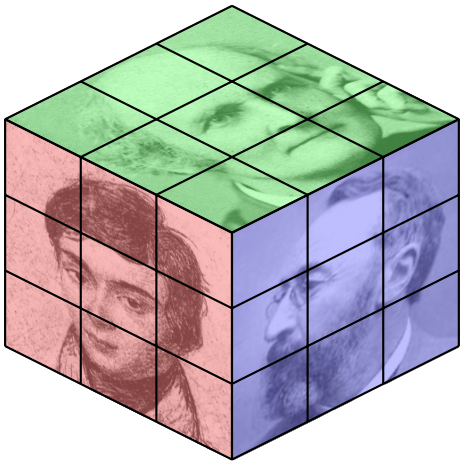
Group Theory

Lecture notes winter semester 2020/21

Benjamin Sambale
Leibniz Universität Hannover

Version: April 4, 2026



Contents

Warning: This is an AI-translated version of my German lecture notes, performed by *Gemini 3 Flash Preview*. I have not checked whether Gemini introduced errors. Use with care!

Preface

This script originated from lectures at the Technical University of Kaiserslautern (winter semester 2016/17) and at the Leibniz University Hannover (winter semester 2020/21). This lecture is primarily aimed at Bachelor and Master students of mathematics. Knowledge of Algebra 1 & 2 is assumed, whereby the most important results are reviewed in the first chapter without proofs (proofs can be found, for example, in my Algebra notes). Subsequently, some additions have been included: among others, theorems of Gaschütz, Rose, and Shemetkov on complements as well as Alperin's fusion theorem, Puig's hyperfocal theorem, and Tate's transfer theorem with a relatively unknown proof by Brandis.

I thank Stefanos Aivazidis, Annika Bartelt, Luca Blaas, Jonathan Gruber, Gereon Koßmann, Julia Liebner, Gabriel Navarro, Scheima Sara Obeidi and Claude Sonnet (4.6) for valuable error reports.

Literature:

- H. Kurzweil, B. Stellmacher, *The Theory of Finite Groups*, Springer, Berlin, 2004[1]
- B. Huppert, *Finite Groups I*, Springer, Cham, 2025 [2]
- I. M. Isaacs, *Finite group theory*, Amer. Math. Soc., R.I., 2008[3]
- 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 Subgroups, Normal Subgroups and Quotient Groups

In this chapter, we review some results from the Algebra lecture.

Definition 1.1. A *group* G is a set together with a map $G \times G \to G$, $(x, y) \mapsto xy$, such that the following properties hold:[4]

- $\forall x, y, z \in G : (xy)z = x(yz)$ (*associativity*).
- $\exists e \in G : \forall x \in G : ex = x$ (*(left) neutral element*).
- $\forall x \in G : \exists y \in G : yx = e$ (*(left) inverse elements*).

If additionally

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

then G is called *abelian*. The *order* of G is the cardinality $|G|$.

[1] The subtitle "An introduction" is an understatement. German original from 1998.
[2] A classic with almost 800 pages. German original from 1967.
[3] Beginner-friendly with very detailed proofs. For my taste too detailed – no personal "aha" effects remain.
[4] One can also define groups with a single axiom, see [W. McCune and A. D. Sands, *Computer and Human Reasoning: Single Implicative Axioms for Groups and for Abelian Groups*, Amer. Math. Monthly 103 (1996), 888–892].

Remark 1.2.

(i) In the following, let G always be a group.

(ii) From the associative law, it follows inductively that a product of finitely many group elements does not depend on the parenthesization (but it does depend on the order). For example,

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

holds for $a, b, c, d \in G$.[5]

(iii) For $x \in G$ there exist $y, z \in G$ with $yx = e = zy$. It follows

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

and $xe = x(yx) = (xy)x = ex = x$. Therefore, e is also right neutral and left inverse elements are right inverse. If $e' \in G$ is also a neutral element, then $e' = e'e = e$ holds. Thus e is uniquely determined and we write $e = 1_G = 1$. Now let $y' \in G$ with $y'x = e$. Then $y' = y'e = y'(xy) = (y'x)y = ey = y$. Consequently, x has exactly one inverse and we write $y = x^{-1}$. Obviously, $(x^{-1})^{-1} = y^{-1} = z = x$.

(iv) Attention: The existence of inverse elements is *not* equivalent to $\forall x \in G : \exists y \in G : xy = e$ (right inverse). Consider for example $G = \left\{ \left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 1 \\ 0 & 0 \end{smallmatrix}\right) \right\}$ with respect to matrix multiplication. One must therefore require "left neutral + left inverse" or "right neutral + right inverse".

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

(vi) For $x \in G$ and $k \in \mathbb{Z}$ we define

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

Then certainly $x^m x^n = x^{m+n}$ and $(x^m)^n = x^{mn}$ for $n, m \in \mathbb{Z}$. One calls $\inf\{n \geq 1 : x^n = 1\}$ the *order* of x. Here, let $\inf \varnothing = \infty$. If G consists of powers of x, then G is called *cyclic*. In this case, G is also abelian. Elements of order 2 are called *involutions*.

Example 1.3.

(i) The *trivial* group $G = \{1\}$. We then also write $G = 1$.

(ii) The integers $\mathbb{Z}$ form an abelian group with respect to addition. The neutral element is 0. In contrast, $\mathbb{Z}$ is *not* a group with respect to multiplication.

(iii) The invertible $n \times n$ matrices over a field K form the *general linear group* $\mathrm{GL}(n, K)$ with respect to matrix multiplication. The neutral element is the identity matrix 1_n. We have $\mathrm{GL}(1, K) = K^\times = K \setminus \{0\}$. For $n \geq 2$, $\mathrm{GL}(n, K)$ is non-abelian. If $|K| = q < \infty$, we write $\mathrm{GL}(n, q) := \mathrm{GL}(n, K)$ (this is well-defined, since there is only one field with q elements up to isomorphism).

(iv) The bijections of a set Ω form the *symmetric group* $\mathrm{Sym}(\Omega)$ with respect to composition of mappings, with neutral element id_Ω. The elements of $\mathrm{Sym}(\Omega)$ are called *permutations*. For $\Omega = \{1, \dots, n\}$ we write $S_n := \mathrm{Sym}(\Omega)$. Then $|S_n| = n!$ holds.

[5] The number of different parenthesizations of n factors is the *Catalan number* $\frac{1}{n}\binom{2n-2}{n-1}$. See lecture notes on discrete mathematics.

(v) For every non-empty family of groups $(G_i)_{i\in I}$, the *direct product* $\bigtimes_{i\in I} G_i$ is a group with $(g_i)_{i\in I}(h_i)_{i\in I} := (g_ih_i)_{i\in I}$ for $(g_i)_{i\in I}, (h_i)_{i\in I} \in \bigtimes_{i\in I} G_i$. For $I = \{1,\dots,n\}$ one also writes $G_1 \times \dots \times G_n$ and G^n, if $G := G_1 = \dots = G_n$.

Definition 1.4. A non-empty subset $H \subseteq G$ with $xy^{-1} \in H$ for all $x, y \in H$ is called a *subgroup* of G. We then write $H \leq G$ and $H < G$, if $H \neq G$. The sets of the form $gH := \{gh : h \in H\}$ are called (*left*) *cosets* of H in G. The set of all left cosets is $G/H := \{gH : g \in G\}$ and $|G : H| := |G/H|$ is the *index* of H in G.

Remark 1.5. One easily shows that H with the restricted operation is then also a group. If G is abelian, then so is H. If $K \leq H$, then $K \leq G$ also holds.

Example 1.6.

(i) Every group G possesses the subgroups 1 and G. A subgroup $H < G$ is called *maximal*, if no subgroup K with $H < K < G$ exists. Analogously, one defines *minimal* subgroups.

(ii) For $H_i \leq G$, $\bigcap_{i\in I} H_i \leq G$.

(iii) For $U \subseteq G$,
$$\langle U\rangle := \bigcap_{U\subseteq H\leq G} H \leq G$$
is the subgroup *generated* by U. Obviously, $\langle U\rangle$ consists of the elements of the form $x_1^{\pm 1} \dots x_n^{\pm 1}$ with $x_1, \dots, x_n \in U$ (this corresponds to linear combinations in linear algebra). In the case $\langle U\rangle = G$, U is a *generating set* of G. If additionally $U = \{x_1, \dots, x_n\}$, then one writes $G = \langle x_1, \dots, x_n\rangle$ instead of $\langle U\rangle$. In this case, G is *finitely generated*. If $|U| \leq 1$, then G is cyclic. In general, $|\langle x\rangle|$ is the order of x.

(iv) For $n \in \mathbb{Z}$, $n\mathbb{Z} \leq \mathbb{Z}$.

(v) Every finite subgroup of the multiplicative group of a field K is cyclic (Algebra). For $n \in \mathbb{N}$, $K^\times$ possesses at most one subgroup of order n; this consists of the n-th roots of unity.

(vi) The *special linear group* is $\mathrm{SL}(n, K) := \{A \in \mathrm{GL}(n, K) : \det(A) = 1\} \leq \mathrm{GL}(n, K)$.

(vii) The *alternating group* $\mathrm{Alt}(\Omega) := \{\sigma \in \mathrm{Sym}(\Omega) : \mathrm{sgn}(\sigma) = 1\} \leq \mathrm{Sym}(\Omega)$ for a non-empty, finite set Ω. We set $A_n := \mathrm{Alt}(\{1, \dots, n\})$ for $n \geq 1$.

Theorem 1.7 (Lagrange)**.** *For a group G and $H \leq G$, it holds that*
$$\boxed{|G| = |G : H||H|.}$$
In particular, $|H|$ and $|G : H|$ are divisors of $|G|$, if $|G| < \infty$.

Proof. Algebra. □

Definition 1.8. For $X, Y \subseteq G$, let $XY := \{xy : x \in X, y \in Y\}$ and $X^{-1} := \{x^{-1} : x \in X\}$.

Lemma 1.9. *For $U, V, W \leq G$, it holds that*

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

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

(iii) $\boxed{|UV||U \cap V| = |U||V|}$ (*product formula*).

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

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

(vi) *If* $|G : U|$ *and* $|G : V|$ *are finite and coprime, then* $|G : U \cap V| = |G : U||G : V|$ *and* $G = UV$.

Proof. Exercise 2. □

Theorem 1.10. *If G is finitely generated and $H \leq G$ with $|G : H| < \infty$, then H is also finitely generated.*

Proof. Let $X = X^{-1}$ be a finite generating set of G and R a transversal for G/H with $1 \in R$. For $x \in X$ and $r \in R$ there exist $\alpha(x, r) \in H$ and $\gamma(x, r) \in R$ with $xr = \gamma(x, r)\alpha(x, r)$. Every element in H has the form $h = x_1 \dots x_n$ with $x_1, \dots, x_n \in X$. It holds that

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

Because of $h \in H$, it holds that $\gamma(x_1, \dots) = 1$. It follows that $H = \langle \alpha(x, r) : x \in X, r \in R \rangle$. □

Remark 1.11. The above proof shows that one can generate H with $|X||G : H|$ elements. The Reidemeister-Schreier theorem provides the optimal bound $|G : H|(|X| - 1) + 1$ for the number of generators (without proof).

Definition 1.12. A subgroup $H \leq G$ is called a *normal subgroup* of G if $ghg^{-1} \in H$ holds for all $g \in G$ and $h \in H$. One also says: H is *normal* in G. In this case we write $H \trianglelefteq G$ and $H \triangleleft G$ if $H < G$.

Remark 1.13.

(i) $H \leq G$ is normal if and only if $gH = Hg$ holds for all $g \in G$.

(ii) For $N \trianglelefteq G$, G/N becomes a group via $(xN)(yN) := xyN$ for $x, y \in G$. One then calls G/N the *factor group* of G by N (although "quotient group" would be more appropriate). If G is abelian, then so is G/N. We also write the equality $xN = yN$ in the form $x \equiv y \pmod{N}$.

Example 1.14.

(i) Subgroups of abelian groups are always normal. In particular, $n\mathbb{Z} \trianglelefteq \mathbb{Z}$ and $\mathbb{Z}/n\mathbb{Z}$ is cyclic of order n if $n > 0$.

(ii) Subgroups with index 2 are normal (Exercise 1).

(iii) For $H \leq G$, $H^G := \langle \bigcup_{g \in G} gHg^{-1} \rangle$ is the *normal closure* of H in G. This is the "smallest" normal subgroup of G containing H. Analogously, $H_G := \bigcap_{g \in G} gHg^{-1}$ is the *core* of H in G, i. e. the "largest" normal subgroup of G contained in H.

(iv) For every family of normal subgroups $(N_i)_{i \in I}$ of G, $\bigcap_{i \in I} N_i \trianglelefteq G$ and $\langle N_i : i \in I \rangle \trianglelefteq G$. For $N, M \trianglelefteq G$,

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

according to Lemma 1.9.

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

Definition 1.15. A map $f\colon G \to H$ for groups G and H is called

(i) *homomorphism*, if $f(xy) = f(x)f(y)$ holds for $x, y \in G$.

(ii) *monomorphism*, if f is an injective homomorphism.

(iii) *epimorphism*, if f is a surjective homomorphism.

(iv) *isomorphism*, if f is a bijective homomorphism.

(v) *endomorphism*, if f is a homomorphism with $G = H$.

(vi) *automorphism*, if f is a bijective endomorphism.

Example 1.16.

(i) The *trivial* homomorphism $G \to H$, $g \mapsto 1$ and the *trivial* automorphism id_G.

(ii) For $H \leq G$, the inclusion map $H \to G$, $h \mapsto h$ is a monomorphism.

(iii) For groups G, H, the *projection* $G \times H \to G$, $(g,h) \mapsto g$ is an epimorphism.

(iv) If $f\colon G \to H$ is a homomorphism and $U \leq G$, then the restriction $f_{|U}\colon U \to H$ is also a homomorphism.

(v) For $N \trianglelefteq G$, there is the *canonical* epimorphism $G \to G/N$, $g \mapsto gN$.

Remark 1.17.

(i) For a homomorphism $f\colon G \to H$, it clearly holds that $f(1_G) = 1_H$ and $f(x^{-1}) = f(x)^{-1}$ for $x \in G$. If $g\colon H \to K$ is another homomorphism, then $g \circ f\colon G \to K$ is also a homomorphism. For $U \leq G$ and $V \leq H$, we have $f(U) \leq H$ and $f^{-1}(V) := \{x \in G : f(x) \in V\} \leq G$. For $U \trianglelefteq G$, it holds that $f(U) \trianglelefteq f(G)$, but not necessarily $f(U) \trianglelefteq H$! For $V \trianglelefteq H$, however, it is always the case that $f^{-1}(V) \trianglelefteq G$.[6] In particular, $f(G) \leq H$ and $\mathrm{Ker}(f) = f^{-1}(1) \trianglelefteq G$ (*kernel* of f). f is injective if and only if $\mathrm{Ker}(f) = 1$ holds.

(ii) If $f\colon G \to H$ is an isomorphism, then so is $f^{-1}\colon H \to G$. One then says G and H are *isomorphic* and writes $G \cong H$. Clearly, the isomorphism of groups is an equivalence relation. Since isomorphic groups have the same properties, one is usually only interested in groups up to isomorphism.

(iii) According to (ii), the automorphisms of G form a subgroup $\mathrm{Aut}(G) \leq \mathrm{Sym}(G)$. One calls $\mathrm{Aut}(G)$ the *automorphism group* of G. For $x \in G$, the map $f_x\colon G \to G$, $g \mapsto xgx^{-1}$ is an *inner* automorphism of G. Because of $f_x \circ f_y = f_{xy}$ for $x, y \in G$, $f\colon G \to \mathrm{Aut}(G)$, $x \mapsto f_x$ is a homomorphism with image $\mathrm{Inn}(G) := f(G)$. For $\alpha \in \mathrm{Aut}(G)$ and $g, x \in G$, it holds that

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

Therefore, $\mathrm{Inn}(G) \trianglelefteq \mathrm{Aut}(G)$. One calls $\mathrm{Out}(G) := \mathrm{Aut}(G)/\mathrm{Inn}(G)$ the *outer* automorphism group of G.

Theorem 1.18.

(i) (Homomorphism Theorem) For a homomorphism $f\colon G \to H$, it holds that $\boxed{G/\mathrm{Ker}(f) \cong f(G).}$

[6] In analysis, preimages of open sets under continuous maps are again open, but images are not necessarily.

(ii) (*Correspondence Theorem*) *For $N \trianglelefteq G$, the canonical epimorphism $G \to G/N$ induces a bijection between the set of subgroups $H \leq G$ with $N \leq H$ and the set of subgroups of G/N.*

(iii) (*1st Isomorphism Theorem*) *For $H \leq G$ and $N \trianglelefteq G$, it holds that $N \trianglelefteq HN \leq G$, $H \cap N \trianglelefteq H$ and*

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

(iv) (*2nd Isomorphism Theorem*) *For $N \trianglelefteq G$ and $N \leq H \leq G$, $H \trianglelefteq G$ holds if and only if $H/N \trianglelefteq G/N$. In this case,* $\boxed{G/H \cong (G/N)/(H/N).}$

Proof. Algebra. □

Definition 1.19. An *action* of G on a non-empty set Ω is a map $G \times \Omega \to \Omega$, $(x, \omega) \mapsto {}^x\omega$ with the following properties:

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

One then also says G *acts* on Ω or Ω is a *G-set*. The cardinality $|\Omega|$ is the *degree* of the action. Provided the action is clear in the context, we will in the following sometimes also assign properties of actions to the corresponding groups (e. g. the degree of G).

Remark 1.20.

(i) If G acts on Ω, then the map $f_x \colon \Omega \to \Omega$, $\omega \mapsto {}^x\omega$ for $x \in G$ is a bijection, i. e. $f_x \in \mathrm{Sym}(\Omega)$. Furthermore, the map $f \colon G \to \mathrm{Sym}(\Omega)$, $x \mapsto f_x$ is a homomorphism.

Conversely, let a homomorphism $f \colon G \to \mathrm{Sym}(\Omega)$, $x \mapsto f_x$ be given. Then one obviously obtains an action by ${}^x\omega := f_x(\omega)$. Actions are therefore nothing else than homomorphisms into the symmetric group. The action is called *faithful* (resp. *trivial*) if $\mathrm{Ker}(f) = 1$ (resp. $\mathrm{Ker}(f) = G$) holds.

(ii) By

$$\alpha \sim \beta :\Longleftrightarrow \exists x \in G : {}^x\alpha = \beta \qquad (\alpha, \beta \in \Omega)$$

one obtains an equivalence relation on Ω. The equivalence classes are called *orbits*. For an orbit $\Delta \subseteq \Omega$, $|\Delta|$ is the *length* of Δ. For $\omega \in \Omega$, let ${}^G\omega$ be the orbit containing ω. If only one orbit exists, the action is *transitive*.

(iii) For $\omega \in \Omega$,

$$G_\omega := \{x \in G : {}^x\omega = \omega\} \leq G$$

is the *stabilizer* of ω in G. For $g \in G$, it holds that

$$G_{g_\omega} = \{x \in G : {}^{xg}\omega = {}^g\omega\} = \{x \in G : g^{-1}xg \in G_\omega\} = gG_\omega g^{-1}.$$

Example 1.21.

(i) Every subgroup $H \leq G$ acts on G by left multiplication, i. e. ${}^hg := hg$ for $g \in G$, $h \in H$. The orbits Hg are called *right cosets*. Analogously, H acts from the right by ${}^hg := gh^{-1}$ and one obtains left cosets gH. Because of $gH = (gHg^{-1})g$, every left coset is also a right coset, although not necessarily with respect to the same subgroup.

(ii) Let $H, K \leq G$. Then $H \times K$ acts on G by ${}^{(h,k)}g := hgk^{-1}$. The orbits have the form HgK and are called *double cosets* of G by (H, K). If H (resp. K) is normal, then $HgK = gHK$ is a left coset (resp. right coset). In general, $|HgK| = |H(gKg^{-1})| = |H : H \cap gKg^{-1}||K|$ is not a divisor of $|G|$.

