8$ durch Zählen von Involutionen.

Aufgabe 11 (3. Isomorphiesatz[23])**.** Für $B \trianglelefteq A \leq G$ und $D \trianglelefteq C \leq G$ gilt

$$(A \cap C)B/(A \cap D)B \cong (C \cap A)D/(C \cap B)D.$$

Aufgabe 12 (Schreiers Verfeinerungssatz)**.** Je zwei Subnormalreihen $1 = A_0 \trianglelefteq \ldots \trianglelefteq A_k = G$ und $1 = B_0 \trianglelefteq \ldots \trianglelefteq B_l = G$ lassen sich verfeinern, sodass die Faktoren der neuen Reihen bis auf die Reihenfolge isomorph sind. Folgern Sie daraus den Satz von Jordan-Hölder.
Hinweis: Aufgabe 11

Aufgabe 13. Sei $A \to \mathrm{Aut}(G)$ eine Gruppenoperation. Eine Subnormalreihe $1 = N_0 \trianglelefteq \ldots \trianglelefteq N_k = G$ heißt *A-invariant*, falls ${}^aN_i = N_i$ für $i = 1, \ldots, k$ und alle $a \in A$ gilt. Eine A-invariante Subnormalreihe heißt *A-Kompositionsreihe*, falls die N_i paarweise verschieden sind und sich die Reihe nicht weiter als A-invariante Reihe verfeinern lässt. Zeigen Sie, dass die *A-Kompositionsfaktoren* N_i/N_{i-1} bis auf Isomorphie und Reihenfolge eindeutig bestimmt ist. Folgern Sie, dass die Hauptfaktoren von G nicht von der Wahl einer Hauptreihe abhängen.
Hinweis: Beweis von Jordan-Hölder oder Aufgabe 12.

[23] oder Zassenhaus-Lemma

Aufgabe 14.

(a) Bestimmen Sie die Kompositionsfaktoren und Hauptfaktoren von S_4.

(b) Bestimmen Sie die Kompositionsfaktoren und Hauptfaktoren von $\mathrm{GL}(2,3)$.
Hinweis: Betrachten Sie die natürliche Operation von $\mathrm{GL}(2,3)$ auf der Menge der 1-dimensionalen Unterräume von $\mathbb{F}_3^2$.

Aufgabe 15. Eine Untergruppe $H \leq G$ heißt *vollständig invariant* in G, falls $\alpha(H) \subseteq H$ für jeden Endomorphismus α von G. Zeigen Sie:

(a) Jede vollständig invariante Untergruppe ist charakteristisch in G.

(b) Jede Untergruppe einer zyklischen Gruppe ist vollständig invariant.

(c) Welche Untergruppen von S_4 sind charakteristisch und welche sind vollständig invariant?

(d) $\mathrm{Z}(G)$ ist stets charakteristisch in G.

(e) $\mathrm{Z}(G)$ ist nicht unbedingt vollständig invariant in G.

Aufgabe 16. Sei G eine Gruppe und $x, y \in G$. Zeigen Sie:

(a) Aus $[x,x,y] = 1$ folgt $[x^n, y] = [x,y]^n$ für alle $n \in \mathbb{Z}$.

(b) Aus $[x,x,y] = [y,x,y] = 1$ folgt $(xy)^n = x^n y^n [y,x]^{\binom{n}{2}}$ für alle $n \in \mathbb{N}$.

Aufgabe 17.

(a) Zeigen Sie $D_{4n} \cong D_{2n} \times C_2$ für alle ungeraden Zahlen $n \geq 3$.

(b) Bestimmen Sie alle natürlichen Zahlen $n \geq 3$, sodass die Diedergruppe D_{2n} nilpotent ist. Berechnen Sie ggf. die Nilpotenzklasse.

Aufgabe 18. Sei $G = N \oplus M$ endlich. Zeigen Sie $\mathrm{F}(G) = \mathrm{F}(N) \oplus \mathrm{F}(M)$.
Achtung: Nicht jede Untergruppe von $N \oplus M$ hat die Form $N_1 \oplus M_1$ mit $N_1 \leq N$ und $M_1 \leq M$.

Aufgabe 19. Zeigen Sie für jede Gruppe G:

(a) $\exp(\mathrm{Z}_k(G)/\mathrm{Z}_{k-1}(G)) \leq \exp(\mathrm{Z}(G))$ für $k \geq 1$.
Hinweis: Induktion nach k und Aufgabe 16(a).

(b) $[G^{[i]}, \mathrm{Z}_j(G)] \leq \mathrm{Z}_{j-i}(G)$ für $1 \leq i \leq j$.
Hinweis: Induktion nach $i+j$ und das 3-Untergruppen-Lemma.