(iii) G acts on itself by *conjugation* ${}^{x}g := xgx^{-1}$ for $x, g \in G$. The orbits are called *conjugacy classes* and the stabilizer of $x \in G$ is the *centralizer*

$$\mathrm{C}_G(x) := \{g \in G : gx = xg\}.$$

Two elements in the same conjugacy class are called *conjugate*. The kernel of the action is the *center* $\mathrm{Z}(G) := \{x \in G : \forall y \in G : xy = yx\}$ of G and the image is $\mathrm{Inn}(G)$. According to the isomorphism theorem,

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

(iv) Analogously, G acts by conjugation on the set of subgroups of G. The orbits are also called conjugacy classes here and the stabilizer of $H \leq G$ is the *normalizer*

$$\mathrm{N}_G(H) := \{x \in G : xHx^{-1} = H\}.$$

The orbits of length 1 correspond to the normal subgroups. More generally, $\mathrm{N}_G(H)$ acts by conjugation on H with kernel $\mathrm{C}_G(H) := \bigcap_{h \in H} \mathrm{C}_G(h)$. In particular, $\mathrm{N}_G(H)/\mathrm{C}_G(H)$ is isomorphic to a subgroup of $\mathrm{Aut}(H)$.

Theorem 1.22. *For an action of G on Ω and $\omega \in \Omega$, the map $G/G_\omega \to {}^{G}\omega$, $xG_\omega \mapsto {}^{x}\omega$ is well-defined and bijective. In particular,* $\boxed{|G/G_\omega| = |{}^{G}\omega|.}$ *If $|G| < \infty$, then every orbit length is a divisor of $|G|$. If G is additionally transitive, then $|\Omega|$ is a divisor of $|G|$.*

Proof. Well-definedness and injectivity:

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

Surjectivity is obvious. The last two statements follow from Lagrange's theorem. □

Remark 1.23. If $(\omega_i)_{i \in I}$ are representatives for the orbits of G on Ω, then the *orbit equation* holds:

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

In the special case of the conjugation action, one obtains the *class equation*

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

where $(x_i)_{i \in I}$ is a transversal for the conjugation classes of G. If $J := \{i \in I : x_i \notin \mathrm{Z}(G)\}$, then also

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

Theorem 1.24 (Frattini argument)**.** *Given an action of G on Ω and $H \leq G$. If H acts transitively on Ω, then $G = HG_\omega$ for all $\omega \in \Omega$.*

Proof. Let $g \in G$ be arbitrary. Then there exists an $h \in H$ with ${}^g\omega = {}^h\omega$. Thus $h^{-1}g \in G_\omega$ and $g = h(h^{-1}g) \in HG_\omega$. Conversely, $HG_\omega \subseteq G$ certainly holds as well. □

Remark 1.25. If every non-trivial element in G has infinite order, then G is called *torsion-free*. If, on the other hand, every element has finite order, then G is a *torsion group*. If the orders of the elements are additionally bounded, then G is *periodic* and

$$\exp(G) := \min\{k \geq 1 : \forall x \in G : x^k = 1\}$$

is the *exponent* of G. Burnside asked in 1902 whether every finitely generated periodic group is finite (*Burnside problem*). It is known today that this is false in general. In fact, there are infinite groups in which even every proper subgroup has order p for very large prime numbers p (*Tarski monster*). On the other hand, it is not known whether every group with two generators and exponent 5 is finite. Solved, however, is the *restricted Burnside problem*: For $d, e \in \mathbb{N}$, there are only finitely many finite groups with d generators and exponent e. Zelmanov received the *Fields Medal* for this.

2 Abelian and solvable groups

Lemma 2.1. *Let $x \in G$ with $n := |\langle x \rangle| < \infty$. Then*

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

for $k \in \mathbb{Z}$. In particular, $x^k = 1$ if and only if $n \mid k$. For $y \in \mathrm{C}_G(x)$ with $m := |\langle y \rangle| < \infty$ and $\gcd(n,m) = 1$, it holds that $|\langle xy \rangle| = mn$.

Proof. For $l := \frac{n}{\gcd(n,k)} \geq 1$, it holds that $(x^k)^l = (x^n)^{\frac{k}{\gcd(n,k)}} = 1$. Thus $s := |\langle x^k \rangle| \leq l$. Conversely, $x^{ks} = 1$. Division with remainder yields $a \in \mathbb{Z}$ and $0 \leq r < n$ with $ks = an + r$. It follows that

$$x^r = x^r(x^n)^a = x^{an+r} = x^{ks} = 1$$

and $r = 0$. Thus $n \mid ks$. Now l is a divisor of $\frac{k}{\gcd(n,k)}s$, but coprime to $\frac{k}{\gcd(n,k)}$. This shows $l \mid s$ and $l = s$. It follows that

$$x^k = 1 \iff n = \gcd(n,k) \iff n \mid k.$$

Now let $y \in \mathrm{C}_G(x)$ be as specified. Because of $xy = yx$, we have $(xy)^{mn} = (x^n)^m(y^m)^n = 1$, thus $s := |\langle xy \rangle| \leq mn$. According to the Euclidean algorithm, there exist $a, b \in \mathbb{Z}$ with $an + bm = 1$. It then holds that

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

Lagrange shows $n = |\langle x \rangle| \mid s$ and analogously $m = |\langle y \rangle| \mid s$. Because $\gcd(n,m) = 1$, we also have $nm \mid s$ and $s = mn$. □

Definition 2.2. We denote a cyclic group of order $n \in \mathbb{N} \cup \{\infty\}$ by C_n.

Remark 2.3.

(i) For $G = \langle g \rangle \cong C_n$, the map $\mathbb{Z} \to G$, $i \mapsto g^i$ is an epimorphism with kernel $n\mathbb{Z}$ according to Lemma 2.1. This shows $C_n \cong \mathbb{Z}/n\mathbb{Z}$ and $C_\infty \cong \mathbb{Z}$.

(ii) From Lemma 2.1 it follows that $C_n \times C_m \cong C_{nm}$ if $\gcd(n,m) = 1$ (*Chinese Remainder Theorem*).

Theorem 2.4. *Let $n \in \mathbb{N}$.*

(i) For each $d \mid n$, C_n has exactly one subgroup (or factor group) of order d. This is isomorphic to C_d.

(ii) $\mathrm{Aut}(C_n) \cong (\mathbb{Z}/n\mathbb{Z})^\times$. In particular, $\mathrm{Aut}(C_n)$ is abelian of order $\varphi(n)$ (Euler's φ-function).

Proof. Let $\langle x \rangle \cong C_n$.

(i) For $d \mid n$, $\langle x^{n/d} \rangle$ is a subgroup of order d according to Lemma 2.1. Conversely, let $H \leq \langle x \rangle$ with $d = |H| \,\big|\, n$. According to Lagrange, $x^{n/d}H = (xH)^{|\langle x \rangle / H|} = H$ and $x^{n/d} \in H$. This shows $H = \langle x^{n/d} \rangle$. Because of $\langle x \rangle / H = \langle xH \rangle \cong C_{n/d}$, the claim about factor groups is also clear.

(ii) For $\alpha \in \mathrm{Aut}(\langle x \rangle)$, $\alpha(x) = x^i$ with $i \in \mathbb{Z}$. In the case $\gcd(n, i) > 1$, $\langle x^i \rangle < \langle x \rangle$ would hold according to Lemma 2.1. One thus obtains a map $\Phi \colon \mathrm{Aut}(\langle x \rangle) \to (\mathbb{Z}/n\mathbb{Z})^\times$, $\alpha \mapsto i + n\mathbb{Z}$. For $\beta \in \mathrm{Aut}(\langle x \rangle)$ with $\beta(x) = x^j$, it holds that $\alpha(\beta(x)) = \alpha(x^j) = \alpha(x)^j = x^{ij}$. This shows that Φ is a homomorphism. If $i + n\mathbb{Z} = 1 + n\mathbb{Z}$, then $\alpha(x) = x^i = x$ and $\alpha = 1$. Thus Φ is injective. Conversely, if $i + n\mathbb{Z} \in (\mathbb{Z}/n\mathbb{Z})^\times$ is given, one easily sees that the map $x \mapsto x^i$ induces an automorphism of $\langle x \rangle$. Thus Φ is an isomorphism. □

Lemma 2.5. *For $N, M \trianglelefteq G$ with $N \cap M = 1$, $xy = yx$ holds for all $x \in N$ and $y \in M$. This holds in particular if $\gcd(|N|, |M|) = 1$.*

Proof. For $x \in N$ and $y \in M$, it holds that

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

i.e., $xy = yx$. According to Lagrange, $|N \cap M|$ is a divisor of $\gcd(|N|, |M|)$. Therefore, the second statement follows from the first. □

Definition 2.6. One calls G a *direct sum* of normal subgroups $N_1, \ldots, N_k \trianglelefteq G$ if the following statements hold:

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

In this case, we write $G = N_1 \oplus \ldots \oplus N_k$. If $G \neq 1$ cannot be written as a direct sum of proper subgroups, then G is called *indecomposable*.

Lemma 2.7. *It holds that $G := N_1 \oplus \ldots \oplus N_k \cong N_1 \times \ldots \times N_k$.*

Proof. We show that the map

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

is an isomorphism. For $i > j$, by assumption $N_i \cap N_j \subseteq N_i \cap N_1 \ldots N_{i-1} = 1$. Lemma 2.5 shows $xy = yx$ for $x \in N_i$ and $y \in N_j$. Now let $x_i, y_i \in N_i$ for $i = 1, \ldots, k$. Then

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

Thus F is a homomorphism. Because of $G = N_1 \dots N_k$, F is surjective. Let $(x_1, \dots, x_k) \in \mathrm{Ker}(F)$. Suppose there exists $1 \leq l \leq k$ with $x_l \neq 1$. Let l be maximal. Then $x_l^{-1} = x_1 \dots x_{l-1} \in N_l \cap N_1 \dots N_{l-1} = 1$. Thus $\mathrm{Ker}(F) = 1$ and F is also injective. □

Remark 2.8.

(i) Obviously $G_1 \oplus G_2 = G_2 \oplus G_1$. Let $G = G_1 \oplus G_2 \oplus G_3$. Then certainly $G_1G_2 = G_1 \oplus G_2 \trianglelefteq G$ and $G = (G_1 \oplus G_2) \oplus G_3$. Conversely, let $G = (G_1 \oplus G_2) \oplus G_3$. Then $G_3 \subseteq \mathrm{C}_G(G_1G_2)$. This shows $G_1, G_2 \trianglelefteq G$ and $G = G_1 \oplus G_2 \oplus G_3$. Direct sums are therefore commutative and associative.

(ii) The summands of a direct sum are generally not uniquely determined. For example,

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

Furthermore, in Definition 2.6 the second condition cannot be replaced by $N_i \cap N_j = 1$ for $i \neq j$ (otherwise it would be $\langle (1,2) \rangle \oplus \langle (3,4) \rangle \oplus \langle (1,2)(3,4) \rangle$). The following theorem shows that the indecomposable summands of a finite group are uniquely determined up to order and isomorphism.

Theorem 2.9 (Krull-Schmidt)**.** *Let G be finite and*

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

with indecomposable groups $G_1, \dots, G_s, H_1, \dots, H_t$. Then for every i there exists a j with

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

In particular, $s = t$ and with suitable numbering $G_i \cong H_i$ for $i = 1, \dots, s$.

Proof (Kurosch). Induction on $|G|$. Wlog. let $i = 1$. Let $\pi_i \colon G \to H_i$ be the i-th projection of the second decomposition and $H_{i1} := \pi_i(G_1) \leq H_i$ for $i = 1, \dots, t$.

Case 1: There exists an i with $H_{i1} < H_i$.
Let $H := H_{11} \oplus \dots \oplus H_{t1} < G$. Because $g = \pi_1(g) \dots \pi_t(g)$ for all $g \in G_1$, it holds that $G_1 \leq H$. By Dedekind, $H = G_1 \oplus (G_2 \dots G_s \cap H)$. We decompose the H_{j1} into indecomposable factors. By induction, there exists an indecomposable summand K of H_{j1} that can be substituted for G_1, i. e. $H = K \oplus (G_2 \dots G_s \cap H)$ and $K \cap G_2 \dots G_s = 1$. Every element in K has the form $\pi_j(g_1)$ for some $g_1 \in G_1$. For $g \in G_2 \dots G_s$ it holds that

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

It follows that $K \leq \mathrm{C}_G(G_2 \dots G_s)$. From $|G_1| = |K|$ we obtain $G = K \oplus G_2 \oplus \dots \oplus G_s$. Again by Dedekind, $H_j = K \oplus (G_2 \dots G_s \cap H_j)$. Since H_j is indecomposable, $K = H_{j1} = H_j$ must hold.

Case 2: It holds that $G = H_{11} \oplus \dots \oplus H_{t1}$.
Then $|G_1| \geq |\pi_i(G_1)| = |H_{i1}| = |H_i|$ for $i = 1, \dots, t$. Let us consider the reverse projection $\rho_1 \colon G \to G_1$. Suppose $\rho_1(H_i) = G_1$ holds for some i. Then $G = H_iG_2 \dots G_s$ and because $|H_i| \leq |G_1|$ the sum must be direct. We can therefore assume $\rho_1(H_i) < G_1$ for $i = 1, \dots, t$. One can now, as in Case 1 (only with reversed roles), successively replace each H_i by a G_j (the assumption $\rho_1(H_i) < G_1$ remains preserved). The G_j used in this process must be pairwise distinct so that the sum remains direct. In order for the right side of the equation to have the correct size at the end, G_1 must also be used at some point. Suppose H_i is replaced by G_1. If one follows the argumentation of Case 1 up to the equation $K = H_{j1} = H_j$, one recognizes that this can only hold in the case $\rho_1(H_i) = G_1$. Contradiction.

Thus the first statement is proven. For the second claim, one observes that

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

holds. One can now replace each G_i one by one with an H_j. As explained in Case 2, one must use pairwise distinct H_j for this. In the end, all H_j must be used up so that the order is correct. This shows $s = t$. □

Remark 2.10. Infinite groups cannot necessarily be written as direct sums of indecomposable factors (Exercise 9). For finitely generated abelian groups, such a decomposition exists according to (ii) of the following theorem and the Krull-Schmidt theorem remains true.

Theorem 2.11 (Fundamental Theorem of Finitely Generated Abelian Groups)**.** *For a finitely generated abelian group G, the following hold:*

(i) There exist uniquely determined numbers $s, t \geq 0$ and $1 < d_1 \mid \dots \mid d_t$ with

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

(ii) There exist uniquely determined prime powers $1 < p_1^{a_1} \leq \dots \leq p_t^{a_t}$ and an $s \geq 0$ with

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

Proof.

(i) **Step 1:** Existence.
Let $x_1, \dots, x_r$ be a minimal generating system, i. e. G cannot be generated by $r-1$ elements. Since G is abelian, one can write every $g \in G$ in the form $g = x_1^{n_1}x_2^{n_2} \dots x_r^{n_r}$ with $n_1, \dots, n_r \in \mathbb{Z}$. An equation of the form $x_1^{n_1}x_2^{n_2} \dots x_r^{n_r} = 1$ is called a *relation*. If there is only the trivial relation with $n_1 = \dots = n_r = 0$, then $\mathbb{Z}^r \to G$, $(n_1, \dots, n_r) \mapsto x_1^{n_1}x_2^{n_2} \dots x_r^{n_r}$ is an isomorphism.

Assume now that non-trivial relations also exist. We choose $x_1, \dots, x_r$ among all minimal generating systems such that a relation with minimal exponent $d_1 > 0$ holds.Wlog. let $x_1^{d_1}x_2^{n_2} \dots x_r^{n_r} = 1$. In the case $r = 1$, $G \cong C_{d_1}$. So let $r > 1$. We show $d_1 \mid n_2$. Division with remainder yields $n_2 = qd_1 + u$ with $0 \leq u < d_1$. The relation becomes

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

Since one can write every element $x_1^{l_1} \dots x_r^{l_r}$ also in the form $(x_1x_2^q)^{l_1}x_2^{l_2-ql_1}x_3^{l_3} \dots x_r^{l_r}$, $x_1x_2^q, x_2, \dots, x_r$ is also a minimal generating system. From the choice of d_1 as well as (2.1) it follows that $u = 0$ and thus $d_1 \mid n_2$. Analogously one shows $d_1 \mid n_3, \dots, d_1 \mid n_r$. We write $n_i = q_i d_1$ for $i = 3, \dots, r$. Setting $z := x_1x_2^q x_3^{q_3} \dots x_r^{q_r}$, then $z, x_2, \dots, x_r$ is again a minimal generating system and the relation becomes $1 = z^{d_1}$. Thus z has order d_1, because $1 = z^l = z^l x_2^0 \dots x_r^0$ with $0 < l < d_1$ would be a contradiction to the choice of d_1. With $H := \langle z \rangle$ and $G_1 := \langle x_2, \dots, x_r \rangle$ we have $G = HG_1$. In the case $H \cap G_1 \neq 1$ there would exist $l_1, \dots, l_r \in \mathbb{Z}$ with $1 \neq z^{l_1} = x_2^{l_2} \dots x_r^{l_r}$ and $0 < l_1 < d_1$. But then $z^{l_1}x_2^{-l_2} \dots x_r^{-l_r} = 1$ would be a contradiction to the choice of d_1. Consequently $H \cap G_1 = 1$ and $G = H \oplus G_1 \cong C_{d_1} \times G_1$.

Now one can repeat the process with G_1. Then $G_1 \cong C_\infty^{r-1}$ or $G_1 \cong C_{d_2} \times G_2$. In the first case $G \cong C_\infty^{r-1} \times C_{d_1}$ and we are done. In the second case $G \cong C_{d_1} \times C_{d_2} \times G_2$, where d_2 appears as the exponent of a relation $y_2^{d_2}y_3^{n_3'} \dots y_r^{n_r'} = 1$ with a minimal generating system $y_2, \dots, y_r$ of G_1. Now $z, y_2, \dots, y_r$ is a minimal generating system of G and the relation $z^{d_1}y_2^{d_2}y_3^{n_3'} \dots y_r^{n_r'} = 1$

holds. As above one shows $d_1 \mid d_2$. One now iterates the process with G_2. In the end G has the desired form.

Step 2: Uniqueness.
Let $C_\infty^s \times C_{d_1} \times \ldots \times C_{d_t} \cong G \cong C_\infty^{s'} \times C_{e_1} \times \ldots \times C_{e_{t'}}$ with $d_1 \mid \ldots \mid d_t$ and $e_1 \mid \ldots \mid e_{t'}$. The elements of finite order form a subgroup $H \leq G$ with $C_{d_1} \times \ldots \times C_{d_t} \cong H \cong C_{e_1} \times \ldots \times C_{e_{t'}}$. Wlog. let $t \geq t'$. We argue by induction on $|H|$. Let

$$K := \{x \in H : x^{d_1} = 1\} \leq H.$$

Then $K \cong C_{d_1}^t$ and because of $t' \leq t$ it follows that $d_1 \mid e_1$. This also shows $t = t'$. Now

$$C_{\frac{d_2}{d_1}} \times \ldots \times C_{\frac{d_t}{d_1}} \cong H/K \cong C_{\frac{e_1}{d_1}} \times \ldots \times C_{\frac{e_t}{d_1}}.$$

Induction yields $d_i = e_i$ for $i = 1, \ldots, t$. We finally consider

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

For $\overline{G}_2 := \{x^2 : x \in \overline{G}\} \leq \overline{G}$ we have $2^s = |\overline{G}/\overline{G}_2| = 2^{s'}$ and $s = s'$.

(ii) If $d = p_1^{a_1} \ldots p_k^{a_k}$ is the prime factorization of d, then $C_d \cong C_{p_1^{a_1}} \times \ldots \times C_{p_k^{a_k}}$ by Remark 2.3. From (i) one thus obtains the decomposition in (ii). Cyclic groups of prime power order are indecomposable, since they contain only one subgroup of prime order. The uniqueness of the decomposition therefore follows from Krull-Schmidt. □

Example 2.12. It holds that $C_\infty \times C_2 \times C_6 \times C_{18} \cong C_\infty \times C_2^3 \times C_3 \times C_9$. On the other hand, $C_4 \ncong C_2^2$.