Aufgabe 20. Wie viele nilpotente Gruppen der Ordnung 72 gibt es bis auf Isomorphie?

Aufgabe 21. Zeigen Sie, dass jede Gruppe der Ordnung 220 einen Normalteiler der Ordnung 55 besitzt.
Hinweis: Konstruieren Sie zunächst einen kleineren Normalteiler.

Aufgabe 22. Seien P und Q zwei verschiedene p-Sylowgruppen von G, sodass $|P \cap Q|$ so groß wie möglich ist. Zeigen Sie

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

Aufgabe 23.

(a) Berechnen Sie $\Phi(S_4)$.

(b) Sei $G = N \oplus M$. Zeigen Sie $\Phi(G) = \Phi(N) \oplus \Phi(M)$.

(c) Bestimmen Sie die Frattinigruppe einer endlichen abelschen Gruppe.
Hinweis: Benutzen Sie *nicht* die Definition.

Aufgabe 24. Eine Gruppe G heißt *vollständig*, falls $\mathrm{Z}(G) = 1 = \mathrm{Out}(G)$. Zeigen Sie:

(a) S_3 ist vollständig.

(b) Ist G vollständig, so ist $\mathrm{Aut}(G) \cong G$.

(c) Ist N ein vollständiger Normalteiler von G, so ist $G = N \oplus \mathrm{C}_G(N)$.

(d) Ist S eine nichtabelsche einfache Gruppe, so ist $\mathrm{Aut}(S)$ vollständig.
Hinweis: Aufgabe 8.

Aufgabe 25. Konstruieren Sie Gruppen $X, Y, Z \leq G$ mit $[X, Y, Z] \neq [Y, X, Z]$.

Aufgabe 26. Sei A ein abelscher Normalteiler von G, sodass G/A zyklisch ist, sagen wir $G/A = \langle xA \rangle$ mit $x \in G$. Zeigen Sie, dass die Abbildung $A \to G'$, $a \mapsto [a, x]$ ein Epimorphismus ist. Folgern Sie $|A| = |G'||A \cap \mathrm{Z}(G)|$.

Aufgabe 27.

(a) Zeigen Sie $\Phi(G) \leq \mathrm{F}(G)$ und $\mathrm{F}(G/\Phi(G)) = \mathrm{F}(G)/\Phi(G)$ für jede endliche Gruppe G.

(b) Sei P eine endliche p-Gruppe mit $Q \leq P$, $N \trianglelefteq P$. Zeigen Sie $\Phi(Q) \leq \Phi(P)$ und $\Phi(P/N) = \Phi(P)N/N$.

(c) Zeigen Sie $\Phi(P) = \langle x^2 : x \in P \rangle$ für jede endliche 2-Gruppe P.

Aufgabe 28. Für eine endliche Gruppe G sei $\mathrm{F}_0(G) := 1$, $\mathrm{K}_0(G) := G$ und induktiv

$$\mathrm{F}_n(G)/F_{n-1}(G) := \mathrm{F}(G/\mathrm{F}_{n-1}(G)), \qquad \mathrm{K}_n(G) := \bigcap_{i \geq 1} \mathrm{K}_{n-1}(G)^{[i]}$$

für $n \geq 1$. Zeigen Sie:

(a) Sei $1 = N_0 \trianglelefteq \ldots \trianglelefteq N_k = G$ eine Normalreihe mit nilpotenten Faktoren N_i/N_{i-1} für $i = 1, \ldots, k$. Dann gilt $K_{k-i}(G) \leq N_i \leq \mathrm{F}_i(G)$ für $i = 0, \ldots, k$.

(b) Genau dann ist G auflösbar, falls ein $l(G) = l \geq 0$ mit $\mathrm{F}_{l-1}(G) < \mathrm{F}_l(G) = G$ und $\mathrm{K}_{l-1}(G) > \mathrm{K}_l(G) = 1$ existiert. Ggf. nennt man $l(G)$ die *Fitting-Länge* von G.

Bemerkung: Im Allgemeinen ist $G^{[\infty]} := \mathrm{K}_1(G)$ das *nilpotente Residuum*, $\mathrm{F}_\infty(G) := \bigcup_{n\in\mathbb{N}} \mathrm{F}_n(G)$ das *auflösbare Radikal* und $G^{(\infty)} := \bigcap_{n\in\mathbb{N}} G^{(n)} = \bigcap_{n\in\mathbb{N}} \mathrm{K}_n(G)$ das *auflösbare Residuum* von G.

Aufgabe 29. Sei G eine Gruppe und A, B konjugierte Untergruppen von $\mathrm{Aut}(G)$. Zeigen Sie $G \rtimes A \cong G \rtimes B$.

Aufgabe 30. Sei G eine endliche Gruppe und $x, y \in G$ verschiedene Involutionen. Zeigen Sie $\langle x, y\rangle \cong D_{2n}$ (wobei $D_4 = C_2^2$).

Aufgabe 31. (Levi) Sei G eine endliche Gruppe, in der je zwei konjugierte Elemente vertauschbar sind. Zeigen Sie, dass G nilpotent ist.
Hinweis: Zeigen Sie, dass Elemente teilerfremder Ordnungen vertauschbar sind.

Aufgabe 32. Sei H eine π-Hallgruppe von G und $N \trianglelefteq G$. Zeigen Sie:

(a) $H \cap N$ ist eine π-Hallgruppe von N und HN/N ist eine π-Hallgruppe von G/N.

(b) Für $U \leq G$ ist nicht unbedingt $H \cap U$ eine π-Hallgruppe von U.

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

Aufgabe 33. Eine endliche Gruppe G heißt *Frobeniusgruppe*, falls eine Untergruppe $1 < H < G$ mit $H \cap gHg^{-1} = 1$ für alle $g \in G \setminus H$ existiert (H ist also besonders weit davon entfernt ein Normalteiler zu sein). Zeigen Sie, dass H eine Hallgruppe von G ist.
Hinweis: Satz 4.10 ist nützlich.

Aufgabe 34.

(a) Zeigen Sie, dass A_5 keine $\{2, 5\}$-Hallgruppe besitzt.

(b) Zeigen Sie, dass nicht jede $\{2, 3\}$-Untergruppe von A_5 in einer $\{2, 3\}$-Hallgruppe liegt.

(c) Konstruieren Sie eine endliche Gruppe G mit zwei nicht-konjugierten Hallgruppen der gleichen Ordnung.
Hinweis: Betrachten Sie $G = \mathrm{GL}(3, 2)$.
Bemerkung: Die Gruppe $\mathrm{PSL}(2, 11)$ besitzt sogar nicht-isomorphe Hallgruppen der gleichen Ordnung.

Aufgabe 35. Sei G eine auflösbare Gruppe, p eine Primzahl und $|\mathrm{Syl}_p(G)| = p_1^{a_1} \dots p_n^{a_n}$ (Primfaktorzerlegung). Zeigen Sie $p_i^{a_i} \equiv 1 \pmod{p}$ für $i = 1, \dots, n$.
Bemerkung: Dies verfeinert die Kongruenz aus dem Satz von Sylow.

Aufgabe 36. (Goursat) Seien G_1 und G_2 Gruppen. Konstruieren Sie eine Bijektion zwischen der Menge der Untergruppen von $G_1 \times G_2$ und der Menge der 5-Tupel $(H_1, H_2, K_1, K_2, \varphi)$, wobei $K_i \trianglelefteq H_i \leq G_i$ $(i = 1, 2)$ und $\varphi\colon H_1/K_1 \to H_2/K_2$ ein Isomorphismus ist.

Aufgabe 37. Zeigen Sie für $n \geq 3$:

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

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

Hinweis: Sie dürfen benutzen, dass S_n von allen Transpositionen erzeugt wird.

Aufgabe 38. Bestimmen Sie die transitiven Permutationsgruppen vom Grad ≤ 4. Welche davon sind primitiv oder regulär?
Hinweis: Satz 6.21 ist hilfreich.

Aufgabe 39. Sei G eine transitive Permutationsgruppe vom Grad > 1, in der jedes nicht-triviale Element höchstens einen Fixpunkt hat und mindestens ein Element genau einen Fixpunkt hat. Zeigen Sie, dass G eine Frobeniusgruppe ist (siehe Aufgabe 33).

Aufgabe 40. Realisieren Sie A_5 als primitive Permutationsgruppe vom Grad 5, 6 und 10.
Hinweis: Nach Satz 6.9 genügt es, geeignete Untergruppen zu finden.

Aufgabe 41. Zeigen Sie, dass eine auflösbare Permutationsgruppe nicht 5-transitiv operieren kann.

Aufgabe 42. Sei G eine endliche Gruppe, $N \trianglelefteq G$ und $G/N \cong H$. Zeigen Sie, dass G zu einer Untergruppe von $N \wr H$ isomorph ist.
Hinweis: Wenden Sie Satz 6.26 auf die reguläre Operation an.

Aufgabe 43. Zeigen Sie, dass die p-Sylowgruppen von S_{p^n} zu $C_p \wr \ldots \wr C_p$ (n Faktoren) isomorph sind.

Aufgabe 44. Berechnen Sie die Nilpotenzklasse von $C_p \wr C_p \in \mathrm{Syl}_p(S_{p^2})$ für jede Primzahl p.