Definition 2.13.

(i) In the situation of Theorem 2.11, the elements of finite order of G form a subgroup isomorphic to $C_{d_1} \times \ldots \times C_{d_t}$, which is called the *torsion part* of G. The group C_∞^s is called the *free abelian group* of rank s.

(ii) A finite abelian group G is called *elementary abelian* if there exists a prime p with $x^p = 1$ for all $x \in G$.

Remark 2.14.

(i) Theorem 2.11 shows that the terms *torsion-free* and *free abelian* are equivalent for finitely generated groups. For infinitely generated abelian groups, this is in general false (Exercise 9).

(ii) According to Theorem 2.11, every elementary abelian group E has the form C_p^n for a prime p and $n \geq 0$. One can then regard E as a vector space over $\mathbb{F}_p$:

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

One calls $n = \dim_{\mathbb{F}_p} E$ the *rank* of E. Every automorphism of E is obviously also $\mathbb{F}_p$-linear. This shows $\mathrm{Aut}(E) \cong \mathrm{GL}(n, p)$.

Definition 2.15.

- A group $G \neq 1$ is called *simple* if 1 and G are the only normal subgroups of G (cf. prime number).

- A *subnormal series* σ of G is a sequence of subgroups $1 = G_0 \trianglelefteq G_1 \trianglelefteq \ldots \trianglelefteq G_k = G$ (we do not require $G_i \trianglelefteq G$). Here k is the *length* of σ. If the factors G_i/G_{i-1} are simple for $i = 1, \ldots, k$, then σ is a *composition series*.
- G is called *solvable* if a subnormal series with abelian factors exists.

Remark 2.16. Every finite group G possesses a composition series, because one can always refine the subnormal series $1 \leq G$ to a composition series.

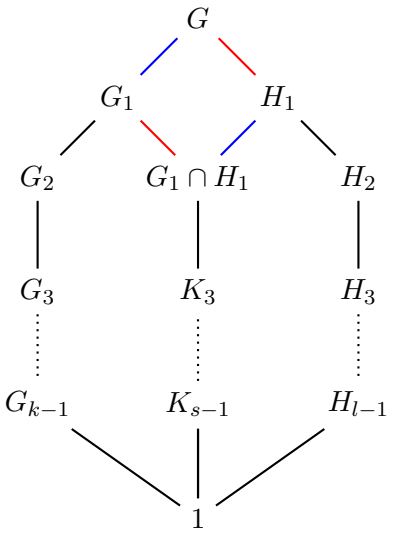
Theorem 2.17 (Jordan-Hölder). *Let* $1 = G_k \trianglelefteq \ldots \trianglelefteq G_0 = G$ *and* $1 = H_l \trianglelefteq \ldots \trianglelefteq H_0 = G$ *be composition series of a finite group* G. *Then* $k = l$ *and there exists a* $\pi \in S_k$ *with* $G_{i-1}/G_i \cong H_{\pi(i)-1}/H_{\pi(i)}$ *for* $i = 1, \ldots, k$. *One calls* $G_0/G_1, \ldots, G_{k-1}/G_k$ *the* composition factors *of* G.

Proof. Induction on $|G|$: Wlog. let $G \neq 1$. In the case $G_1 = H_1$, the assertion follows by induction. So let $G_1 \neq H_1$. Because $G_1, H_1 \trianglelefteq G$, it follows that $G_1 H_1 = H_1 G_1 \trianglelefteq G$. Since G/G_1 is simple, $G = G_1 H_1$ holds. The first isomorphism theorem shows

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

Let $1 = K_s \trianglelefteq \ldots \trianglelefteq K_2 = G_1 \cap H_1$ be any composition series. By induction, the composition series $G_k \trianglelefteq \ldots \trianglelefteq G_1$ and $K_s \trianglelefteq \ldots \trianglelefteq K_2 \trianglelefteq G_1$ then have the same length (i. e. $k = s$) and their factors are isomorphic (up to the order). Now the composition series $1 = K_k \trianglelefteq \ldots \trianglelefteq K_2 \trianglelefteq H_1$ and $1 = H_l \trianglelefteq \ldots \trianglelefteq H_1$ also have the same length with isomorphic factors. Thus $k = s = l$ and according to (2.2), the composition series

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



have isomorphic factors. □

Example 2.18.

(i) Every abelian group G is solvable via $1 = G_0 \trianglelefteq G_1 = G$.

(ii) Let G be solvable and simple. Then $1 \leq G$ is the only subnormal series and $G \cong G/1$ is abelian. For $x \in G \setminus \{1\}$, $\langle x \rangle \trianglelefteq G$ holds, so $G = \langle x \rangle$, i. e. G is cyclic. For every divisor d of $|G|$, there exists a normal subgroup of order d according to Theorem 2.4. This shows that $|G|$ is a prime number. Conversely, C_p is simple for every prime number p.

(iii) The group S_3 possesses only one composition series $1 \lhd A_3 \lhd S_3$.

(iv) C_∞ possesses no composition series, because according to (ii) the composition factors would have to be finite.

(v) The composition factors of a finite solvable group have prime order.

Remark 2.19.

(i) According to Jordan-Hölder, simple groups are the "prime numbers" of finite group theory. Every finite simple group belongs to one of the following families:[7]

- C_p (p prime),
- A_n for $n \geq 5$ (Theorem 6.38),
- Groups of "Lie type" (PSL(n,q) (Theorem 10.11), PSU(n,q) (Remark 10.12), $\ldots, E_8(q)$),
- 26 sporadic groups, the largest of which is the *Monster group* with approx. 10^{54} elements.

The proof of this classification (CFSG) was, with over 10,000 journal pages by over 100 mathematicians, one of the largest mathematical projects ever. Only in 2002 was the last known(!) gap in the proof closed.[8]

(ii) To classify all finite groups, one must investigate extensions of simple groups. Given simple groups $K_1, \ldots, K_n$, there is always a finite group with composition factors $K_1, \ldots, K_n$, namely $K_1 \times \ldots \times K_n$. On the other hand, there can be non-isomorphic groups with the same composition factors; for example, there are 49,487,367,289 groups of order 2^{10} with the same composition factors (C_2 with multiplicity 10). The extension problem is in general still unsolved.[9]

Definition 2.20. A *normal series* $\sigma : 1 = G_0 \trianglelefteq G_1 \trianglelefteq \ldots \trianglelefteq G_k = G$ is a subnormal series with $G_i \trianglelefteq G$ for $i = 0, \ldots, k$. Let additionally $G_0 < \ldots < G_k$. If σ cannot be refined further (i.e., there are no normal subgroups of G between G_i and G_{i+1}), then σ is a *chief series*. According to Exercise 15, the factors of a chief series are uniquely determined up to isomorphism and order. These are the *chief factors* of G.

Example 2.21. The normal series $1 \lhd V_4 \lhd A_4$ is a chief series of A_4, but not a composition series, since $V_4 \cong C_2^2$ is not simple.

Lemma 2.22. *Let $H \leq G$ and $N \trianglelefteq G$. If G is solvable, then so is H. G is solvable if and only if N and G/N are solvable.*

Proof. Let $1 = G_0 \trianglelefteq \ldots \trianglelefteq G_k = G$ with abelian factors. Then $1 = G_0 \cap H \trianglelefteq \ldots \trianglelefteq G_k \cap H = H$ with

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

Thus H is solvable. In particular, N is also solvable. Furthermore, $1 = G_0N/N \trianglelefteq \ldots \trianglelefteq G_kN/N = G/N$ holds with

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

Thus G/N is also solvable.

[7] The non-abelian simple groups of order $\leq 10^6$ are listed in Table 2.

[8] Current status: [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`]

[9] A "periodic table" of simple groups can be found here.

Conversely, assume that N and G/N are solvable. Then there exist $1 = N_0 \trianglelefteq \ldots \trianglelefteq N_k = N$ and $1 = G_0/N \trianglelefteq \ldots \trianglelefteq G_l/N = G/N$ with abelian factors. Concatenating the series, one obtains $1 = N_0 \trianglelefteq \ldots \trianglelefteq N_k = G_0 \trianglelefteq \ldots \trianglelefteq G_l = G$ with $G_i/G_{i-1} \cong (G_i/N)/(G_{i-1}/N)$. Thus all factors of this series are abelian and G is solvable. □

Example 2.23.

(i) If G and H are solvable, then so is $G \times H$.

(ii) If $N, M \trianglelefteq G$ are solvable, then so is NM, because $NM/N \cong M/M \cap N$. In a finite group there is therefore a uniquely determined largest solvable normal subgroup, which is called the *solvable radical*.

Definition 2.24. A subgroup $H \leq G$ is *characteristic* in G if $\alpha(H) = H$ for all $\alpha \in \mathrm{Aut}(G)$. A group $G \neq 1$ is called *characteristically simple* if 1 and G are the only characteristic subgroups.

Example 2.25.

(i) Because of $\mathrm{Inn}(G) \leq \mathrm{Aut}(G)$, every characteristic subgroup is normal.

(ii) Obviously $\mathrm{Z}(G)$ is characteristic in G (Exercise 17).

(iii) In a cyclic group, according to Theorem 2.4, every subgroup is characteristic (Exercise 17).

(iv) According to Remark 2.14, $\langle (1,2) \rangle$ is normal but not characteristic in $\langle (1,2), (3,4) \rangle \cong C_2^2$.

Lemma 2.26. *Let H be characteristic in $N \trianglelefteq G$. Then $H \trianglelefteq G$. If additionally N is characteristic in G, then H is characteristic in G.*

Proof. Let $g \in G$. Then $N \to N$, $x \mapsto gxg^{-1}$ is an automorphism of N. Thus $gHg^{-1} = H$ holds. Now let N be characteristic in G and $\alpha \in \mathrm{Aut}(G)$. Then the restriction of α to N is an automorphism of N. Therefore $\alpha(H) = H$ holds. □

Theorem 2.27. *A finite group G is characteristically simple if and only if G is a direct sum of isomorphic simple groups.*

Proof. First, let G be characteristically simple. Let N be a minimal normal subgroup of G. For $\alpha \in \mathrm{Aut}(G)$, $\alpha(N)$ is then also a minimal normal subgroup of G. Let $\widetilde{N}$ be a direct sum of subgroups of the form $\alpha(N)$ that is as large as possible (in case of doubt $\widetilde{N} = N$). Assume $\alpha(N) \not\subseteq \widetilde{N}$ for some $\alpha \in \mathrm{Aut}(G)$. Because of $\alpha(N) \cap \widetilde{N} \trianglelefteq G$, it follows that $\alpha(N) \cap \widetilde{N} = 1$ from the minimality of $\alpha(N)$. Thus $\alpha(N)\widetilde{N} = \alpha(N) \oplus \widetilde{N}$ in contradiction to the choice of $\widetilde{N}$. This shows $\widetilde{N} = \langle \alpha(N) : \alpha \in \mathrm{Aut}(G) \rangle$. In particular, $\widetilde{N}$ is characteristic in G. Since G is characteristically simple, it follows that $G = \widetilde{N}$. Thus G is a direct sum of groups that are isomorphic to N. Now assume that a normal subgroup $1 \neq M \trianglelefteq N$ exists. For $\alpha \in \mathrm{Aut}(G)$ with $\alpha(N) \neq N$, we have $\alpha(N) \leq \mathrm{C}_G(N) \subseteq \mathrm{N}_G(M)$ according to Lemma 2.5. This shows $M \trianglelefteq \widetilde{N} = G$ and the minimality of N yields $M = N$. Thus N is simple.

Let $G = N_1 \oplus \ldots \oplus N_k$ with isomorphic simple groups $N_1, \ldots, N_k$. Let $H \neq 1$ be characteristic in G. We first consider the case in which the N_i are abelian. Then G is elementary abelian and $\mathrm{Aut}(G) \cong \mathrm{GL}(k,p)$ for a prime p according to Remark 2.14. From linear algebra, it is known that for $x, y \in G \setminus \{1\}$ there exists an $\alpha \in \mathrm{Aut}(G)$ with $\alpha(x) = y$. This shows $H = G$. Now let N_i be non-abelian and

$1 \neq x_1 \dots x_k \in H$ with $x_i \in N_i$ for $i = 1, \dots, k$. wlog. let $x_1 \neq 1$. Because of $\mathrm{Z}(N_1) = 1$, there exists a $y \in N_1$ with $x_1 y \neq y x_1$. It then holds that

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

Since N_1 is simple, it follows that $N_1 \leq H$. For every permutation $\sigma \in S_k$, there exists an $\alpha \in \mathrm{Aut}(G)$ with $\alpha(N_i) = N_{\sigma(i)}$ for $i = 1, \dots, k$. This shows $N_i \leq H$ for $i = 1, \dots, k$, i. e. $H = G$. Thus G is characteristically simple. □

Theorem 2.28. *Chief factors are always characteristically simple. Every chief factor of a finite group G is elementary abelian. In particular, every minimal normal subgroup of G is elementary abelian.*

Proof. Let N/M be a chief factor with $N, M \trianglelefteq G$, and let K/M be characteristic in N/M. According to Lemma 2.26, $K/M \trianglelefteq G/N$ and $K \trianglelefteq G$. This shows $K \in \{N, M\}$. Thus N/M is characteristically simple. Now let G be finite and . Every chief factor of G is then characteristically simple and according to Lemma 2.22. The second assertion now follows from Theorem 2.27. Since every minimal normal subgroup can be extended to a chief series, the third assertion is also clear. □

Remark 2.29.

(i) A normal series with characteristically simple factors is *not* necessarily a chief series!

(ii) If G has a normal series with cyclic factors, then G is called *supersolvable*. According to Theorem 2.28, the chief factors of G then have prime order, provided that $|G| < \infty$. Every supersolvable group is obviously solvable, but the converse is false (example: A_4). According to Theorem 2.11, finitely generated abelian groups are supersolvable.

3 Commutators and nilpotent groups

Definition 3.1. For $x, y \in G$ let $[x, y] := xyx^{-1}y^{-1}$ be the *commutator* of x and y. Inductively, let $[x_1, \dots, x_n] := [x_1, [x_2, \dots, x_n]]$ for $x_1, \dots, x_n \in G$. For $X, Y \subseteq G$ let analogously

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

In particular, $G' := G^{(1)} := [G, G]$ is the *derived subgroup* of G. We set $G'' := (G')'$ and more generally $G^{(k)} := (G^{(k-1)})'$ for $k \geq 2$. Furthermore, let $G^{[1]} := G$ and $G^{[k]} := [G^{[k-1]}, G]$ for $k \geq 2$.[10]

Remark 3.2.

(i) Simple calculations show

$[x, y]^{-1} = [y, x]$,	${}^z[x, y] = [{}^z x, {}^z y]$,
$[x, yz] = [x, y] \cdot {}^y[x, z]$,	$[xy, z] = {}^x[y, z][x, z]$.

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

[10] This notation is not uniform in the literature. One also uses G^k (confusion with direct product), $K_k(G)$ or $\gamma_k(G)$.

(ii) For a homomorphism $f\colon G \to H$, it holds that $f([x,y]) = [f(x), f(y)]$. In particular, $[X,Y]N/N = [XN/N, YN/N]$ for $N \trianglelefteq G$. If X, Y are normal (resp. characteristic) in G, then so is $[X,Y]$. In particular, $G^{(k)}$ and $G^{[k]}$ are characteristic in G.

(iii) For $x, y \in G$, it holds that $xyG' = yx[x^{-1}, y^{-1}]G' = yxG'$. Thus G/G' is abelian. Now let $N \trianglelefteq G$ such that G/N is abelian. Then $[x,y]N = xyx^{-1}y^{-1}N = 1$ and $[x,y] \in N$ for all $x, y \in G$. This shows $G' \subseteq N$. Thus G' is the smallest normal subgroup with an abelian factor group. In particular, G is abelian if and only if $G' = 1$ holds.

Lemma 3.3.

(i) For $X, Y \leq G$, it holds that $[X,Y] \trianglelefteq \langle X, Y\rangle$.

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

Proof.

(i) Certainly $[X,Y] \leq \langle X, Y\rangle$. For $x, z \in X$ and $y \in Y$, we have ${}^z[x,y] = [zx,y][z,y]^{-1} \in [X,Y]$ according to Remark 3.2. This shows $X \leq \mathrm{N}_G([X,Y])$. Analogously, $Y \leq \mathrm{N}_G([Y,X]) = \mathrm{N}_G([X,Y])$.

(ii) We show by induction on k that every element of $G^{[k]}$ is a product of commutators of the form $[g_1, \ldots, g_k]$ (i. e. no inverses are needed). The case $k = 2$ is clear because $[x,y]^{-1} = [y,x]$. Let $k \geq 3$, $x \in G^{[k-1]}$ and $y \in G$. By induction, x is a product of commutators $[g_1, \ldots, g_{k-1}]$. For $x = x_1x_2$, we have $[x_1x_2, y] = {}^{x_1}[x_2,y][x_1,y] = [{}^{x_1}x_2, {}^{x_1}y][x_1,y]$. From this, the claim follows easily. □

Theorem 3.4. *G is solvable if and only if there exists a $k \in \mathbb{N}$ with $G^{(k)} = 1$.*

Proof. Let $1 = G_0 \trianglelefteq \ldots \trianglelefteq G_k = G$ with abelian factors. We argue by induction on k. The case $k = 0$ is clear. So let $k \geq 1$. Since G/G_{k-1} is abelian, $G' \subseteq G_{k-1}$ holds. By induction, there exists an $l \in \mathbb{N}$ with $G^{(l+1)} = (G')^{(l)} \subseteq G_{k-1}^{(l)} = 1$.

Conversely, let $G^{(k)} = 1$. Then $1 = G^{(k)} \trianglelefteq G^{(k-1)} \trianglelefteq \ldots \trianglelefteq G' \trianglelefteq G$ is a (sub)normal series with abelian factors. Thus G is solvable. □

Remark 3.5.

(i) The smallest $k \geq 1$ with $G^{(k)} = 1$ (if it exists) is called the *derived length* of G. In the case $G'' = 1$, G is called *metabelian*. Groups G with $G' = G$ are called *perfect*. Obviously, every non-abelian simple group is perfect.

(ii) For $X, Y, Z \leq G$, we have $[X,Y,Z] = [X,Z,Y]$, but not necessarily $[X,Y,Z] = [Y,X,Z]$ (Exercise 27). The next lemma gives a relationship between the commutators of three subgroups.

Lemma 3.6 (Three-Subgroup Lemma)**.** *Let $X, Y, Z \leq G$ with $[X,Y,Z] = [Y,Z,X] = 1$. Then $[Z,X,Y] = 1$.*

Proof. It suffices to show $[z,x,y]=1$ for $z\in Z$, $x\in X$ and $y\in Y$. For this, we verify the *Hall-Witt identity*[11]

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

We have ${}^{y}[x,y^{-1},z]=yx[y^{-1},z]x^{-1}[z,y^{-1}]y^{-1}=yxy^{-1}zyz^{-1}x^{-1}zy^{-1}z^{-1}$. The left side of (3.1) is thus

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

Definition 3.7. Let $\mathrm{Z}_0(G):=1$ and $\mathrm{Z}_i(G)/\mathrm{Z}_{i-1}(G):=\mathrm{Z}(G/\mathrm{Z}_{i-1}(G))$ for $i\geq 1$. If there exists a $k\geq 0$ with $\mathrm{Z}_k(G)=G$, then G is called *nilpotent*. The smallest k with this property is the (*nilpotency*) *class* of G. If applicable, $1=\mathrm{Z}_0(G)<\ldots<\mathrm{Z}_k(G)=G$ is the *upper central series* of G. In general, $\mathrm{Z}_\infty(G):=\bigcup_{k\geq 0}\mathrm{Z}_k(G)$ is called the *hypercentre* of G.

Example 3.8.

(i) Abelian groups are nilpotent with class ≤ 1.