Aufgabe 45. Zeigen Sie für $n \in \mathbb{N}$, dass die 2-Sylowgruppen von S_n Cartergruppen sind.

Aufgabe 46. Zeigen Sie, dass eine auflösbare Gruppe G genau dann eine primitive Permutationsgruppe ist, wenn ein minimaler Normalteiler $A \trianglelefteq G$ mit $\mathrm{C}_G(A) = A$ existiert.

Aufgabe 47. Zeigen Sie, dass $\mathrm{SL}(2,\mathbb{F}_{2^n})$ 3-transitiv auf der Menge der 1-dimensionalen Unterräume von $\mathbb{F}_{2^n}^2$ operiert.

Aufgabe 48. Zeigen Sie:

(a) Für jede echte Untergruppe H einer nichtabelschen einfachen Gruppe G gilt $|G : H| \geq 5$.
Hinweis: Aufgabe 4.

(b) Es gibt keine einfache Gruppe der Ordnung 120.
Hinweis: Realisieren Sie ein Gegenbeispiel als Untergruppe von A_6.

(c) $\mathrm{GL}(3,2)$ ist eine einfache Gruppe der Ordnung 168.

(d) Die unendliche Gruppe $A_\infty := \bigcup_{n\geq 1} A_n$ ist einfach.

Aufgabe 49. Berechnen Sie die Verlagerung $V_{G/G'}$ explizit.
Bemerkung: Der *Hauptidealsatz* aus der Klassenkörpertheorie besagt, dass die Verlagerung $V_{G'/G''}$ stets trivial ist.

Aufgabe 50. Sei H eine Hallgruppe einer endlichen Gruppe G mit $\mathrm{N}_G(H) = \mathrm{C}_G(H)$. Zeigen Sie, dass H ein normales Komplement besitzt.

Aufgabe 51. Sei G eine endliche Gruppe mit einer zyklischen p-Sylowgruppe. Sei $N \trianglelefteq G$, sodass $|G:N|$ durch p teilbar ist. Zeigen Sie, dass N p-nilpotent ist.
Hinweis: Für $Q \in \mathrm{Syl}_p(N)$ gilt $\mathrm{N}_N(Q) = Q \rtimes K$ nach Schur-Zassenhaus. Zeigen Sie $[Q,K] = 1$.

Aufgabe 52. Beweisen Sie die folgenden Aussagen für jede überauflösbare Gruppe G:

(a) Ist p der kleinste Primteiler von $|G|$, so ist G p-nilpotent.

(b) Ist q der größte Primteiler von $|G|$, so besitzt G eine normale q-Sylowgruppe.

Aufgabe 53. Zeigen Sie:

(a) Jede nichtabelsche einfache Gruppe der Ordnung < 168 ist zu A_5 isomorph.
Hinweis: Mit geeigneten Sätzen aus der Vorlesung muss man höchstens drei Ordnungen diskutieren.

(b) Jede Gruppe der Ordnung 612 ist auflösbar.

Aufgabe 54. Sei G eine p-nilpotente Gruppe und $Q \leq P \in \mathrm{Syl}_p(G)$. Zeigen Sie, dass $\mathrm{N}_G(Q)/\mathrm{C}_G(Q)$ eine p-Gruppe ist.
Bemerkung: Das ist die Umkehrung von Frobenius' Verlagerungssatz.

Aufgabe 55. Zeigen Sie, dass G p-nilpotent ist, falls $G/\Phi(G)$ p-nilpotent ist.
Bemerkung: Die lokalisiert den Satz von Frattini.

Aufgabe 56 ($2+2+2+2$ Punkte)**.** Seien $N, M \trianglelefteq G$. Zeigen Sie:

(a) Sind $N, M \trianglelefteq G$ p-nilpotent, so auch MN. Das Produkt aller p-nilpotenten Normalteiler $\mathrm{F}_{(p)}(G)$ ist daher p-nilpotent.

(b) $\mathrm{O}_{p'}(G) \leq \mathrm{F}_{(p)}(G)$ und $\mathrm{F}_{(p)}(G)/\mathrm{O}_{p'}(G) = \mathrm{O}_p(G/\mathrm{O}_{p'}(G))$.

(c) Sind G/N und G/M p-nilpotent, so auch $G/(N \cap M)$.

(d) Der kleinste Normalteiler von G mit p-nilpotenter Faktorgruppe ist $\mathrm{O}^{p'}(\mathrm{O}^p(G))$.[24]

[24] In einigen Büchern schreibt man $\mathrm{O}^{pp'}(G) := \mathrm{O}^{p'}(\mathrm{O}^p(G))$ und $\mathrm{O}_{p'p}(G)$ anstelle von $\mathrm{F}_{(p)}(G)$.

Aufgabe 57. Wir zeigen, dass man ein Wort w über einem Alphabet A nur in genau ein reduziertes Wort $\overline{w}$ überführen kann. Nehmen wir indirekt an, dass $v \neq w$ reduzierte Wörter sind und eine Folge von Worten $v = v_1, \ldots, v_k = w$ existiert, sodass sich v_i und v_{i+1} nur durch ein Teilwort der Form aa^{-1} oder $a^{-1}a$ ($a \in A$) unterscheiden (für $i = 1, \ldots, k-1$). Sei $|v_i|$ die Anzahl der Buchstaben von v_i. Wir wählen die Folge, sodass $\sum_{i=1}^{k} |v_i|$ minimal ist. Zeigen Sie:

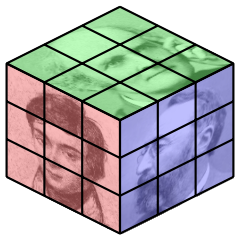
(a) Es existiert ein i mit $|v_{i-1}| < |v_i| > |v_{i+1}|$.

(b) Gilt $v_{i-1} = \ldots a \ldots$, $v_i = \ldots aa^{-1}a \ldots$, $v_{i+1} = \ldots a \ldots$, so kann man v_i und v_{i+1} streichen.

(c) Gilt $v_{i-1} = \ldots aa^{-1} \ldots$, $v_i = \ldots aa^{-1} \ldots bb^{-1} \ldots$, $v_{i+1} = \ldots bb^{-1} \ldots$, so kann man v_i durch v_i' mit $|v_i'| = |v_i| - 4$ ersetzen.

(d) Alle anderen Fälle sind analog und führen ebenso zum Widerspruch.

Weihnachtsrätsel. Sei $G \leq S_{48}$ die Gruppe des Zauberwürfels wie in der Weihnachtsvorlesung. Wir betrachten den „erweiterten“ Zauberwürfel mit Bildern auf allen Seiten:



(a) Beschreiben Sie die Gruppe aller Zustände des erweiterten Zauberwürfels unter Benutzung von G. Wie viele Zustände gibt es?

(b) Wie lässt sich der erweiterte Zauberwürfel lösen, wenn man bereits den gewöhnlichen Zauberwürfel lösen kann?

(c) Wer sind die drei Männer?

Aufgabe 58.

(a) Geben Sie eine Präsentation von S_4 mit Erzeugern und Relationen an.

(b) Bestimmen Sie die Struktur von $\langle x, y \mid x^2 = y^2 = 1 \rangle$.
Hinweis: Es ist ein semidirektes Produkt von bekannten Gruppen.

Aufgabe 59. Sei G eine Gruppe mit Normalteiler N, sodass G/N eine freie Gruppe ist. Zeigen Sie, dass N ein Komplement in G besitzt.
Hinweis: Bemerkung 5.3.

Aufgabe 60. Sei G eine nichtabelsche Gruppe der Ordnung 12. Seien $P \in \mathrm{Syl}_3(G)$ und $Q \in \mathrm{Syl}_2(G)$. Zeigen Sie:

(a) Im Fall $P \trianglelefteq G$ ist $G \cong A_4$.
Hinweis: Benutzen Sie die Operation auf $\mathrm{Syl}_3(G)$.

Sei nun $P \trianglelefteq G$ und damit $G = P \rtimes Q$.

(b) Im Fall $Q \cong C_2^2$ ist $G \cong D_{12}$.

(c) Im Fall $Q \cong C_4$ ist
$$G := \langle x, y \mid x^3 = y^4 = 1,\ yxy^{-1} = x^{-1} \rangle.$$
Bemerkung: Diese Gruppe nennt man *dizyklisch*.

(d) Wie viele Gruppen der Ordnung 12 gibt es bis auf Isomorphie?

Aufgabe 61. Sei $P := \langle x, y \mid x^4 = y^2 = [x, y]^2 = [x, x, y] = [y, x, y] = 1 \rangle$. Zeigen Sie, dass die folgenden 14 Gruppen der Ordnung 16 paarweise nicht isomorph sind:

$$C_{16}, C_8 \times C_2, C_4^2, C_4 \times C_2^2, C_2^4, D_{16}, SD_{16}, Q_{16}, M_{16}, D_8 \times C_2, Q_8 \times C_2, C_4 \rtimes C_4, D_8 * C_4, P.$$

Hinweis: Vergleichen Sie G', $\exp(G)$, $\Phi(G)$ und $\mathrm{Z}(G)$ in dieser Reihenfolge.
Bemerkung: Dies sind alle Gruppen der Ordnung 16 bis auf Isomorphie.