(ii) Nilpotent groups are solvable, because the upper central series has abelian factors. Since central subgroups are always normal, the upper central series can be refined to a normal series with cyclic factors if G is finite. Finite nilpotent groups are therefore even supersolvable. Note:

$$\text{prime order}\Longrightarrow\text{cyclic}\Longrightarrow\text{abelian}\Longrightarrow\text{nilpotent}\Longrightarrow\text{supersolvable}\Longrightarrow\text{solvable}$$

(iii) Because of $Z_k(G)\leq\mathrm{Z}_{k+1}(G)$ for all $k\in\mathbb{N}$, we have $\mathrm{Z}_\infty(G)\leq G$. There are (infinitely generated) non-nilpotent groups with $G=\mathrm{Z}_\infty(G)$ (e. g. $\times_{n=3}^{\infty}D_{2^n}$ according to Exercise 19). These are called *hypercentral*.

Theorem 3.9. *$G\neq 1$ is nilpotent with class k if and only if $G^{[k]}>G^{[k+1]}=1$ holds.*

Proof. Let G be nilpotent with class k. We show by induction $G^{[i+1]}\subseteq\mathrm{Z}_{k-i}(G)$ for $i\geq 0$. This is clear for $i=0$. So let $i\geq 1$. Suppose that the claim holds for $i-1$. Then

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

i. e. $G^{[i+1]}\subseteq\mathrm{Z}_{k-i}(G)$. In particular, $G^{[k+1]}\subseteq\mathrm{Z}_0(G)=1$.

Conversely, suppose $G^{[l]}=1$ for some $l\geq 1$. We show by induction $G^{[l-i]}\subseteq\mathrm{Z}_i(G)$ for $i\geq 0$. Since this holds for $i=0$, we may assume that the claim is true for $i-1\geq 0$. Then

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

and $G^{[l-i]}\mathrm{Z}_{i-1}(G)/\mathrm{Z}_{i-1}(G)\leq\mathrm{Z}(G/\mathrm{Z}_{i-1}(G))=\mathrm{Z}_i(G)/\mathrm{Z}_{i-1}(G)$. Thus $G^{[l-i]}\subseteq\mathrm{Z}_i(G)$ and $\mathrm{Z}_{l-1}(G)=G$. This shows that G is nilpotent with class at most $l-1$. The claim follows. $\square$

Remark 3.10.

(i) If G is nilpotent with class k, then $1=G^{[k+1]}<\ldots<G^{[1]}=G$ is called the *lower central series* of G (as in the proof above, $G^{[i+1]}\subseteq\mathrm{Z}_{k-i}(G)$). The lower and upper central series are thus two normal series of the same length.

[11] cf. Jacobi identity for Lie algebras

(ii) Let G be nilpotent with class k and $H \leq G$ as well as $N \trianglelefteq G$. Then $H^{[k+1]} \leq G^{[k+1]} = 1$ and $(G/N)^{[k+1]} = G^{[k+1]}N/N = 1$. Therefore, H and G/N are also nilpotent, where the class is bounded by k in each case. Conversely, if $N \trianglelefteq G$ and G/N are nilpotent, G does not necessarily have to be nilpotent! An example is $G = S_3$ with $N = A_3$.

Lemma 3.11. *For $n, m \geq 1$, it holds that $[G^{[n]}, G^{[m]}] \subseteq G^{[n+m]}$.*

Proof. Induction on n: In the case $n = 1$, $[G, G^{[m]}] = [G^{[m]}, G] = G^{[m+1]}$. So let $n \geq 2$ and the statement be already proven for $n-1$. For $\overline{G} := G/G^{[n+m]}$, it holds by induction that

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

and $[\overline{G}^{[n-1]}, \overline{G}^{[m]}, \overline{G}] = [\overline{G}^{[n-1]}, \overline{G}^{[m+1]}] \subseteq \overline{G}^{[n+m]} = 1$. Lemma 3.6 therefore implies

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

This shows the claim. □

Theorem 3.12. *If k is the nilpotency class of $G \neq 1$, then the derived length of G is at most $\log_2(k)+1$.*

Proof. We show $G^{(i)} \subseteq G^{[2^i]}$ by induction on $i \geq 1$. In the case $i = 1$, equality holds. So let $i \geq 1$ and the claim be already proven for $i-1$. Then $G^{(i)} = [G^{(i-1)}, G^{(i-1)}] \subseteq [G^{[2^{i-1}]}, G^{[2^{i-1}]}] \subseteq G^{[2^i]}$ by Lemma 3.11. For $l := \lfloor \log_2(k) \rfloor + 1 \geq \log_2(k+1)$, we now have $G^{(l)} \subseteq G^{[2^l]} \subseteq G^{[k+1]} = 1$. □

Example 3.13. There are metabelian groups with arbitrarily high nilpotency class (dihedral groups of the form D_{2^n}, see Exercise 19).

Theorem 3.14. *Let G be nilpotent, $H < G$ and $1 \neq N \trianglelefteq G$. Then $H < \mathrm{N}_G(H)$, $[G, N] < N$ and $N \cap \mathrm{Z}(G) \neq 1$.*

Proof. Let $k \geq 1$ be minimal with $G^{[k]} \subseteq H$. Since $H < G$, it follows that $k \geq 2$. We have $[G^{[k-1]}, H] \subseteq [G^{[k-1]}, G] = G^{[k]} \subseteq H$. For $x \in G^{[k-1]}$ and $h \in H$, we thus have $xhx^{-1}h^{-1} \in H$ and $xhx^{-1} \in H$. This shows $G^{[k-1]} \subseteq \mathrm{N}_G(H)$. On the other hand, $G^{[k-1]} \nsubseteq H$ due to the minimality of k.

Let $N_1 := N$ and $N_{i+1} := [G, N_i] \leq N$ for $i \geq 1$. By induction, one easily sees $N_i \subseteq G^{[i]}$. Thus there exists a $k \geq 1$ with $N_k = 1$. In particular, $[G, N] = N_2 < N_1$, for otherwise $N_3 = [G, N_2] = [G, N] = N$, $N_4 = N$ etc. For the last statement, we choose $l \geq 1$ maximal with $N_l \neq 1$. Then $[G, N_l] = N_{l+1} = 1$ and $N_l \subseteq N \cap \mathrm{Z}(G)$. □

Theorem 3.15 (Fitting)**.** *If N and M are nilpotent normal subgroups of G, then NM is also nilpotent. If N has class n and M has class m, then NM has at most class $n+m$.*

Proof. For arbitrary normal subgroups $X, Y, Z \trianglelefteq G$ and $x \in X$, $y \in Y$ and $z \in Z$, we have

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

according to Remark 3.2. This shows $[X, YZ] \subseteq [X, Y][X, Z] \subseteq [X, YZ]$ and thus $[X, YZ] = [X, Y][X, Z]$. Analogously, $[XY, Z] = [X, Z][Y, Z]$. Therefore, $(NM)^{[n+m+1]}$ is a product of normal subgroups of the form $[X_0, \ldots, X_{n+m}]$ with $X_0, \ldots, X_{n+m} \in \{N, M\}$. wlog. we can assume that N occurs at least $n+1$ times among the X_i (otherwise M occurs at least $m+1$ times). We show by induction on $n+m$ that then

$[X_0, \ldots, X_{n+m}] \subseteq N^{[n+1]}$ holds. If $X_0 = M$, then by induction already $[X_1, \ldots, X_{n+m}] \subseteq N^{[n+1]}$ and the claim follows. If, on the other hand, $X_0 = N$, then $[X_1, \ldots, X_{n+m}] \subseteq N^{[n]}$ and $[X_0, \ldots, X_{n+m}] \subseteq [N, N^{[n]}] = N^{[n+1]}$. The claim now follows from Theorem 3.9. □

Definition 3.16. The *Fitting group* $\mathrm{F}(G)$ of a finite group G is the product of all nilpotent normal subgroups of G. According to Theorem 3.15, $\mathrm{F}(G)$ is the largest nilpotent normal subgroup of G (this corresponds to the solvable radical).

Remark 3.17. Obviously, $\mathrm{F}(G)$ is characteristic in G.

Example 3.18. Let N be a minimal normal subgroup of a finite solvable group G. According to Theorem 2.28, N is (elementary) abelian and therefore nilpotent. This shows $\mathrm{F}(G) \neq 1$. For example, $\mathrm{F}(S_3) = A_3$.

Theorem 3.19. *If G is finite and solvable, then $\mathrm{C}_G(\mathrm{F}(G)) \leq \mathrm{F}(G)$.*

Proof. Let $C := \mathrm{C}_G(\mathrm{F}(G)) \trianglelefteq G$. We assume indirectly $\overline{C} := C/\mathrm{Z}(\mathrm{F}(G)) = C/C \cap \mathrm{F}(G) \neq 1$. Since $\overline{C}$ is solvable, $N/\mathrm{Z}(\mathrm{F}(G)) := \mathrm{F}(\overline{C}) \neq 1$ holds. Here $\mathrm{Z}(\mathrm{F}(G)) \leq N \cap \mathrm{Z}(C) \leq \mathrm{Z}(N)$ and $N/\mathrm{Z}(N) \cong \mathrm{F}(\overline{C})/(\mathrm{Z}(N)/\mathrm{Z}(\mathrm{F}(G)))$ is nilpotent. Thus N is also nilpotent. Since $\mathrm{Z}(\mathrm{F}(G))$ is characteristic in $\mathrm{F}(G)$, $\mathrm{Z}(\mathrm{F}(G)) \trianglelefteq G$ holds by Lemma 2.26. Furthermore, $\mathrm{F}(\overline{C})$ is characteristic in $\overline{C} \trianglelefteq G/\mathrm{Z}(\mathrm{F}(G))$. This shows $N \trianglelefteq G$ and one obtains the contradiction $N \leq \mathrm{F}(G) \cap C = \mathrm{Z}(\mathrm{F}(G))$. □

Remark 3.20. For finite, solvable groups G, $G/\mathrm{Z}(\mathrm{F}(G)) = \mathrm{N}_G(\mathrm{F}(G))/\mathrm{C}_G(\mathrm{F}(G)) \leq \mathrm{Aut}(\mathrm{F}(G))$ and $G/\mathrm{F}(G) \leq \mathrm{Out}(\mathrm{F}(G))$ holds by Theorem 3.19.

4 p-groups and the Frattini group

Remark 4.1. From now on, let G always be a finite group. As is well known, a subgroup of order d does not exist for every divisor d of $|G|$ (A_4 has no subgroup of order 6). However, if d is a prime power, then there are subgroups of order d. This fact is of fundamental importance for group theory.

Definition 4.2. Let π be a set of prime numbers. An element $x \in G$ is called a *π-element* if every prime divisor of $|\langle x \rangle|$ lies in π. If every element in G is a π-element, then G is called a *π-group*. If $\pi = \{p\}$, one speaks of p-elements and p-groups. The set of prime numbers that are not in π is denoted by π' (analogously p').

Theorem 4.3 (Sylow)**.** *Let $|G| = p^a m$ for a prime number $p \nmid m$. Then:*

(i) G possesses a subgroup P of order p^a. P is called a Sylow p-subgroup *of G. Let the set of Sylow p-subgroups be $\mathrm{Syl}_p(G)$.*

(ii) Every subgroup of order p^b of G is contained in a Sylow p-subgroup.

(iii) Any two Sylow p-subgroups of G are conjugate.

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

Proof.

(i) Induction on $|G|$: For $G = 1$, $P = 1$ is a Sylow p-subgroup (with $a = 0$). So let $G \neq 1$. Assume first that $|\mathrm{Z}(G)|$ is divisible by p. According to the fundamental theorem of finitely generated abelian groups, there exists a subgroup $Z \leq \mathrm{Z}(G)$ with $|Z| = p^b \neq 1$. By induction, G/Z has a Sylow p-subgroup P/Z. Because of $|P| = |P/Z||Z| = p^{a-b+b} = p^a$, we have $P \in \mathrm{Syl}_p(G)$.

Now let $|\mathrm{Z}(G)| \not\equiv 0 \pmod{p}$. The (refined) class equation (1.1) yields an $x \in G \setminus \mathrm{Z}(G)$ with $p \nmid |G : \mathrm{C}_G(x)|$. Because of $x \notin \mathrm{Z}(G)$, we have $\mathrm{C}_G(x) < G$ and by induction there exists $P \in \mathrm{Syl}_p(\mathrm{C}_G(x))$. Obviously, then also $P \in \mathrm{Syl}_p(G)$.

(ii) Let $U \leq G$ be a p-subgroup. The orbit lengths of the action of U on G/P by left multiplication (see Exercise 5) are then divisors of $|U|$, hence p-powers. Because of $p \nmid m = |G : P|$, there exists a fixed point $xP \in G/P$ of U, i. e. $Ux \subseteq UxP = xP$ and $U \subseteq xPx^{-1}$. As the image of P under an inner automorphism, $xPx^{-1} \in \mathrm{Syl}_p(G)$.

(iii) This follows from the proof of (ii).

(iv) According to (iii), G acts transitively on $\mathrm{Syl}_p(G)$ by conjugation. The stabilizer of P is $\mathrm{N}_G(P)$. Thus $|\mathrm{Syl}_p(G)| = |G : \mathrm{N}_G(P)|$ follows from Theorem 1.22. For the congruence, we consider the action of P on $\mathrm{Syl}_p(G)$ by conjugation. Let $Q \in \mathrm{Syl}_p(G)$ be a fixed point, i. e. $P \leq \mathrm{N}_G(Q)$. Because of $P, Q \in \mathrm{Syl}_p(\mathrm{N}_G(Q))$, there exists by (iii) an $x \in \mathrm{N}_G(Q)$ with $P = xQx^{-1} = Q$. Thus P has exactly one fixed point on $\mathrm{Syl}_p(G)$ and the orbit equation shows $|\mathrm{Syl}_p(G)| \equiv 1 \pmod{p}$. □

Corollary 4.4 (Cauchy)**.** *For every prime divisor p of $|G|$, G has an element of order p.*

Proof. Choose $1 \neq x \in P \in \mathrm{Syl}_p(G)$. By Lagrange, $|\langle x \rangle| = p^n$ with $n \geq 1$. By Lemma 2.1, $y := x^{p^{n-1}} \in G$ has order p. □

Example 4.5.

(i) Let $p < q$ be prime numbers with $q \not\equiv 1 \pmod{p}$ (for example $pq = 15$). Let G be a group of order pq. According to Sylow, $|\mathrm{Syl}_p(G)|$ is a divisor of pq and simultaneously congruent to 1 modulo p. This shows $|\mathrm{Syl}_p(G)| = 1$ and analogously $|\mathrm{Syl}_q(G)| = 1$. Let $P \in \mathrm{Syl}_p(G)$ and $Q \in \mathrm{Syl}_q(G)$. Then $P, Q \trianglelefteq G$ (even characteristic) and $P \cap Q = 1$ by Lagrange. Because of $|PQ| = |P||Q| = pq = |G|$, it follows $G = P \oplus Q \cong C_p \times C_q \cong C_{pq}$ (alternative argument: Because of $|P \cup Q| = p + q - 1 < pq$, G must possess elements of order pq).

(ii) In algebra, one shows that all groups of order < 60 are solvable. A "difficult" case is $|G| = 30 = 2 \cdot 3 \cdot 5$. One can assume inductively here that G is simple. According to Sylow, it then holds $\mathrm{Syl}_5(G) = \{P_1, \ldots, P_6\}$. Because of $|P_1 \cup \ldots \cup P_6| = 1 + 6 \cdot 4 = 25$, there is only room for at most two 3-Sylow groups. According to Sylow, it follows $|\mathrm{Syl}_3(G)| = 1$ in contradiction to the simplicity of G.

Remark 4.6.

(i) According to Lagrange and Cauchy, G is a π-group if and only if every prime divisor of $|G|$ lies in π. In particular, the order of a p-group is a power of p. However, this characterization of π-groups cannot be extended to infinite groups.

(ii) For π-normal subgroups $N, M \trianglelefteq G$, the product $NM \trianglelefteq G$ is also a π-normal subgroup, since $|NM| \mid |N||M|$. Thus, there exists a largest π-normal subgroup $\mathrm{O}_\pi(G)$, which is called the *π-core* or *π-radical*. For $\pi = \{p\}$, one writes $\mathrm{O}_p(G)$. For $H \leq G$, $H \cap \mathrm{O}_\pi(G)$ is a π-normal subgroup of H and it follows that $H \cap \mathrm{O}_\pi(G) \leq \mathrm{O}_\pi(H)$.

(iii) If $N, M \trianglelefteq G$ with π-factor groups G/N and G/M, then $G/(N \cap M)$ is also a π-group, since

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

There is therefore a smallest normal subgroup $\mathrm{O}^\pi(G)$ with π-factor group $G/\mathrm{O}^\pi(G)$. One calls $\mathrm{O}^\pi(G)$ the *π-residue* of G (analogously $\mathrm{O}^p(G)$). Obviously, every π'-element lies in $\mathrm{O}^\pi(G)$. Conversely, all π'-elements of G generate a normal subgroup with π-factor group. This shows $\mathrm{O}^\pi(G) = \langle g \in G : g \text{ is a } \pi'\text{-element}\rangle$. For $H \leq G$, $H/(H \cap \mathrm{O}^\pi(G)) \cong H\mathrm{O}^\pi(G)/\mathrm{O}^\pi(G) \leq G/\mathrm{O}^\pi(G)$ is a π-group and it follows that $\mathrm{O}^\pi(H) \leq \mathrm{O}^\pi(G)$.

(iv) For $P \in \mathrm{Syl}_p(G)$ and $N \trianglelefteq G$, we have $p \nmid |PN : P| = |N : N \cap P|$ and $p \nmid |G : PN| = |G/N : PN/N|$. This shows $P \cap N \in \mathrm{Syl}_p(N)$ and $PN/N \in \mathrm{Syl}_p(G/N)$.

(v) Let $N \trianglelefteq G$ and $P \in \mathrm{Syl}_p(N)$. Then G acts on $\mathrm{Syl}_p(N)$ by conjugation and N acts transitively. The Frattini argument thus shows $G = N\mathrm{N}_G(P)$.

Theorem 4.7. *It holds that* $\mathrm{O}_p(G) = \bigcap_{P \in \mathrm{Syl}_p(G)} P$ *and* $\mathrm{O}^{p'}(G) = \langle P : P \in \mathrm{Syl}_p(G)\rangle$.

Proof. Obviously, $\bigcap_{P \in \mathrm{Syl}_p(G)} P$ is a p-normal subgroup and therefore contained in $\mathrm{O}_p(G)$. Conversely, by Sylow, there exists a $P \in \mathrm{Syl}_p(G)$ with $\mathrm{O}_p(G) \leq P$. For $g \in G$, we have $\mathrm{O}_p(G) = g\mathrm{O}_p(G)g^{-1} \leq gPg^{-1}$. Since all Sylow p-subgroups are conjugate, the first assertion follows.

According to Remark 4.6, $\mathrm{O}^{p'}(G)$ is generated by all p-elements. Every p-element lies in a Sylow p-subgroup. This shows the second assertion. □

Theorem 4.8. *Every p-group is nilpotent.*

Proof. Let P be a p-group. We argue by induction on $|P|$. Let wlog. $P \neq 1$. Considering the class equation modulo p, one obtains $|\mathrm{Z}(P)| \equiv 0 \pmod p$. In particular, $\mathrm{Z}(P) \neq 1$. By induction, $P/\mathrm{Z}(P)$ is nilpotent and therefore so is P. □

Remark 4.9. From a statistical perspective, almost all groups are p-groups. Among the groups of order ≤ 2000, for example, over 99% have order 2^{10} (see Table 1). The number of groups of order 2^{11} is unknown (see Remark 2.19).

Theorem 4.10. *The following statements are equivalent:*

(1) G is nilpotent.

(2) For all $H < G$, $H < \mathrm{N}_G(H)$.

(3) Every maximal subgroup of G is normal.

(4) For every prime p, G contains exactly one Sylow p-subgroup.

(5) G is the direct sum of its Sylow subgroups.

Proof.

(1)⇒(2): Theorem 3.14.

(2)⇒(3): Trivial.

(3)⇒(4): Let $P \in \mathrm{Syl}_p(G)$. If $\mathrm{N}_G(P) < G$, then $\mathrm{N}_G(P)$ lies in a maximal subgroup $H < G$. By (3), $H \trianglelefteq G$. From Remark 4.6 the contradiction $G = H\mathrm{N}_G(P) = H$ now follows.