Aufgabe 62.

(a) Sei $G = N_1 \oplus \ldots \oplus N_k$ mit charakteristischen Untergruppen $N_1, \ldots, N_k \leq G$. Zeigen Sie
$$\mathrm{Aut}(G) \cong \mathrm{Aut}(N_1) \times \ldots \times \mathrm{Aut}(N_k).$$

(b) Bestimmen Sie alle $n \in \mathbb{N}$, sodass $\mathrm{Aut}(C_n)$ zyklisch ist.
Hinweis: Benutzen Sie (a).

(c) Zeigen Sie $\mathrm{Aut}(G) \ncong C_3$ für jede endliche Gruppe G.

Aufgabe 63. Sei p eine Primzahl, $n \geq 3$ und $P := M_{p^n}$. Zeigen Sie:

(a) $\mathrm{Z}(P) = \Phi(P)$.

(b) Jede echte Untergruppe von P ist abelsch.

(c) $UV = VU$ für alle $U, V \leq P$.

(d) Für $p = 2$ ist $\mathrm{Aut}(P)$ eine 2-Gruppe.
Hinweis: Bemerkung 4.21.

Aufgabe 64. Eine endliche Gruppe heißt *Dedekind-Gruppe*, falls alle Untergruppen normal sind.

(a) Nach Satz 4.10 ist jede Dedekind-Gruppe nilpotent. Zeigen Sie, dass eine nilpotente Gruppe genau dann eine Dedekind-Gruppe ist, wenn jede ihrer Sylowgruppen eine Dedekind-Gruppe ist.

(b) Zeigen Sie, dass eine p-Gruppe für $p > 2$ genau dann eine Dedekind-Gruppe ist, wenn sie abelsch ist.
Hinweis: Satz 9.6.

(c) Zeigen Sie, dass $Q_8 \times C_2^n$ für alle $n \geq 0$ eine Dedekind-Gruppe ist.
Bemerkung: Dedekind bewies, dass $Q_8 \times C_2^n$ die einzige nichtabelsche Dedekind-Gruppe der Ordnung 2^{n+3} ist.

Aufgabe 65. Sei P eine nichtabelsche p-Gruppe und $A \leq P$ mit $|A| = p^2$ und $\mathrm{C}_P(A) = A$. Zeigen Sie, dass P maximale Klasse hat.
Hinweis: Induktion nach $|P|$.

Aufgabe 66. (Wong) Sei $n \geq 4$ und $M_{2^n} \cong P \in \mathrm{Syl}_2(G)$. Zeigen Sie, dass G 2-nilpotent ist.
Hinweis: Aufgabe 63 und Bemerkung 7.19.

Aufgabe 67. Sei E extraspeziell der Ordnung p^{d+1}. Dann ist $\overline{E} := E/E'$ ein d-dimensionaler Vektorraum über $\mathbb{F}_p \cong E'$. Zeigen Sie, dass

$$\beta\colon \overline{E} \times \overline{E} \to E', \quad (xE', yE') \mapsto [x, y]$$

eine wohldefinierte nicht-ausgeartete alternierende Bilinearform ist (alternierend heißt $\beta(x, x) = 0$ für alle $x \in \overline{E}$). Folgern Sie, dass d gerade ist ohne Satz 9.20 zu benutzen.

Aufgabe 68. Zeigen Sie, dass für jede endliche p-Gruppe $P \neq 1$ die folgenden Aussagen äquivalent sind:

(a) P ist extraspeziell.

(b) $|\mathrm{Z}(P)| = |\Phi(P)| = p$.

(c) $|\mathrm{Z}(P)| = |P'| = p$.

(d) $\mathrm{Z}(P) = P' = \Phi(P)$ ist zyklisch.

Hinweis: Aufgabe 16.
Bemerkung: Im Fall $\Phi(P) = 1$ oder $P' = \Phi(P) = \mathrm{Z}(P)$ nennt man P *speziell*.

Aufgabe 69. Sei G eine endliche Gruppe. Zeigen Sie:

(a) Genau dann gilt $H \leq \mathrm{F}(G)$, wenn H eine subnormale nilpotente Untergruppe von G ist.

(b) Für $H, K \trianglelefteq\trianglelefteq G$ gilt $H \cap K \trianglelefteq\trianglelefteq G$.

(c) Für $H \trianglelefteq\trianglelefteq G$ und $P \in \mathrm{Syl}_p(G)$ gilt $H \cap P \in \mathrm{Syl}_p(H)$.
Bemerkung: Kleidman hat mit der CFSG die Umkehrung bewiesen, d. h. $H \trianglelefteq\trianglelefteq G$, falls $H \cap P \in \mathrm{Syl}_p(H)$ für alle Primzahlen p und alle $P \in \mathrm{Syl}_p(G)$.