(4)⇒(5): Let $p_1, \ldots, p_n$ be the prime divisors of $|G|$ and $\mathrm{Syl}_{p_i}(G) = \{P_i\}$. Then $P_i \trianglelefteq G$ and $|P_1 \ldots P_n| = |P_1| \ldots |P_n|$. It follows easily that $G = P_1 \oplus \ldots \oplus P_n$.

(5)⇒(1): By Theorem 4.8, every Sylow subgroup is nilpotent and therefore so is G (Theorem 3.15). □

Theorem 4.11. *It holds that* $\mathrm{F}(G) = \bigoplus_{p\,||G|} \mathrm{O}_p(G)$.

Proof. The right side is a nilpotent normal subgroup and therefore contained in $\mathrm{F}(G)$. By Theorem 4.10, $\mathrm{F}(G) = Q_1 \oplus \ldots \oplus Q_n$ with $Q_i \in \mathrm{Syl}_{p_i}(\mathrm{F}(G))$. As the unique p_i-Sylow subgroup of $\mathrm{F}(G)$, Q_i must be characteristic in $\mathrm{F}(G)$. By Lemma 2.26, it follows that $Q_i \trianglelefteq G$ and thus $Q_i \leq \mathrm{O}_{p_i}(G)$. □

Theorem 4.12 (Baer)**.** *For the hypercenter,* $\mathrm{Z}_\infty(G) = \bigcap_{p\,||G|} \bigcap_{P \in \mathrm{Syl}_p(G)} \mathrm{N}_G(P)$ *holds.*

Proof. Obviously $\mathrm{Z}_0(G) = 1 \leq \bigcap_{p\,||G|} \bigcap_{P \in \mathrm{Syl}_p(G)} \mathrm{N}_G(P) =: U$. Suppose inductively that $Z := \mathrm{Z}_k(G) \leq U$ has already been shown. For $g \in \mathrm{Z}_{k+1}(G)$ and $P \in \mathrm{Syl}_p(G)$, we have $gZ \in \mathrm{Z}(G/Z) \leq \mathrm{N}_G(PZ/Z)$ and $g \in \mathrm{N}_G(PZ)$. By Sylow, there exists a $z \in Z \leq U \leq \mathrm{N}_G(P)$ such that $gPg^{-1} = zPz^{-1} = P$. This shows $g \in \mathrm{N}_G(P)$ and $\mathrm{Z}_{k+1}(G) \leq U$. It follows that $\mathrm{Z}_\infty(G) \leq U$.

For the converse, let $Z := \mathrm{Z}_\infty(G)$. Every Sylow subgroup of G/Z has the form PZ/Z with $P \in \mathrm{Syl}_p(G)$ and $\mathrm{N}_G(P)Z/Z \leq \mathrm{N}_{G/Z}(PZ/Z)$. We can therefore assume $Z = 1$ and must show $U = 1$. Suppose indirectly that $U \neq 1$. Then there exists a $P \in \mathrm{Syl}_p(G)$ with $U \cap P \neq 1$ by Cauchy. Since $U \trianglelefteq G$, we also have $U_0 := U \cap \mathrm{Z}(P) \neq 1$ by Theorem 3.14. For all $Q \in \mathrm{Syl}_p(G)$, we have $U_0 \leq P \cap \mathrm{N}_G(Q) = P \cap Q$. This shows $U_0 \leq \mathrm{O}_p(G)$ by Theorem 4.7. Since $\mathrm{Z}(G) = 1$, G is not a p-group. Thus, let $S \in \mathrm{Syl}_q(G)$ with $q \neq p$. Then $U_0 \leq \mathrm{N}_G(S) \cap \mathrm{O}_p(G) \leq \mathrm{C}_G(S)$ by Lemma 2.5. Since $\mathrm{O}^p(G)$ is generated by all q-Sylow subgroups with $q \neq p$ (cf. Theorem 4.7), it follows that $U_0 \leq \mathrm{C}_G(\mathrm{O}^p(G))$. From $G = \mathrm{O}^p(G)P$ and $U_0 \leq \mathrm{Z}(P)$, one obtains the contradiction $U_0 \leq \mathrm{Z}(G) = 1$. □

Definition 4.13. The *Frattini group* $\Phi(G)$ is the intersection of all maximal subgroups of G.[12] For $G = 1$, one sets $\Phi(G) = 1$.

Remark 4.14. For $G \neq 1$, certainly $\Phi(G) < G$. Furthermore, $\Phi(G)$ is characteristic in G.

Lemma 4.15. *For $H \leq G$ and $N \trianglelefteq G$, the following hold:*

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

[12] cf. Jacobson radical in ring theory

Proof.

(i) In the case $H < G$, H lies in a maximal subgroup $M < G$. By definition, however, $\Phi(G) \leq M$ also holds, and one obtains the contradiction $G = H\Phi(G) \leq M$.

(ii) In the case $N \not\subseteq \Phi(G)$, there exists a maximal subgroup $M < G$ with $N \not\subseteq M$ and therefore $G = MN$. By Dedekind, $H = NM \cap H = N(M \cap H) = \Phi(H)(M \cap H)$. By (i), it follows that $H = M \cap H \leq M$, and one has the contradiction $N \leq M$.

(iii) Since $\Phi(N)$ is characteristic in N, it follows that $\Phi(N) \trianglelefteq G$. Thus, one can apply (ii) with $\Phi(N)$ instead of N and N instead of H. The assertion follows.

(iv) If M/N is a maximal subgroup of G/N, then M is also maximal in G. This shows $\Phi(G)N/N \subseteq MN/N$ and the assertion follows.

(v) By (iv), we only need to show $\Phi(G/N) \leq \Phi(G)/N$. If $M < G$ is maximal, then $N \leq \Phi(G) \leq M$ and $M/N < G/N$ is also maximal. This shows $\Phi(G/N) \leq M/N$ and the assertion follows. □

Theorem 4.16 (Frattini)**.** *The following holds:*

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

(ii) If $G/\Phi(G)$ *is nilpotent, then so is* G*.*

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

Proof.

(i) Let $P \in \mathrm{Syl}_p(\Phi(G))$. According to Remark 4.6, $G = \Phi(G)\mathrm{N}_G(P)$ and Lemma 4.15 shows $G = \mathrm{N}_G(P)$, i. e. $P \trianglelefteq G$. Then also $P \trianglelefteq \Phi(G)$ and the assertion follows from Theorem 4.10.

(ii) For $P \in \mathrm{Syl}_p(G)$, $P\Phi(G)/\Phi(G) \in \mathrm{Syl}_p(G/\Phi(G))$. According to Theorem 4.10, $P\Phi(G)/\Phi(G) \trianglelefteq G/\Phi(G)$ and thus $P\Phi(G) \trianglelefteq G$. Because $P \in \mathrm{Syl}_p(P\Phi(G))$, $G = \mathrm{N}_G(P)P\Phi(G) = \mathrm{N}_G(P)\Phi(G)$ according to Remark 4.6. Lemma 4.15 now shows $G = \mathrm{N}_G(P)$ and $P \trianglelefteq G$. The assertion follows with Theorem 4.10.

(iii) If $D := G' \cap \mathrm{Z}(G) \not\subseteq \Phi(G)$, then there exists a maximal subgroup $M < G$ with $D \not\subseteq M$, hence $G = DM$. Because $D \leq \mathrm{Z}(G)$, $M \trianglelefteq G$. According to Cauchy, $|G/M|$ must be a prime number. In particular, G/M is abelian and therefore $D \leq G' \leq M$. Contradiction. □

Theorem 4.17 (Wielandt)**.** *G is nilpotent if and only if $G' \leq \Phi(G)$ holds.*

Proof. If G is nilpotent, then every maximal subgroup $M < G$ is normal in G (Theorem 4.10). In particular, $|G/M|$ is a prime number and G/M is abelian. This shows $G' \leq M$ and therefore $G' \leq \Phi(G)$.

Conversely, let $G' \leq \Phi(G)$. Then $G/\Phi(G)$ is abelian and therefore nilpotent. The assertion now follows from Theorem 4.16. □

Theorem 4.18. *For every p-group P, $\Phi(P) = P'\langle x^p : x \in P\rangle$. In particular, $P/\Phi(P)$ is elementary abelian. If $N \trianglelefteq P$ with elementary abelian factor group P/N, then $\Phi(P) \leq N$ holds. Thus $\Phi(P)$ is the smallest normal subgroup with elementary abelian factor group.*

Proof. According to Wielandt, $P' \leq \Phi(P)$. For every maximal subgroup $M < P$, $M \trianglelefteq P$ and therefore $|P/M| = p$. This shows $\langle x^p : x \in P\rangle \leq M$ and it follows $P'\langle x^p : x \in P\rangle \leq \Phi(P)$. Now let $N \trianglelefteq P$ such that P/N is elementary abelian. Suppose $\Phi(P) \not\subseteq N$. Then there exists an $x \in \Phi(P) \setminus N$. In particular, $1 \neq xN \in P/N$. As usual, P/N is a vector space over $\mathbb{F}_p$. We can thus extend xN to a basis $xN, x_2N, \ldots, x_rN$ of P/N. Obviously, then

$$P = \langle x, x_2, \ldots, x_r\rangle N = \Phi(P)\langle x_2, \ldots, x_r\rangle N.$$

It follows $P = \langle x_2, \ldots, x_r\rangle N$ and $P/N = \langle x_2N, \ldots, x_rN\rangle$. This contradicts the choice of $x_2, \ldots, x_r$. Thus $\Phi(P) \leq N$. Obviously, $N := P'\langle x^p : x \in P\rangle$ is a normal subgroup with elementary abelian factor group. Therefore, $\Phi(P) \leq P'\langle x^p : x \in P\rangle$ also holds. □

Theorem 4.19 (BURNSIDE's Basis Theorem)**.** *For a p-group P, $P = \langle x_1, \ldots, x_n\rangle$ holds if and only if $P/\Phi(P) = \langle x_1\Phi(P), \ldots, x_n\Phi(P)\rangle$. Thus, if $|P/\Phi(P)| = p^r$, then P can be generated by r elements, but not by fewer than r.*

Proof. It holds that

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

The second statement follows by regarding $P/\Phi(P)$ again as a vector space over $\mathbb{F}_p$. □

Theorem 4.20. *Let $\alpha \in \mathrm{Aut}(G)$ with $\gcd(|\langle\alpha\rangle|, |\Phi(G)|) = 1$ and $\alpha(x) \equiv x \pmod{\Phi(G)}$ for all $x \in G$. Then $\alpha = \mathrm{id}_G$.*

Proof. Let $x_1, \ldots, x_n \in G$ be a generating system of G and $\Omega := x_1\Phi(G) \times \ldots \times x_n\Phi(G)$. By assumption, $\langle\alpha\rangle$ acts component-wise on Ω. For $\omega = (y_1, \ldots, y_n) \in \Omega$, it holds that $G = \langle y_1, \ldots, y_n\rangle\Phi(G) = \langle y_1, \ldots, y_n\rangle$ and $\langle\alpha\rangle_\omega = 1$ (stabilizer). The orbit equation now yields $|\langle\alpha\rangle| \mid |\Omega| = |\Phi(G)|^n$. Due to $\gcd(|\langle\alpha\rangle|, |\Phi(G)|) = 1$, we have $\alpha = \mathrm{id}_G$. □

Remark 4.21. Let P be a p-group and α a non-trivial p'-automorphism of P. Then Theorem 4.20 states that α acts non-trivially on $P/\Phi(P)$. In particular, the kernel of the canonical homomorphism $\mathrm{Aut}(P) \to \mathrm{Aut}(P/\Phi(P))$ is a p-group.

Example 4.22. Let P be a non-abelian p-group of order p^3. Then $1 \neq P' \leq \Phi(P) < P$ and $|P : \Phi(P)| = p^2$ according to Theorem 4.19. This shows $P' = \Phi(P)$. According to Theorem 3.14, $P' \leq \mathrm{Z}(P)$ and according to Exercise 10, $P/\mathrm{Z}(P)$ is not cyclic. Thus $P' = \Phi(P) = \mathrm{Z}(P)$ holds. We will fully classify these groups later (Theorem 9.9). Now let $\alpha \in \mathrm{Aut}(P)$ be a p'-automorphism. According to Remark 4.21, α acts faithfully on $P/\Phi(P)$. We can therefore assume $\alpha \in \mathrm{Aut}(P/\Phi(P)) \cong \mathrm{GL}(2, p)$. Because of

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

$|\langle\alpha\rangle|$ is a divisor of $(p - 1)^2(p + 1)$.

Theorem 4.23. *Let p, q be prime numbers and $n \geq 1$. Then every group of order p^nq is solvable.*

Proof. Let G be a minimal counterexample. Then certainly $p \neq q$. Let $P \in \mathrm{Syl}_p(G)$. In the case $P \trianglelefteq G$, G would be solvable, since P and G/P are solvable (Lemma 2.22). Thus $\mathrm{N}_G(P) = P$. We choose $Q \in \mathrm{Syl}_p(G) \setminus \{P\}$ such that $|P \cap Q|$ is as large as possible. First, assume $P \cap Q = 1$. Then any two Sylow p-subgroups intersect trivially and there are

$$1 + (|P| - 1)|G : \mathrm{N}_G(P)| = |G| - q + 1$$

many p-elements in G. Thus there is only room for one q-Sylow subgroup, which must then be normal. But then G would again be solvable. Thus $D := P \cap Q \neq 1$. Let $N := \mathrm{N}_G(D)$. If N is contained in a Sylow p-subgroup S of G, then one has $D < \mathrm{N}_P(D) \leq P \cap S$ and $D < \mathrm{N}_Q(D) \leq Q \cap S$ by Theorem 4.10. The choice of P and Q then yields the contradiction $P = S = Q$. Thus N contains a q-Sylow subgroup T of G. For order reasons, $G = PT$. For every $g \in G$ there exist $x \in P$ and $y \in T \leq N$ with $g = xy$ and $gDg^{-1} = xyDy^{-1}x^{-1} = xDx^{-1} \leq P$. Consequently $K := D^G = \langle gDg^{-1} : g \in G \rangle \leq P$ and $K \trianglelefteq G$. By the choice of G, K and G/K are solvable. Thus G is also solvable. □

Lemma 4.24. *Let $N \trianglelefteq G$ with nilpotent factor group G/N. Then:*

(i) There exists a nilpotent subgroup $H \leq G$ with $G = HN$.

(ii) If N is also nilpotent, then there exists a nilpotent subgroup H with $G = HN$ and $\mathrm{N}_G(H) = H$.

Proof.

(i) If $N \leq \Phi(G)$, then $H = G$ is nilpotent by Frattini. So let $M < G$ be maximal with $N \not\subseteq M$. Then $G = MN$ and $M/(M \cap N) \cong G/N$ is nilpotent. By induction on $|G|$ we can assume that a nilpotent subgroup $H \leq M$ with $M = H(M \cap N)$ exists. It now holds that $G = MN = H(M \cap N)N = HN$.

(ii) We choose H as in (i) such that $|H|$ is as large as possible. By Dedekind, $\mathrm{N}_G(H) = HN \cap \mathrm{N}_G(H) = H\mathrm{N}_N(G)$. By assumption, H and $\mathrm{N}_N(H)$ are nilpotent normal subgroups of $\mathrm{N}_G(H)$. Thus $\mathrm{N}_G(H)$ is also nilpotent by Fitting. The maximality of $|H|$ shows $\mathrm{N}_G(H) = H$. □

Definition 4.25. A nilpotent subgroup $C \leq G$ is called a *Carter group* of G if $\mathrm{N}_G(C) = C$ (*self-normalizing*).

Example 4.26.

(i) In a nilpotent group G, G is the unique Carter subgroup according to Theorem 4.10.

(ii) The 2-Sylow subgroups of S_4 are Carter subgroups.

(iii) Let C be a Carter subgroup of $G = A_5$. Since G has no elements of order 6, 10 or 15, C must be a p-group. According to Sylow and Theorem 4.10, C is even a Sylow p-subgroup of G. The cases $p \in \{3, 5\}$ are excluded because $|G : \mathrm{N}_G(C)| = |G : C| \not\equiv 1 \pmod{p}$. So let $C = V_4$. Then $A_4 \leq \mathrm{N}_G(C) = C$ would hold. Thus A_5 has no Carter subgroup. The following theorem implies that A_5 is not solvable.

Theorem 4.27 (Carter)**.** *Every solvable group has exactly one Carter subgroup up to conjugation.*

Proof. We argue by induction on $|G|$ and choose a minimal normal subgroup $N \trianglelefteq G$. According to Theorem 2.28, N is an (elementary) abelian p-group.

By induction, G/N has a Carter subgroup K/N. Lemma 4.24 provides a nilpotent subgroup $C \leq K$ with $K = CN$ and $\mathrm{N}_K(C) = C$. It follows that

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

and $\mathrm{N}_G(C) = \mathrm{N}_K(C) = C$. Thus C is a Carter subgroup of G.

Conversely, let $D \leq G$ be a Carter subgroup of G. Then DN/N is nilpotent and, in the case $DN = G$, also self-normalizing in G/N. Now let $DN < G$. By induction, the Carter subgroups of DN are then conjugate. The Frattini argument yields $\mathrm{N}_G(DN) = \mathrm{N}_G(D)N = DN$. Thus DN/N is in any case a Carter subgroup of G/N. By induction, CN and DN are conjugate. Wlog. let $CN = G = DN$. If G is nilpotent, then $C = G = D$ holds according to Theorem 4.10. So let $C, D < G$. Since N is abelian, $G = CN \leq \mathrm{N}_G(C \cap N)$ holds. The minimality of N yields $C \cap N = 1 = D \cap N$. Since G is not nilpotent, there exists a prime divisor $q \neq p$ of $|C| = |D|$. Let $Q \in \mathrm{Syl}_q(C) \subseteq \mathrm{Syl}_q(G)$. Since C is nilpotent, it follows that $C \leq \mathrm{N}_G(Q)$. In the case $Q \trianglelefteq G$, $Q \leq D$ holds. As Carter subgroups of G/Q, C/Q and D/Q are then conjugate by induction. So let $\mathrm{N}_G(Q) < G$. Because of $G = CN \leq \mathrm{N}_G(\mathrm{N}_N(Q))$, $\mathrm{N}_N(Q) = 1$ and $\mathrm{N}_G(Q) = C$. Analogously, there exists $R \in \mathrm{Syl}_q(G)$ with $\mathrm{N}_G(R) = D$. By Sylow, Q and R as well as $\mathrm{N}_G(Q)$ and $\mathrm{N}_G(R)$ are conjugate. □

Remark 4.28. Using the classification of finite simple groups, Vdovin proved that every group has at most one Carter subgroup up to conjugation. The Sylow p-subgroups of an arbitrary group can therefore be self-normalizing for at most one prime p. If G has self-normalizing Sylow p-subgroups for $p > 3$, then G is solvable according to a theorem of Guralnick-Malle-Navarro.

5 Complements and Hall subgroups

Remark 5.1. As a generalization of Sylow, we show that in solvable groups G there always exists a subgroup of order d, provided that d and $|G|/d$ are coprime. For supersolvable groups, a subgroup of order d exists for every divisor d of $|G|$.

Definition 5.2. Let $N \leq G$. A subgroup $H \leq G$ with $G = NH$ and $H \cap N = 1$ is called a *complement* of N in G.

Remark 5.3.

(i) In this chapter, we are only interested in the case $N \trianglelefteq G$. In section 7, however, we look for *normal* complements $H \trianglelefteq G$.

(ii) Note that a complement in the sense above is not a set-theoretic complement!

(iii) If H is a complement of $N \trianglelefteq G$, then every element $g \in G$ can be uniquely written in the form $g = xh$ with $x \in N$ and $h \in H$. Indeed, if $g = x'h'$ with $x' \in N$ and $h' \in H$, then it follows that $(x')^{-1}x = h'h^{-1} \in N \cap H = 1$.