Aufgabe 70. Sei G eine endliche perfekte Gruppe. Zeigen Sie, dass $\mathrm{Aut}(G)$ zu einer Untergruppe von $\mathrm{Aut}(G/\mathrm{Z}(G))$ isomorph ist.

Aufgabe 71. Konstruieren Sie eine endliche, nicht-auflösbare Gruppe G mit $\mathrm{E}(G) = 1$.

Aufgabe 72. Zeigen Sie $\mathrm{GL}(2, 4) \cong A_5 \times C_3$.

Aufgabe 73. Zeigen Sie:

(a) Alle Involutionen in $G := \mathrm{GL}(3, 4)$ sind konjugiert.
Hinweis: Da das Minimalpolynom zerfällt, kann man die Jordansche Normalform benutzen.

(b) Alle Involutionen in $S := \mathrm{SL}(3,4)$ sind konjugiert.
Hinweis: Wählen Sie konkret $x \in S$ und zeigen Sie $\mathrm{C}_G(x) \not\subseteq S$.

(c) Alle Involutionen in $\overline{S} := S/\mathrm{Z}(S) = \mathrm{PSL}(3,4)$ sind konjugiert.

(d) $\mathrm{PSL}(3,4)$ und A_8 sind nicht-isomorphe einfache Gruppen der gleichen Ordnung.

Aufgabe 74. Sei $\widehat{G}$ eine Schur-Erweiterung einer endlichen Gruppe G mit $\widehat{G}/Z \cong G$.

(a) Zeigen Sie, dass für $W \leq Z$ auch $\widehat{G}/W$ eine Schur-Erweiterung von G ist.

(b) Sei $\widehat{H}$ eine Schur-Erweiterung einer endlichen Gruppe H. Zeigen Sie, dass $\widehat{G} \times \widehat{H}$ eine Schur-Erweiterung von $G \times H$ ist.

Aufgabe 75. Bestimmen Sie den Schur-Multiplikator und eine entsprechende Schur-Erweiterung von D_{2n} mit $n \geq 3$.

Aufgabe 76. Seien A und B endliche abelsche Gruppen und $f\colon A \to B$ ein Homomorphismus. Sei $A^* := \mathrm{Hom}(A, \mathbb{C}^\times)$. Zeigen Sie:

(a) Die Abbildung $f^*\colon B^* \to A^*$, $\lambda \mapsto \lambda \circ f$ ist ein Homomorphismus.

(b) Die Abbildung $\Gamma_A\colon A \to (A^*)^*$ mit $\Gamma_A(a)(\lambda) := \lambda(a)$ für $a \in A$ ist ein Isomorphismus.
Hinweis: Nach Lemma 11.14 genügt es zu zeigen, dass Γ_A ein Monomorphismus ist.

(c) $(f^*)^* \circ \Gamma_A = \Gamma_B \circ f$.

(d) $|\mathrm{Hom}(A,B)| = |\mathrm{Hom}(B,A)|$.

(e) Genau dann ist f surjektiv (bzw. injektiv), wenn f^* injektiv (bzw. surjektiv) ist.

(f) Die Anzahl der zu B isomorphen Untergruppen von A ist die Anzahl der zu B isomorphen Faktorgruppen von A.

Aufgabe 77 (Alperin-Kuo)**.** Zeigen Sie $\exp(M(G))\exp(G) \mid |G|$ für jede endliche Gruppe G.
Hinweis: Wenden Sie Satz 11.18 auf eine zyklische p-Untergruppe $H \leq G$ an.

Aufgabe 78. Sei $Z \leq \mathrm{Z}(G)$ mit $\mathrm{ggT}(|Z|, |G/Z|) = 1$. Zeigen Sie:

(a) $H^2(G/Z, Z) = 1$.

(b) Z besitzt ein Komplement in G.
Bemerkung: Damit kann man den Satz von Schur-Zassenhaus beweisen.

Aufgabe 79. Sei A eine abelsche Gruppe und $\alpha\colon G \to \mathrm{Aut}(A)$, $x \to \alpha_x$ ein Homomorphismus. Wir definieren

$$Z^2_\alpha(G,A) := \big\{\gamma\colon G \times G \to A : \forall x,y,z \in G : \gamma(x,y)\gamma(xy,z) = \alpha_x(\gamma(y,z))\gamma(x,yz)\big\}.$$

Zeigen Sie:

(a) Für $\gamma \in Z^2_\alpha(G,A)$ wird $\widehat{G}_\gamma := A \times G$ mit der Verknüpfung

$$(a,x) * (b,y) := (a\alpha_x(b)\gamma(x,y), xy)$$

zu einer Gruppe.