(iv) An *exact sequence* is a sequence of group homomorphisms

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

with $\alpha_i(G_i) = \mathrm{Ker}(\alpha_{i+1})$ for all i. A *short exact sequence* has the form

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

Then $N \cong \alpha(N) = \mathrm{Ker}(\beta) \trianglelefteq G$ and $G/N = G/\mathrm{Ker}(\beta) \cong \beta(G) = H$ (α is injective and β is surjective). The sequence *splits*, if a homomorphism $\gamma\colon H \to G$ with $\beta \circ \gamma = \mathrm{id}_H$ exists. In this case, $\gamma(H) \cong H$ with $\gamma(H) \cap \mathrm{Ker}(\beta) = 1$ and $G = \mathrm{Ker}(\beta)\gamma(H)$.

(v) If $N \trianglelefteq G$ has a complement H, then one obtains a splitting exact sequence $1 \to N \hookrightarrow G \twoheadrightarrow H \to 1$ via embedding.

Example 5.4.

(i) Let K be a complement of $N \trianglelefteq G$ and $N \leq H \leq G$. Then $H \cap K$ is a complement of N in H, because $(H \cap K)N = H \cap KN = H$. If $M \trianglelefteq G$ with $M \leq N$, then KM/M is a complement of N/M, because $N \cap KM = (N \cap K)M = M$ by Dedekind.

(ii) In a direct sum $N \oplus M$, N is a complement of M and vice versa. According to Remark 2.8, complements are therefore in general not uniquely determined.

(iii) In an elementary abelian group, every subgroup (normal subgroup) has a complement (linear algebra).

(iv) According to Theorem 4.10, every Sylow subgroup of a nilpotent group has a complement.

(v) According to Exercise 26, every complete normal subgroup has a complement.

(vi) S_2 is a complement of A_3 in S_3.

(vii) The subgroup C_2 of C_4 possesses *no* complement, because $C_4 \ncong C_2^2$.

Theorem 5.5 (Rose)**.** *For every finite group G, the following statements are equivalent:*

(1) $\mathrm{Z}(G) = 1$ *and* $\mathrm{Inn}(G)$ *possesses a complement in* $\mathrm{Aut}(G)$.

(2) If G is a normal subgroup of a finite group H, then G possesses a complement in H.

Proof.

(1)⇒(2): For $N := \mathrm{C}_H(G) \trianglelefteq H$, we have $G \cap N = \mathrm{Z}(G) = 1$ and $\mathrm{Inn}(G) \cong GN/N \trianglelefteq H/N \leq \mathrm{Aut}(G)$. Thus there exists $K/N \leq H/N$ with $H = GK$ and $GN \cap K = N$. It follows that $G \cap K \leq G \cap GN \cap K = G \cap N = 1$.

(2)⇒(1): Assume $|\mathrm{Z}(G)|$ is divisible by a prime p. Let $x \in \mathrm{Z}(G)$ with order p and let p^n be the maximal order of a p-element in G. Let $C = \langle y \rangle \cong C_{p^{n+1}}$ and

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

We define $H := (G \times C)/Z$ (a central product, see Definition 9.14). Obviously $f\colon G \to H$, $g \mapsto (g, 1)Z$ is a monomorphism. By assumption, $f(G)$ possesses a complement $K \leq H$. By construction, $[f(G), K] = 1$ and $H = f(G) \times K$. Because $|K| = |H|/|G| = p^n$, H possesses no element of order p^{n+1}. On the other hand, $C \to H$, $y \mapsto (1, y)Z$ is a monomorphism. This contradiction shows $\mathrm{Z}(G) = 1$. Now $\mathrm{Inn}(G) \cong G$ possesses a complement in $\mathrm{Aut}(G)$. □

Remark 5.6. In the following, we consider homomorphisms of the form $G \to \mathrm{Aut}(H)$, where G and H are groups. Because $\mathrm{Aut}(H) \leq \mathrm{Sym}(H)$, G then acts on H. For $g \in G$ and $x, y \in H$, it holds that ${}^g(xy) = ({}^g x)({}^g y)$.

Lemma 5.7. *Let $\varphi\colon H \to \mathrm{Aut}(N)$ be a homomorphism for groups H, N. Then $G := N \times H$ becomes a group by means of*

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

Proof. For $x, y, z \in N$ and $g, h, k \in H$ we have

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

Thus G is associative. Furthermore, $(1,1) * (x,g) = (x,g)$ and $(1,1)$ is the identity element. Finally,

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

Definition 5.8. One calls G the *semidirect product* of N with H and writes $G = N \rtimes_\varphi H$. [13]

Remark 5.9.

(i) In contrast to the direct product, one cannot swap the factors in a semidirect product.

(ii) If the action φ is clear from the context or immaterial, one also writes $N \rtimes H$. In particular, in the case $H \leq \mathrm{Aut}(N)$, one often chooses the inclusion map $\varphi\colon H \hookrightarrow \mathrm{Aut}(N)$.

(iii) If φ is trivial, then obviously $N \rtimes_\varphi H \cong N \times H$. Now let φ be non-trivial. Then there exist $h \in H$ and $x \in N$ with ${}^h x \neq x$. It follows that $(x,1) * (1,h) = (x,h) \neq ({}^h x, h) = (1,h) * (x,1)$. In particular, G is non-abelian.

(iv) We now prove the non-commutative version of Lemma 2.7.

Lemma 5.10. *Let $N \trianglelefteq G$ with complement $H \leq G$. Then $G \cong N \rtimes H$. Conversely, if a semidirect product $G = N \rtimes_\varphi H$ is given, then there exists a normal subgroup $\widetilde{N} \trianglelefteq G$ with complement $\widetilde{H} \leq G$, such that $\widetilde{N} \cong N$ and $\widetilde{H} \cong H$ hold.*

Proof. Let $\varphi\colon H \to \mathrm{Aut}(N)$ be the conjugation map. We show that the map

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

is an isomorphism. For $x, y \in N$ and $h, k \in H$ we have

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

Thus F is a homomorphism. Obviously F is also bijective.

For the second claim, we consider the short exact sequence

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

According to Remark 5.3, it suffices to show that this sequence splits. This is seen via the homomorphism $H \to G$, $h \mapsto (1,h)$. $\square$

[13] more rarely one finds the notation $N \leftthreetimes H$

Example 5.11.

(i) According to Exercise 4, every abelian group A possesses the automorphism $x \mapsto x^{-1}$ ($x \in A$). If $\varphi\colon C_2 \to \mathrm{Aut}(A)$ is the corresponding homomorphism, then one can construct $A \rtimes_\varphi C_2$. For $n \geq 3$, $D_{2n} := C_n \rtimes_\varphi C_2$ is called the *dihedral group* of order $2n$ (cf. Exercise 8). Obviously, φ is then non-trivial and D_{2n} is non-abelian. On the other hand, $D'_{2n} \leq C_n$ and D_{2n} is metabelian.

(ii) According to Exercise 26, there exists an isomorphism $\varphi\colon S_3 \to \mathrm{Aut}(S_3)$ with $S_3 \rtimes_\varphi S_3 \cong S_3 \times S_3$. Semidirect products can therefore not be classified by the corresponding homomorphisms without further ingredients.

Theorem 5.12. *Let $|G| = pq$ with prime numbers $p \leq q$. Then one of the following statements holds:*

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

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

(iii) $p \mid q-1$ *and* $G \cong C_q \rtimes C_p$ *is non-abelian.*

Proof. In the case $p = q$, G is abelian, for example according to Theorem 4.19. Then the claim follows from Theorem 2.11. Now let G be non-abelian and $p < q$. According to Example 4.5, $q \equiv 1 \pmod{p}$ and G possesses a normal q-Sylow subgroup Q. Obviously, $P \in \mathrm{Syl}_p(G)$ is a complement of Q, i. e. $G = Q \rtimes P$. Because of $\mathrm{Aut}(Q) \cong C_{q-1}$, there exists a non-trivial homomorphism $\varphi\colon P \to \mathrm{Aut}(Q)$. Therefore, such a group also exists. According to Exercise 31, the isomorphism type of this group is uniquely determined by p and q. □

Example 5.13. Up to isomorphism, C_{21} and $C_7 \rtimes C_3$ are the only groups of order 21.

Lemma 5.14. *Let $N \trianglelefteq G$ and $H \leq G$ be minimal with respect to the property $G = HN$. Then $H \cap N \leq \Phi(H)$.*

Proof. In the case $H \cap N \not\subseteq \Phi(H)$, there exists a maximal subgroup $M < H$ with $M(H \cap N) = H$ (note $H \cap N \trianglelefteq H$). But then $G = HN = MN$ would be a contradiction to the choice of H. □

Theorem 5.15. *Let A be the product of all abelian minimal normal subgroups of G. Then the following statements are equivalent:*

(1) Every abelian normal subgroup of G possesses a complement.

(2) A possesses a complement.

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

Proof.

(1)⇒(2): For two abelian minimal normal subgroups $B, C \trianglelefteq G$, it holds that $[B, C] \leq B \cap C = 1$. Therefore A is abelian and (2) follows.

(2)⇒(3): Let $G = A \rtimes K$ and indirectly $\Phi(G) \neq 1$. Let $N \leq \Phi(G)$ be a minimal normal subgroup of G. Since $\Phi(G)$ is nilpotent, $N \leq A$ holds. As a product of (commuting) elementary abelian groups, A is a direct product of groups of prime order. In particular, $\Phi(A) = 1$ by Exercise 25. Therefore there exists a maximal subgroup $B < A$ with $A = NB$. Now $G = AK = NBK = \Phi(G)BK = BK$ in contradiction to $|BK| = |B||K| < |A||K| = |G|$.

(3)⇒(1): Let $1 \neq N \trianglelefteq G$ be abelian and $H \leq G$ as in Lemma 5.14. Then $H \cap N \trianglelefteq H$ and $H \cap N \trianglelefteq N$ hold, since N is abelian. This shows $H \cap N \trianglelefteq HN = G$. From Lemma 4.15 it follows that $H \cap N \leq \Phi(G) = 1$, i. e. H is a complement of N in G. □

Remark 5.16. In the following, we investigate when a fixed normal subgroup possesses a complement. Every complement of $H \leq G$ is obviously a transversal for G/H. Conversely, we will construct complements by "smoothing" arbitrary transversals.

Definition 5.17. Let $A \trianglelefteq G$ be abelian and $A \leq H \leq G$. Let K be a complement of A in H. For $x, y \in G$ with $xH = yH$, there exists exactly one $\kappa_{x,y} \in K$ with $x^{-1}yA = \kappa_{x,y}A$. Let $\mathcal{R}$ be the set of transversals for G/H. For $R, S \in \mathcal{R}$ let

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

(since A is abelian, the order of the factors does not matter).

Lemma 5.18. *For $R, S, T \in \mathcal{R}$, $g \in G$ and $a \in A$ it holds that*

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

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

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

(iv) $(aR|S) = a^{|G:H|}(R|S)$.

Proof.

(i) From $\kappa_{r,r}A = A$ it follows that $(R|R) = 1$. Because of $\kappa_{r,s}^{-1}A = (r^{-1}s)^{-1}A = s^{-1}rA = \kappa_{s,r}A$ we have

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

(ii) From $\kappa_{r,s}\kappa_{s,t}A = r^{-1}ss^{-1}tA = r^{-1}tA = \kappa_{r,t}A$ it follows that

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

(iii) For $x, y \in R$ we have $gxH = gyH \Leftrightarrow xH = yH \Leftrightarrow x = y$. This shows $gR, gS \in \mathcal{R}$. Because of $\kappa_{gr,gs}A = (gr)^{-1}gsA = r^{-1}sA = \kappa_{r,s}$ we have

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

(iv) We have $\kappa_{ar,s}A = (ar)^{-1}sA = r^{-1}sA = \kappa_{r,s}A$. Since A is abelian, one can pull a out of the $|G:H|$ factors:

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

Remark 5.19. For $x, y \in G$ we write in the following $x^y := y^{-1}xy$ and $x^{-y} := (x^y)^{-1}$. Obviously $x^1 = x$, $(x^y)^z = x^{yz}$ and $(xy)^z = x^z y^z$ hold for $x, y, z \in G$.

Definition 5.20. Let $H \leq G$ be finite groups. A map $\alpha\colon G \to H$ with $\alpha(xy) = \alpha(x)^y\alpha(y)$ for all $x, y \in G$ is called a *crossed homomorphism*. As usual, let $\mathrm{Ker}(\alpha) := \{x \in G : \alpha(x) = 1\}$.

Lemma 5.21. *For every crossed homomorphism $\alpha\colon G \to H$, we have $\mathrm{Ker}(\alpha) \leq G$.*

Proof. From $\alpha(1) = \alpha(1 \cdot 1) = \alpha(1)^1\alpha(1) = \alpha(1)^2$ it follows that $\alpha(1) = 1$. For $x, y \in \mathrm{Ker}(\alpha)$ we have $\alpha(xy) = \alpha(x)^y\alpha(y) = 1^y 1 = 1$, thus $xy \in \mathrm{Ker}(\alpha)$. □

Theorem 5.22 (Gaschütz)**.** *Let $A \trianglelefteq G$ be abelian and $A \leq H \leq G$ with $\gcd(|A|, |G : H|) = 1$. Then:*

(i) If A has a complement in H, then also in G.

(ii) If L_1, L_2 are complements of A in G with $H \cap L_1 = H \cap L_2$, then L_1 and L_2 are conjugate in G.

(iii) If any two complements of A in H are conjugate, then any two complements of A in G are also conjugate.

Proof (Brandis).

(i) Let K be a complement of A in H and $R \in \mathcal{R}$ with the notation from Definition 5.17. For $x \in G$ let $\alpha(x) := (x^{-1}R|R) \in A$. According to Lemma 5.18 it holds that

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

for $x, y \in G$. Thus α is a crossed homomorphism and $L := \mathrm{Ker}(\alpha) \leq G$ according to Lemma 5.21. For $a \in A$ it holds that $\alpha(a) = (a^{-1}R|R) = a^{-|G:H|}(R|R) = a^{-|G:H|}$. Because of $\gcd(|A|, |G : H|) = 1$, the restriction $\alpha_{|A}$ is an automorphism of A. In particular, $L \cap A = 1$. For $g \in G$ there also exists an $a \in A$ with $1 = \alpha(g)\alpha(a) = \alpha(g)^a\alpha(a) = \alpha(ga)$. This shows $g = (ga)a^{-1} \in LA$. Thus L is a complement of A in G.

(ii) According to Example 5.4, $K := H \cap L_i$ is a complement of A in H. We construct $(R|S)$ with respect to K. Let $R_1, R_2 \in \mathcal{R}$ with $R_i \subseteq L_i$. For $i = 1, 2$ we construct α_i as in (i) with the help of R_i. For $x \in L_i$ and $r, s \in R_i$ it holds that

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

This shows

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

and $L_i \leq \mathrm{Ker}(\alpha_i)$. According to (i) we have $|L_i| = |\mathrm{Ker}(\alpha_i)|$, thus $L_i = \mathrm{Ker}(\alpha_i)$ for $i = 1, 2$.

Now let $a := (R_1|R_2) \in A$ and $x \in G$. According to (i) there exists $b \in A$ with $\alpha_2(b) = a$. It holds that

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

It follows that $L_2 = \mathrm{Ker}(\alpha_2) = b\mathrm{Ker}(\alpha_1)b^{-1} = bL_1b^{-1}$.

(iii) Let L_1, L_2 be complements of A in G. Then $H \cap L_1, H \cap L_2$ are complements of A in H. By assumption there exists $h \in H$ with $H \cap hL_1h^{-1} = h(H \cap L_1)h^{-1} = H \cap L_2$. The assertion now follows from (ii). □

Theorem 5.23. *Let $A \trianglelefteq G$ be abelian. A possesses a complement in G if and only if every Sylow subgroup of A possesses a complement in a Sylow subgroup of G.*

Proof. Let K be a complement of A in G and $K_p \in \mathrm{Syl}_p(K)$. Let $K_p \leq P \in \mathrm{Syl}_p(G)$. Since A is abelian, $A \cap P = \mathrm{O}_p(A) \trianglelefteq G$ is the unique Sylow p-subgroup of A and $(A \cap P) \cap K_p \leq A \cap K = 1$. Because $|A \cap P||K_p| = |A|_p|K|_p = |G|_p = |P|$, K_p is a complement of $A \cap P$ in P.

We prove the converse by induction on the number of prime divisors $p_1, \ldots, p_s$ of $|A|$. Let $P_1 \in \mathrm{Syl}_{p_1}(G)$. Then $A \cap P_1 = \mathrm{O}_{p_1}(A) \trianglelefteq G$ has a complement in P_1 and, by Gaschütz, also a complement K_1 in G. So let $s \geq 2$. For $i \geq 2$ let $P_i \in \mathrm{Syl}_{p_i}(K_1) \subseteq \mathrm{Syl}_{p_i}(G)$. Then $(A \cap K_1) \cap P_i = A \cap P_i$ has a complement in P_i. By induction, $A \cap K_1$ has a complement K in K_1. It now holds that $G = (A \cap P_1)K_1 = (A \cap P_1)(A \cap K_1)K \leq AK$ and $A \cap K = A \cap K_1 \cap K = 1$. □

Theorem 5.24 (Evans-Shin)**.** *Let K and L be complements of the abelian normal subgroup $A \trianglelefteq G$. If every Sylow subgroup of K is conjugate to a Sylow subgroup of L, then K and L are conjugate.*

Proof. Let G be a minimal counterexample. Let p be a prime divisor of $|A|$ and $B := \mathrm{O}_{p'}(A)$. Assume $B \neq 1$. Then KB/B and LB/B are complements of A/B in G/B. If P is a Sylow subgroup of K, then PB/B is a Sylow subgroup of KB/B. By assumption, there exists a $g \in G$ such that gKg^{-1} is a Sylow subgroup of L. Obviously, $gKg^{-1}B/B$ is a Sylow subgroup of LB/B. Since G is a minimal counterexample, there exists a $g \in G$ with $H := gKg^{-1}B = LB$. Now gKg^{-1} and L are complements of B in H with the same assumption. Because $B < A$, the contradiction follows that gKg^{-1} and L are conjugate in G. Thus $B = 1$ and A is a p-group. After conjugation, we may assume that K and L have a common Sylow p-subgroup P. Then $H := PA \in \mathrm{Syl}_p(G)$. Now the claim follows from Theorem 5.22(ii). □

Theorem 5.25. *Let K and L be complements of the abelian normal subgroup $A \trianglelefteq G$. Then there exists an $\alpha \in \mathrm{Aut}(G)$ with $\alpha(K) = L$ and $\alpha_A = \mathrm{id}_A$.*

Proof. Because $K \cong G/A \cong L$, there exists an isomorphism $\varphi\colon K \to L$ with $\varphi(x) \equiv x \pmod{A}$ for all $x \in K$. Since A is abelian, $\varphi(x)a\varphi(x)^{-1} = xax^{-1}$ for all $x \in K$ and $a \in A$. Obviously, $\alpha\colon G \to G$, $xa \mapsto \varphi(x)a$ for $x \in K$ and $a \in A$ is a well-defined bijection. For $x, y \in K$ and $a, b \in A$ it holds that

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

Thus $\alpha \in \mathrm{Aut}(G)$ with $\alpha(K) = \varphi(K) = L$ and $\alpha_A = \mathrm{id}_A$. □

Theorem 5.26. *Let G be a finite group with elementary abelian Sylow subgroups (for every prime). Then every normal subgroup of G possesses a complement.*

Proof. Let $N \trianglelefteq G$. We argue by induction on $|N|$. Suppose N possesses a non-normal Sylow p-subgroup P. According to Remark 4.6, $G = N\mathrm{N}_G(P)$ and $\mathrm{N}_N(P) < N$. By induction, $\mathrm{N}_N(P)$ possesses a complement K in $\mathrm{N}_G(P)$. It holds that $G = N\mathrm{N}_G(P) = N\mathrm{N}_N(P)K = NK$ and $N \cap K = N \cap \mathrm{N}_N(P) \cap K = 1$. We can therefore assume that N is nilpotent (Theorem 4.10). By assumption, N is even abelian and every Sylow subgroup of N possesses a complement in an (elementary abelian) Sylow subgroup of G (Example 5.4). The assertion now follows from Theorem 5.23. □

Remark 5.27. The simple group A_6 (see Theorem 6.38) with 2-Sylow subgroup D_8 shows that the converse of Theorem 5.26 is false.