(b) $A_\gamma := A \times 1$ ist ein zu A isomorpher Normalteiler von $\widehat{G}_\gamma$ und $G_\gamma/A_\gamma \cong G$.

(c) Sei umgekehrt $\widehat{G}$ mit $A \trianglelefteq \widehat{G}$ und $\widehat{G}/A \cong G$. Sei $\alpha\colon G \to \mathrm{Aut}(A)$ die Konjugationsoperation von $\widehat{G}$ auf A. Zeigen Sie, dass ein $\gamma \in Z^2_\alpha(G, A)$ mit $\widehat{G} \cong \widehat{G}_\gamma$ existiert.

Bemerkung: Für Schur-Erweiterungen ist α die triviale Abbildung.

A Anhang

A.1 Halls Charakterisierung auflösbarer Gruppen

Bemerkung A.1. Burnsides p^aq^b-Satz besagt, dass jede Gruppe der Ordnung p^aq^b für Primzahlen p und q auflösbar ist. Man beweist diesen Satz üblicherweise in der Darstellungstheorie oder Charaktertheorie,[25] auch wenn es (aufwendige) rein gruppentheoretische Beweise gibt. Wir benutzen diesen Satz, um eine Umkehrung von Satz 5.35 zu beweisen.

Lemma A.2. *Seien H_1, H_2, H_3 auflösbare Untergruppen einer Gruppe G mit $G = H_1H_2 = H_1H_3$ und* $\mathrm{ggT}(|G : H_2|, |G : H_3|) = 1$. *Dann ist G auflösbar.*

Beweis. Im Fall $H_1 = 1$ ist $G = H_2$ auflösbar. Sei also $H_1 \neq 1$ und sei A ein minimaler Normalteiler von H_1. Da H_1 auflösbar ist, ist A eine elementarabelsche p-Gruppe. Wegen $\mathrm{ggT}(|G : H_2|, |G : H_3|) = 1$ können wir o. B. d. A. annehmen, dass p kein Teiler von $|G : H_2|$ ist. Dann enthält H_2 eine p-Sylowgruppe von G. Nach Sylow existiert $g \in G$ mit $A \leq gH_2g^{-1}$. Wegen $G = H_1H_2$ dürfen wir $g \in H_1$ annehmen. Dann ist $A = g^{-1}Ag \leq H_2$ und $N := A^G = A^{H_1H_2} = A^{H_2} \leq H_2$. Mit H_2 ist auch N auflösbar. Offenbar erfüllen H_iN/N für $i = 1, 2, 3$ die gleichen Voraussetzungen wie H_i. Nach Induktion nach $|G|$ ist also G/N auflösbar und damit auch G. □

Satz A.3 (Hall)**.** *Für jede endliche Gruppe G sind die folgenden Aussagen äquivalent:*

(1) G ist auflösbar.

(2) Für jede Primzahl p besitzt G eine p'-Hallgruppe.

(3) G besitzt ein Sylowsystem.

Beweis.

(1) ⇒ (2): Satz 5.35

(2) ⇒ (3): Lemma 5.39

(3) ⇒ (1): Sei $(P_1, \ldots, P_n)$ ein Sylowsystem von G. Im Fall $n \leq 2$ ist G auflösbar nach Burnsides p^aq^b-Satz. Sei also $n \geq 3$ und $H_i := \prod_{j \neq i} P_j$ für $i = 1, 2, 3$. Nach Lemma 5.39 ist H_i eine p_i'-Hallgruppe von G. Offenbar ist $\{P_j : j \neq i\}$ ein Sylowsystem von H_i. Durch Induktion nach n können wir annehmen, dass H_i auflösbar ist. Außerdem gilt $G = H_1H_2 = H_1H_3$ sowie $\mathrm{ggT}(|G : H_2|, |G : H_3|) = 1$. Aus Lemma A.2 folgt die Behauptung. □

[25] Siehe Skripte

Tabelle 1: Anzahl von Gruppen der Ordnung ≤ 2000

	1	2	3	4	5	6	7	8	9	10

A.2 Tabellen

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

Tabelle 1: Anzahl von Gruppen der Ordnung ≤ 2000

	1	2	3	4	5	6	7	8	9	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
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[26]	4	66	2	5	19	4
1030+	1	54	1	4	2	11	1	4	1	231

[26] 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
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
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

Tabelle 1: Anzahl von Gruppen der Ordnung ≤ 2000

	1	2	3	4	5	6	7	8	9	10
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
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