Theorem 5.28. *For every solvable group G, the following statements are equivalent:*

(1) Every normal subgroup of G possesses a complement.

(2) For all $N \trianglelefteq G$, $\Phi(G/N) = 1$ holds.

Proof.

(1)⇒(2): Let $M/N := \Phi(G/N) \trianglelefteq G/N$. Let $K \leq G$ be a complement of M in G. Then

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

holds, hence $G = KN$. It follows that $M = KN \cap M = N(K \cap M) = N$, i. e. $\Phi(G/N) = 1$.

(2)⇒(1): Induction on $|G|$: Let $1 \neq N \trianglelefteq G$. Let $M \leq N$ be a minimal normal subgroup of G. Since G is solvable, M is (elementary) abelian. Because $\Phi(G) = \Phi(G/1) = 1$, M possesses a complement H in G according to Theorem 5.15. Because $H \cong G/M$, the assumption transfers from G to H by the second isomorphism theorem. By induction, $H \cap N \trianglelefteq H$ possesses a complement K in H. It holds that $G = HM = K(H \cap N)M \leq KN$ and $K \cap N = K \cap H \cap N = 1$, i. e. K is a complement of N in G. □

Theorem 5.29 (Schur-Zassenhaus)**.** *Let $N \trianglelefteq G$ with $\gcd(|N|, |G/N|) = 1$. Then N possesses a complement in G. If N or G/N is solvable, then any two complements of N in G are conjugate under N.*

Proof.

Step 1: Existence.
Induction on $|G|$: We may certainly assume $1 < N < G$. Let $1 \neq P \in \mathrm{Syl}_p(N)$. Then $\mathrm{N}_N(P) \trianglelefteq \mathrm{N}_G(P)$ and

$$\mathrm{N}_G(P)/\mathrm{N}_N(P) = \mathrm{N}_G(P)/\mathrm{N}_G(P) \cap N \cong \mathrm{N}_G(P)N/N \leq G/N.$$

In the case $\mathrm{N}_G(P) < G$, $\mathrm{N}_N(P)$ has a complement K in $\mathrm{N}_G(P)$ by induction. According to Remark 4.6, $G = N\mathrm{N}_G(P) = N\mathrm{N}_N(P)K = NK$ and $N \cap K = N \cap \mathrm{N}_G(P) \cap K = \mathrm{N}_N(P) \cap K = 1$. We can therefore assume $P \trianglelefteq G$. According to Theorem 4.8 and Lemma 2.26, $1 \neq \mathrm{Z}(P) \trianglelefteq G$ also holds. By induction, $N/\mathrm{Z}(P)$ has a complement $K/\mathrm{Z}(P)$ in $G/\mathrm{Z}(P)$. Then $G = NK$ and $N \cap K = \mathrm{Z}(P)$. It thus suffices to show that $\mathrm{Z}(P)$ has a complement in K. We can therefore assume that N is abelian. Then the claim follows from Gaschütz with $N = A = H$.

Step 2: Uniqueness.
Case 1: N solvable.
Induction on $|N|$: If N is abelian, the claim follows from Gaschütz with $N = A = H$. So let $1 < N' < N$. Let K_1 and K_2 be complements of N in G. Then K_1N'/N' and K_2N'/N' are complements of N/N' in G/N'. By induction, there exists an $x \in N$ with $xK_1x^{-1}N' = xK_1N'x^{-1} = K_2N'$. Thus xK_1x^{-1} and K_2 are complements of N' in K_2N'. By induction, there exists a $y \in N'$ with $yxK_1x^{-1}y^{-1} = K_2$.

Case 2: G/N solvable.
Induction on $|G/N|$: Let K_1 and K_2 be complements of N in G. Then $K_1 \cong G/N \cong K_2$ is solvable. Let M_1 be a minimal normal subgroup of K_1. According to Theorem 2.28, M_1 is an elementary abelian p-group. In the case $M_1 = K_1$, K_1 and K_2 are conjugate in G by Sylow. Because of $G = NK_1 = K_1N$,

K_1 and K_2 are then also conjugate under N. So let $M_1 < K_1$ and $M_2 := K_2 \cap NM_1 \trianglelefteq K_2$. According to Dedekind,

$$NM_2 = N(K_2 \cap NM_1) = NK_2 \cap NM_1 = NM_1.$$

Induction yields an $x \in N$ with $xM_1x^{-1} = M_2$. In particular, $xK_1x^{-1} \leq x\mathrm{N}_G(M_1)x^{-1} = \mathrm{N}_G(M_2)$ and $K_2 \leq \mathrm{N}_G(M_2)$. According to Dedekind, xK_1x^{-1}/M_2 and K_2/M_2 are complements of $\mathrm{N}_N(M_2)M_2/M_2$ in $\mathrm{N}_G(M_2)/M_2$. By induction, there exists a $y \in \mathrm{N}_N(M_2)$ with $yxK_1x^{-1}y^{-1}/M_2 = K_2/M_2$. The claim follows. □

Remark 5.30.

(i) From the condition $\gcd(|N|, |G/N|) = 1$ it follows that $|N|$ or $|G/N|$ is odd. According to the deep theorem of Feit and Thompson (groups of odd order are solvable), the solvability condition in Theorem 5.29 is actually redundant (the proof has 250 pages).

(ii) In contrast to Schur-Zassenhaus, Gaschütz's theorem is in general false for non-abelian normal subgroups A.[14]

Corollary 5.31. *For $N \trianglelefteq G$ there exists an $H \leq G$ with $G = NH$, such that $|H|$ and $|G/N|$ have the same prime divisors.*

Proof. Choose H as in Lemma 5.14 (if necessary $H = G$). Suppose $H \cap N$ contains a non-trivial Sylow p-subgroup P of H. Since $H \cap N \leq \Phi(H)$ is nilpotent, $P \trianglelefteq H$ holds. By Schur-Zassenhaus, P has a complement K in H. This leads to the contradiction $H = PK \leq \Phi(H)K = K$. Thus every prime divisor of $|H|$ is also a divisor of $|H : H \cap N| = |HN/N| = |G/N|$. □

Remark 5.32. Obviously Corollary 5.31 generalizes the Schur-Zassenhaus theorem. In Theorem 7.47 we will encounter another generalization.

Definition 5.33. Let π be a set of prime numbers. A subgroup $H \leq G$ is called a (π-)*Hall subgroup* of G if H is a π-group and no prime divisor of $|G : H|$ lies in π. In this case $\gcd(|H|, |G : H|) = 1$.

Example 5.34.

(i) The p-Hall subgroups are exactly the Sylow p-subgroups.

(ii) If G is nilpotent, then $\mathrm{O}_\pi(G)$ is the unique π-Hall subgroup of G (Theorem 4.10).

(iii) A_5 has *no* $\{3, 5\}$-Hall subgroup, because such a Hall subgroup would be cyclic of order 15 (Example 4.5). The following theorem therefore implies (again) that A_5 is not solvable.

Theorem 5.35 (Hall). *Let G be solvable and π a set of prime numbers. Then*

(i) G possesses a π-Hall subgroup.

(ii) Any two π-Hall subgroups are conjugate in G.

(iii) Every π-subgroup of G is contained in a π-Hall subgroup.

[14] The central product (see Definition 9.14) $G = \mathrm{SL}(2, 3) * C_4$ with $A \cong Q_8$ and $H = Q_8 * C_4$ is a counterexample for Theorem 5.22(i) and $G = \mathrm{GL}(2, 3)$ with $A = \mathrm{O}_2(G) \cong Q_8$ and $H \in \mathrm{Syl}_2(G)$ is a counterexample for (ii) and (iii).

Proof. We can assume that all prime numbers in π divide the group order $|G|$. We write $|G| = rs$ with $\gcd(r, s) = 1$, where π is the set of prime divisors of r. We first show (iii) by induction on $|G|$. Obviously, we may assume $G \neq 1$. Let $U \leq G$ with $|U| \mid r$. Let M be a minimal normal subgroup of G. Since G is solvable, $|M| = p^n$ for a prime power $p^n > 1$. First, let $p^n \mid r$ and $r' := r/p^n$. Then $|G/M| = r's$ and induction shows $UM/M \leq K/M \leq G/M$ with $|K/M| = r'$. Certainly then $U \leq K$ and $|K| = r$. We can now assume $p^n \mid s$. Then by induction again $UM/M \leq K/M \leq G/M$ with $|K/M| = r$. Thus one has $|K| = p^n r$ and Schur-Zassenhaus yields an $L \leq K$ with $|L| = r$. Obviously,

$$M(L \cap UM) = ML \cap UM = K \cap UM = UM$$

and thus $|L \cap UM| = |U|$. Again by Schur-Zassenhaus (applied to $M \trianglelefteq MU$), there exists a $g \in M$ with $U = g(L \cap UM)g^{-1} \leq gLg^{-1}$. This proves (iii) and with $U = 1$ we obtain (i).

Now let H and K be subgroups of G of order r. By induction, HM/M and KM/M are conjugate in G/M. In particular, there exists a $g \in G$ with $gHg^{-1} \leq KM$. By Schur-Zassenhaus, gHg^{-1} and K are then also conjugate (in KM). This implies (ii). □

Remark 5.36.

(i) Conversely, one can show that G is solvable if p'-Hall subgroups exist for every prime divisor p of $|G|$ (see subsection A.1). This generalizes Burnside's $p^a q^b$-theorem.

(ii) Gross proved in the case $2 \notin \pi$ that any two π-Hall subgroups of an arbitrary finite group are conjugate. The proof uses the CFSG. More generally, the existence of π-Hall subgroups can be read from the composition factors. If, for example, all composition factors are π-groups or π'-groups (one then calls G *π-separable*), then Hall's statements hold for π. However, the proof requires Schur-Zassenhaus without the solvability condition (cf. Remark 5.30).

Theorem 5.37. *Let G be supersolvable of order n. Then G has a subgroup of order d for every divisor d of n.*

Proof. Induction on $|G|$. Let N be a minimal normal subgroup of G. One can extend N to a chief series of G. By assumption, $p = |N|$ is a prime number and G/N is also supersolvable. In the case $p \mid d$, G/N has a subgroup H/N of order d/p by induction. Then $|H| = d$. Now let $p \nmid d$. Then G/N has a subgroup H/N of order d. By Schur-Zassenhaus (or Hall), N has a complement of order d in H. □

Definition 5.38. Let $p_1, \ldots, p_n$ be the prime divisors of $|G|$ and $P_i \in \mathrm{Syl}_{p_i}(G)$. One calls $(P_1, \ldots, P_n)$ a *Sylow system* of G, if $P_i P_j \leq G$ holds for all $1 \leq i, j \leq n$ (according to Lemma 1.9 this is equivalent to $P_i P_j = P_j P_i$). Let $\mathcal{S}(G)$ be the set of all Sylow systems of G.

Lemma 5.39. *Let $p_1, \ldots, p_n$ be the prime divisors of $|G|$. Let $\mathcal{H}$ be the set of all sequences $(H_1, \ldots, H_n)$, such that H_i is a p_i'-Hall group of G for $i = 1, \ldots, n$. Then the maps*

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

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

are mutually inverse bijections.

Proof. Let $|G| = p_1^{a_1} \dots p_n^{a_n}$ be the prime factorization of $|G|$ and $(H_1, \dots, H_n) \in \mathcal{H}$. We show $|G : H_{i_1} \cap \dots \cap H_{i_k}| = p_{i_1}^{a_1} \dots p_{i_k}^{a_k}$ for $1 \leq i_1 < \dots < i_k \leq n$ by induction on k. The case $k = 1$ is the Hall group property. Since $|G : H|$ and $|G : H_{i_1}|$ are coprime, it follows

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

from Lemma 1.9. The case $k = n - 1$ yields $P_i := \bigcap_{j \neq i} H_j \in \mathrm{Syl}_{p_i}(G)$ for $i = 1, \dots, n$. Because of $P_i P_j \subseteq \bigcap_{i \neq l \neq j} H_l$ and $|\bigcap_{i \neq l \neq j} H_l| = |P_i||P_j|$, we have

$$P_i P_j = \bigcap_{i \neq l \neq j} H_l = P_j P_i.$$

This shows $(P_1, \dots, P_n) \in \mathcal{S}(G)$.

Conversely, let $(P_1, \dots, P_n) \in \mathcal{S}(G)$ be given. We show $P_{i_1} \dots P_{i_k} \leq G$ for $i_1 < \dots < i_k$. This is clear for $k = 1$. Let $P := P_{i_2} \dots P_{i_k} \leq G$. From the property of the Sylow system it follows

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

Obviously $H_i := \prod_{j \neq i} P_j$ is a p_i'-Hall group and $(H_1, \dots, H_n) \in \mathcal{H}$. Because of

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

the specified maps are mutually inverse. □

Remark 5.40. We call Sylow systems (P_i) and (Q_i) of G *conjugate*, if there exists a g with $gP_ig^{-1} = Q_i$ for all i. The following theorem is a generalization of Sylow for solvable groups.

Theorem 5.41 (Hall)**.** *Every solvable group G possesses a Sylow system and any two Sylow systems of G are conjugate.*

Proof. Let $p_1, \dots, p_n$ be the prime divisors of $|G|$. According to Hall, G possesses a p_i'-Hall subgroup H_i for each i. According to Lemma 5.39, $S := (P_1, \dots, P_n)$ with $P_i := \bigcap_{j \neq i} H_j$ is a Sylow system of G. Because of $H_i = \prod_{j \neq i} P_j$, it holds that $\bigcap_{i=1}^n \mathrm{N}_G(H_i) = \bigcap_{i=1}^n \mathrm{N}_G(P_i)$. Since Hall subgroups of the same order are conjugate, $|G : \mathrm{N}_G(H_i)|$ is the number of p_i'-Hall subgroups in G. Because of $H_i \leq \mathrm{N}_G(H_i)$, $|G : \mathrm{N}_G(H_i)|$ is a p_i-power. In particular, the $|G : \mathrm{N}_G(H_i)|$ are pairwise coprime. From Lemma 1.9 and Lemma 5.39 it follows that

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

This shows that every Sylow system is conjugate to S. □

Theorem 5.42 (Hall-Higman Lemma)**.** *Let every composition factor of G be a π-group or a π'-group. If $\mathrm{O}_\pi(G) = 1$ holds, then $\mathrm{C}_G(\mathrm{O}_{\pi'}(G)) \leq \mathrm{O}_{\pi'}(G)$.*

Proof. Let $N := \mathrm{O}_{\pi'}(G)$. Then $\mathrm{C}_G(N)N/N \trianglelefteq G/N$. In the case $\mathrm{C}_G(N) \not\subseteq N$, there exists a minimal normal subgroup $M/N \trianglelefteq G/N$ with $M \leq \mathrm{C}_G(N)N$. As a chief factor, M/N is a direct sum of isomorphic composition factors (Theorem 2.28). Because of $\mathrm{O}_{\pi'}(G/N) = 1$, M/N must be a π-group by assumption. According to Schur-Zassenhaus, $M = N \rtimes H$ with $H \neq 1$. Since $\mathrm{C}_G(N)N/\mathrm{C}_G(N) \cong N/\mathrm{Z}(N)$ is a π'-group, it holds that $H \leq \mathrm{C}_G(N)$ and $M = N \times H$. But then $H \leq \mathrm{O}_\pi(M) \leq \mathrm{O}_\pi(G) = 1$. □

Theorem 5.43 (Galois)**.** *Let N be a minimal normal subgroup of the solvable group G with $\mathrm{C}_G(N) \leq N$. Then N possesses a complement in G and any two complements are conjugate in G.*

Proof. As is well known, N is an elementary abelian p-group for a prime p. We can assume $N < G$. Let M/N be a minimal normal subgroup of G/N. Then M/N is an elementary abelian q-group for a prime q. First, assume $q = p$. Then M is a p-normal subgroup of G and M. According to Theorem 3.14, $1 \neq \mathrm{Z}(M) \cap N \trianglelefteq G$. Since N is minimal, it follows that $N \subseteq \mathrm{Z}(M)$ and $M \subseteq \mathrm{C}_G(N) = N$. This contradiction shows $q \neq p$. Let $Q \in \mathrm{Syl}_q(M)$. Then $M = QN$ and

$$G = \mathrm{N}_G(Q)M = \mathrm{N}_G(Q)QN = \mathrm{N}_G(Q)N$$

according to Remark 4.6. Obviously, $\mathrm{N}_N(Q) = \mathrm{N}_G(Q) \cap N \trianglelefteq \mathrm{N}_G(Q)$. Since N is abelian, $\mathrm{N}_N(Q) \trianglelefteq N$ also holds. In total, $\mathrm{N}_N(Q) \trianglelefteq G$. The minimality of N shows $\mathrm{N}_N(Q) \in \{1, N\}$. Assume that the case $N \subseteq \mathrm{N}_G(Q)$ occurs. As above, then $G = \mathrm{N}_G(Q)N = \mathrm{N}_G(Q)$, so $Q \trianglelefteq G$. For order reasons, $N \cap Q = 1$ and thus $Q \subseteq \mathrm{C}_G(N) = N$ (Lemma 2.5). Contradiction. Thus $\mathrm{N}_N(Q) = 1$ and $\mathrm{N}_G(Q)$ is a complement of N.

Now let $K \leq G$ be any complement of N in G. Then $L := K \cap M \trianglelefteq K$ and $M = NK \cap M = N(K \cap M) = NL$ according to Dedekind. Because of $L \cap N \subseteq K \cap N = 1$, $|L| = |M : N| = |Q|$. According to Sylow, there exists an $x \in M$ with $xQx^{-1} = L$. It follows that $K \leq \mathrm{N}_G(L) = \mathrm{N}_G(xQx^{-1}) = x\mathrm{N}_G(Q)x^{-1}$. Because of $|K| = |\mathrm{N}_G(Q)|$, K is conjugate to $\mathrm{N}_G(Q)$. This shows the second assertion. □

Remark 5.44. The following theorem is useful for the construction of minimal counterexamples.

Theorem 5.45 (Schmidt)**.** *Let every proper subgroup of G be nilpotent, but G itself not. Then $G \cong Q \rtimes C_{p^n}$ with $Q \in \mathrm{Syl}_q(G)$ for primes p, q and $n \geq 1$.*

Proof. Induction on $|G|$: Let us first assume there exists a proper normal subgroup $N \neq 1$. By assumption, N is nilpotent. For $U/N < G/N$, $U < G$ is nilpotent and thus also U/N. By induction, G/N is solvable. Therefore, G is also solvable. Now assume that G is non-abelian and simple. Let M_1 and M_2 be two distinct maximal subgroups of G such that $D := M_1 \cap M_2$ is as large as possible. Assume $D \neq 1$. According to Theorem 4.10, it then follows that

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

for $i = 1, 2$. Now $\mathrm{N}_G(D)$ lies in a maximal subgroup $M_3 < G$. Because of $\mathrm{N}_{M_i}(D) \leq M_i \cap M_3$, it follows that $M_i = M_3$ by the choice of M_1 and M_2. However, this yields the contradiction $M_1 = M_3 = M_2$. Thus $D = 1$, i. e. any two distinct maximal subgroups of G intersect trivially. Let $M_1, \ldots, M_s$ be a system of representatives for the conjugacy classes of maximal subgroups. Because of $\mathrm{N}_G(M_i) = M_i$, M_i has exactly $|G : M_i|$ conjugates. It therefore holds that

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

and $s = 1$. But then $|G| = 1 + |G| - |G : M_1|$ and $M_1 = G$. This contradiction finally shows that G is solvable.

Now let $|G| = p_1^{a_1} \ldots p_m^{a_m}$ be the prime factorization of $|G|$. Since G is not nilpotent, $m \geq 2$ holds. Let N be a maximal normal subgroup of G. Then G/N is simple and solvable. Thus $|G/N|$ is a prime number, say $|G/N| = p_1 =: p$. By assumption, N is nilpotent and therefore possesses normal Sylow subgroups $P_i \in \mathrm{Syl}_{p_i}(N)$ for $i = 2, \ldots, m$. Obviously, $P_i \in \mathrm{Syl}_{p_i}(G)$ then. Furthermore, P_i is characteristic in N

and thus normal in G. Let also $P_1 \in \mathrm{Syl}_p(G)$. Assume indirectly $m \geq 3$. For $i = 2, \ldots, m$, $P_1 P_i < G$ is then nilpotent. This shows $P_i \leq \mathrm{N}_G(P_1)$ and $P_1 \trianglelefteq G$. But then G would be nilpotent. Thus $m = 2$ and we can set $Q := P_2$. Finally, assume that P_1 is not cyclic. For $x \in P_1$, $\langle x \rangle P_2 < G$ then holds and $P_2 \leq \mathrm{C}_G(x)$. But then $P_2 \leq \mathrm{C}_G(P_1)$ and again $P_1 \trianglelefteq G$. Consequently, P_1 must be cyclic and the claim is proven. □

Theorem 5.46 (Wielandt)**.** *Let $H \leq G$ be a nilpotent Hall subgroup and $U \leq G$ with $|U| \mid |H|$. Then there exists a $g \in G$ with $gUg^{-1} \leq H$. In particular, all subgroups of order $|H|$ are conjugate to H and therefore nilpotent.*

Proof. Induction on $|U|$. wlog. let $U \neq 1$. Every proper subgroup of U is then conjugate to a subgroup of H. In particular, every proper subgroup of U is nilpotent. By Theorem 5.45, there exists a decomposition $U = Q \rtimes P$ with $1 \neq P \in \mathrm{Syl}_p(U)$ and $Q \trianglelefteq U$ (even if U is nilpotent). Analogously, $H = H_1 \oplus H_2$ with $H_1 \in \mathrm{Syl}_p(H) \subseteq \mathrm{Syl}_p(G)$. By induction, there exists an $x \in G$ with $xQx^{-1} \leq H$ and thus $xQx^{-1} \leq \mathrm{O}_{p'}(H) = H_2$. Then $\langle H_1, xUx^{-1} \rangle \leq \mathrm{N}_G(xQx^{-1})$ holds. Because $H_1 \in \mathrm{Syl}_p(\mathrm{N}_G(xQx^{-1}))$, there exists a $y \in \mathrm{N}_G(xQx^{-1})$ with $yxPx^{-1}y^{-1} \leq H_1$. Because $yxQx^{-1}y^{-1} = xQx^{-1} \leq H_2$, it follows that

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

6 Permutation Groups

Definition 6.1. A *permutation group* G is a subgroup of $\mathrm{Sym}(\Omega)$ for a non-empty set Ω. Here, $|\Omega|$ is the *degree* of G.

Remark 6.2.

(i) If G acts faithfully on Ω, then one obtains a monomorphism $f \colon G \to \mathrm{Sym}(\Omega)$. One can thus identify G with the permutation group $f(G)$. Conversely, every permutation group $G \leq \mathrm{Sym}(\Omega)$ acts faithfully on Ω by means of $G \hookrightarrow \mathrm{Sym}(\Omega)$.

(ii) If $f \colon G \to \mathrm{Sym}(\Omega)$ is an arbitrary action, then $G/\mathrm{Ker}(f)$ becomes a permutation group.

Theorem 6.3 (Cayley)**.** *Every group acts faithfully on itself and thus becomes a permutation group.*

Proof. We consider the action $f \colon G \to \mathrm{Sym}(G)$ by left multiplication. For $x \in \mathrm{Ker}(f)$, we have $1 = {}^x 1 = x1 = x$. Thus f is faithful. □

Theorem 6.4 (Burnside's Lemma)**.** *Let s be the number of orbits of an action of the finite group G on Ω. Let $f(g) := |\{\omega \in \Omega : {}^g\omega = \omega\}|$ be the number of fixed points of $g \in G$. Then*

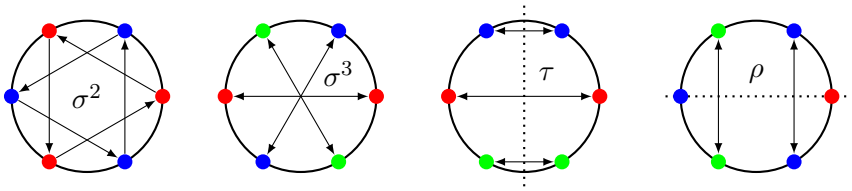
$$s = \frac{1}{|G|} \sum_{g \in G} f(g).$$

Proof. In the case $s = \infty$, we also have $f(1) = |\Omega| = \infty$ and the equation holds. So let $s < \infty$. Let $\omega_1, \ldots, \omega_s$ be representatives for the orbits of G. For $x \in G$ and $\omega \in \Omega$, we have $G_{{}^x\omega} = xG_\omega x^{-1}$. In particular, $|G_{\omega_i}|$ does not depend on the choice of ω_i. It now holds that

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

Example 6.5. We count necklaces with six beads, where beads in three colors are available. Naively, there are initially 3^6 such necklaces, of which some are however identical. We arrange the necklace such that the beads form a regular 6-gon. Rotation by $\pi/3$ will not change the necklace. Likewise, we can rotate the necklace in space and thereby realize a reflection of the 6 vertices. Two necklaces are thus identical if and only if they lie in the same orbit under the dihedral group $G := D_{12}$ (see Exercise 8). We apply Burnside's Lemma to the set Ω of the 3^6 necklaces.

Certainly $f(1) = 3^6$. A rotation $\sigma \in G$ by $\pi/3$ leaves only the three monochromatic necklaces fixed, i. e. $f(\sigma) = 3$. The rotation σ^2 by $2\pi/3$ leaves the monochromatic necklaces and the necklaces with alternating colors fixed. There are $f(\sigma^2) = 3^2$ of these. Analogously, one shows $f(\sigma^3) = 3^3$. Furthermore, $f(\sigma^4) = f(\sigma^{-2}) = 3^2$, $f(\sigma^5) = f(\sigma^{-1}) = 3$ as well as $\sigma^6 = 1$. Now let τ be one of the three reflections through two midpoints of sides. Then $f(\tau) = 3^3$. If finally ρ is one of the three reflections through two vertices, then $f(\rho) = 3^4$ holds.



According to Burnside's Lemma, there are

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

different necklaces.

Remark 6.6. Burnside's Lemma is always useful when $|\Omega|$ is too large to count the orbits explicitly. For example, there are $43,252,003,274,489,856,000$ different states of the $3 \times 3 \times 3$ Rubik's Cube. Under the symmetry group $S_4 \times C_2$ of the cube, this number reduces to $901,083,404,981,813,616$.

Definition 6.7. Two actions $G \to \mathrm{Sym}(\Omega)$ and $G \to \mathrm{Sym}(\Omega')$ are *isomorphic* if there exists a bijection $\varphi\colon \Omega \to \Omega'$ and an $\alpha \in \mathrm{Aut}(G)$ with ${}^{\alpha(g)}\varphi(\omega) = \varphi({}^g\omega)$ for $g \in G$ and $\omega \in \Omega$. If applicable, Ω and Ω' are *isomorphic G-sets*. In applications, often $\alpha = \mathrm{id}_G$.

Remark 6.8. As usual, two isomorphic actions have the same properties (trivial, faithful, transitive, ...). One is therefore usually only interested in actions up to isomorphism.

Theorem 6.9. *Let $\omega_1, \ldots, \omega_s$ be a transversal for the orbits of an action $f\colon G \to \mathrm{Sym}(\Omega)$. Then f is isomorphic to the action of G on $\Delta := \bigsqcup_{i=1}^{s} G/G_{\omega_i}$ (disjoint union) by left multiplication.*

Proof. According to Theorem 1.22, the map $\varphi\colon \Delta \to \Omega$, $gG_{\omega_i} \mapsto {}^g\omega_i$ is a well-defined bijection. For $g \in G$ and $xG_{\omega_i} \in \Delta$, it also holds that ${}^g\varphi(xG_{\omega_i}) = {}^g({}^x\omega_i) = {}^{gx}\omega_i = \varphi(gxG_{\omega_i}) = \varphi({}^g(xG_{\omega_i}))$. □

Remark 6.10. One can therefore describe every action of G by specifying subgroups (one subgroup per orbit).

Definition 6.11. A transitive action $G \to \mathrm{Sym}(\Omega)$ is called *regular* if $|G| = |\Omega|$ holds.

Remark 6.12. Let $f\colon G \to \mathrm{Sym}(\Omega)$ be regular and let $\omega \in \Omega$. Since f is transitive, $|G| = |\Omega| = |G : G_\omega|$ holds, i. e. $G_\omega = 1$. In particular, f is faithful. According to Theorem 6.9, f is isomorphic to the action from Theorem 6.3. One can therefore speak of "the" regular action of G.

Definition 6.13. Let $f\colon G \to \mathrm{Sym}(\Omega)$ be a transitive, non-trivial action. A subset $\Delta \subseteq \Omega$ with $1 < |\Delta| < |\Omega|$ is called a *block* of f if for every $g \in G$ the sets ${}^g\Delta$ and Δ are either equal or disjoint. If blocks exist, then f is called *imprimitive* and otherwise *primitive*.

Remark 6.14.

(i) Let Δ be a block of an action $G \to \mathrm{Sym}(\Omega)$ and let $x \in G$. Then certainly $|{}^x\Delta| = |\Delta|$. For $g \in G$ we have ${}^g({}^x\Delta) \cap {}^x\Delta = {}^{gx}\Delta \cap {}^x\Delta = {}^x({}^{x^{-1}gx}\Delta \cap \Delta) \in \{{}^x\Delta, \varnothing\}$. Therefore ${}^x\Delta$ is also a block. Since G acts transitively on Ω, $\mathcal{B} := \{{}^g\Delta : g \in G\}$ is a partition of Ω. In particular $|\Omega| = |\Delta||\mathcal{B}|$ and $\boxed{|\Delta| \mid |\Omega| \mid |G|.}$ Furthermore, G certainly acts transitively on $\mathcal{B}$.

(ii) Note: For non-transitive actions, blocks are not defined!

Example 6.15.

(i) According to Remark 6.14, every transitive action with prime degree is primitive.

(ii) According to (i), the natural actions of S_2, S_3 and A_3 are primitive. Now let $n \geq 4$ and $\Delta \subseteq \{1, \ldots, n\}$ with $1 < |\Delta| < n$. For distinct elements $\alpha, \beta \in \Delta$ there then exists a 3-cycle $g \in A_n$ with ${}^g\alpha = \alpha$ and ${}^g\beta \in \Omega \setminus \Delta$. Thus Δ is not a block and S_n and A_n are primitive.

(iii) The *Klein four-group* $V_4 := \langle (1,2)(3,4), (1,3)(2,4) \rangle$ acts regularly and imprimitively on $\{1,2,3,4\}$ (every 2-element subset is a block).

Theorem 6.16. *Let $G \to \mathrm{Sym}(\Omega)$ be a transitive action and $\omega \in \Omega$. Then the map $H \to {}^H\omega$ is a bijection between the set of subgroups $H \leq G$ with $G_\omega < H < G$ and the set of blocks containing ω. In particular, G is primitive if and only if G_ω is a maximal subgroup.*

Proof. According to Theorem 6.9 we can assume $\Omega = G/G_\omega$. The point ω corresponds to the trivial coset $1G_\omega$. For $G_\omega < H < G$, H/G_ω is a block containing $1G_\omega$, because $1 < |H : G_\omega| < |\Omega|$ and $gH \cap H \in \{H, \varnothing\}$ for $g \in G$. Conversely, let $\Delta \subseteq \Omega$ be a block containing $1G_\omega$. Let

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

For $x, y \in H$ we have $xG_\omega = x(1G_\omega) \in \Delta \cap x\Delta$. Since Δ is a block, it follows that $xyG_\omega \in x\Delta = \Delta$ and $xy \in H$. This shows $H \leq G$. Obviously also $|G_\omega| < |\Delta||G_\omega| = |H| < |G|$. □

Theorem 6.17. *Let $G \to \mathrm{Sym}(\Omega)$ be an imprimitive action with block Δ chosen maximal with respect to inclusion. Then the action of G on $\mathcal{B} := \{{}^g\Delta : g \in G\}$ is primitive.*

Proof. Again, we may assume $\Omega = G/G_\omega$ with $\omega \in \Omega$ according to Theorem 6.9. According to Theorem 6.16, $\Delta = H/G_\omega$ for a maximal subgroup $H < G$. We already know that G acts transitively on $\mathcal{B}$ (Remark 6.14). In this case, H is precisely the stabilizer of $\Delta \in \mathcal{B}$. According to Theorem 6.16, the action on $\mathcal{B}$ is primitive. □

Remark 6.18.

(i) Let $G \neq 1$ be a permutation group on Ω. According to Remark 6.2, there exists a normal subgroup $N_1 \trianglelefteq G$ such that $G/N_1 \neq 1$ is a transitive permutation group (on an orbit of Ω). Furthermore, according to Theorem 6.17, there exists a normal subgroup $N_2/N_1 \trianglelefteq G/N_1$ such that $(G/N_1)/(N_2/N_1) \cong G/N_2$ is a primitive permutation group. Since N_2 also acts faithfully on Ω, one can repeat this process with N_2 instead of G. This yields a sequence of subgroups $1 = G_1 \trianglelefteq G_2 \trianglelefteq \ldots \trianglelefteq G_k = G$ such that the factors G_i/G_{i-1} are primitive permutation groups. In contrast to composition factors or chief factors, the factors G_i/G_{i-1} are, however, in no way unique.

(ii) Let G be a simple group and $M < G$ a maximal subgroup. According to Exercise 5 and Theorem 6.16, G acts faithfully and primitively on G/M (M is the stabilizer of the trivial coset). If one knows all maximal subgroups of simple groups, then one can classify all primitive permutation groups using the Aschbacher-O'Nan-Scott theorem. For example, every primitive permutation group of degree 34 is isomorphic to A_{34} or S_{34}.[15] The determination of the maximal subgroups of the Monster group (and thus of all sporadic groups) was completed in 2024.[16] In the following, we describe the primitive groups.

Lemma 6.19. *Let $G \to \mathrm{Sym}(\Omega)$ be an action and let $N \trianglelefteq G$ be regular. For $\omega \in \Omega$, the action of G_ω on Ω is then isomorphic to the action on N by conjugation.*

Proof. By assumption, the map $\varphi\colon N \to \Omega$, $x \mapsto {}^x\omega$ is a bijection. For $g \in G_\omega$ and $x \in N$, we have ${}^g\varphi(x) = {}^{gx}\omega = {}^{(gxg^{-1})g}\omega = {}^{gxg^{-1}}\omega = \varphi({}^g x)$. □

Lemma 6.20. *Let $G \to \mathrm{Sym}(\Omega)$ be a primitive action and $N \trianglelefteq G$. Then N acts trivially or transitively on Ω.*

Proof. Let $\Delta \subseteq \Omega$ be a non-trivial orbit of N (i. e. $|\Delta| > 1$). For $g \in G$, ${}^g\Delta$ is then an orbit of $gNg^{-1} = N$. Thus ${}^g\Delta \cap \Delta \in \{\Delta, \varnothing\}$. The primitivity of G yields $\Delta = \Omega$, i. e. N is transitive. □

Theorem 6.21. *Let G be a primitive permutation group on Ω and let $N \neq 1$ be a solvable normal subgroup of G. Then G has exactly one minimal normal subgroup A. Furthermore, $\mathrm{C}_G(A) = A$ and $|\Omega| = |A| = p^n$ for a prime power p^n. Finally, $G = A \rtimes G_\omega$ for $\omega \in \Omega$.*

Proof. Let $A := N^{(k)} > N^{(k+1)} = 1$ (where $N^{(0)} := N$). Then A is abelian and characteristic in N. Thus $A \trianglelefteq G$. According to Lemma 6.20, A acts transitively. For $\omega \in \Omega$, it therefore holds that

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

Thus A is regular and $|A| = |\Omega|$. For every further abelian normal subgroup $1 \neq B \trianglelefteq G$, $|B| = |\Omega|$ must also hold. In particular, A is minimal and $|A|$ is a prime power. Moreover, $A \subseteq \mathrm{C}_G(A) =: C$. For $\omega \in \Omega$ and $a \in A$, it holds as before that $C_\omega = aC_\omega a^{-1} = C_{a\omega}$. Therefore C is also regular and $A = C = \mathrm{C}_G(A)$. If there were another minimal normal subgroup $B \trianglelefteq G$, then $A \cap B = 1$ and $B \leq \mathrm{C}_G(A) = A$. Thus A is the unique minimal normal subgroup. By the Frattini argument, $G = AG_\omega$ and $A \cap G_\omega = A_\omega = 1$. This shows $G = A \rtimes G_\omega$. □

[15] See Table 3 and OEIS.
[16] see arXiv:2411.12230

Remark 6.22.

(i) In the situation of Theorem 6.21, A is an n-dimensional vector space over $\mathbb{F}_p$. Because of $C_G(A) = A$, G_ω acts faithfully on A, i. e. $G_\omega \leq \mathrm{GL}(n,p)$. Since A is minimal, G_ω acts *irreducibly* on A, i. e. 1 and A are the only G_ω-invariant subspaces of A.

(ii) We concern ourselves with the converse of Theorem 6.21. Let $V \cong \mathbb{F}_p^n$ and $H \leq \mathrm{GL}(n,p)$ be irreducible on V. We show that then $G := V \rtimes H$ is a primitive permutation group. Since H acts faithfully on V, $C_G(V) = V$. We consider the action $\varphi\colon G \to \mathrm{Sym}(G/H)$ by left multiplication. For $x \in \mathrm{Ker}(\varphi)$, it holds that $H = 1H = xH$ and $x \in H$. Thus $\mathrm{Ker}(\varphi) \subseteq H$ (cf. Exercise 5). Because of $\mathrm{Ker}(\varphi) \cap V \leq H \cap V = 1$, it follows that $\mathrm{Ker}(\varphi) \leq C_G(V) \leq V$ and $\mathrm{Ker}(\varphi) = 1$. Thus G is a permutation group on G/H. Obviously, H is the stabilizer of the trivial coset $1H$. To show that G is primitive, we can prove according to Theorem 6.16 that H is maximal in G. So let $H < M \leq G$. Then $1 \neq M \cap V \trianglelefteq M$, because $|M : M \cap V| = |MV : V| = |G : V| = |VH : V| = |H|$. Since V is abelian, $M \cap V \trianglelefteq V$ also holds. Overall, $M \cap V \trianglelefteq VM = VH = G$. Since H acts irreducibly, $V \leq M$. But then $G = VH \leq M$. Thus H is maximal and G is a primitive permutation group.

Example 6.23.

(i) Let $V \cong C_p^n$. According to linear algebra, $\mathrm{GL}(n,p)$ acts irreducibly on V. Therefore, the *affine group*

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

is primitive of degree p^n. For $p = n = 2$, one obtains $\mathrm{AGL}(2,2) \cong V_4 \rtimes S_3 \cong S_4$, because S_4 is the largest permutation group of degree 4 and $|\mathrm{AGL}(2,2)| = 24$. We now try to construct smaller groups. For this, we consider V as the additive group of the field $\mathbb{F}_{p^n}$. For $\gamma \in \mathbb{F}_{p^n}^\times$, the map $f_\gamma\colon V \to V$, $v \mapsto \gamma v$ is certainly linear and bijective. Thus, there exists a monomorphism $f\colon \mathbb{F}_{p^n}^\times \to \mathrm{Aut}(V) \cong \mathrm{GL}(n,p)$, $\gamma \mapsto f_\gamma$ with image S. As is well known,

$$S \cong \mathbb{F}_{p^n}^\times \cong C_{p^n-1}$$

(Algebra or Theorem 9.8). Let $s \in S$ be a generator. Since every non-trivial power of s has only the trivial fixed point 0 on V, s corresponds to a cycle of length $p^n - 1$ in $\mathrm{Sym}(V)$. In particular, S acts transitively on $V \setminus \{0\}$. Therefore, S is irreducible and $V \rtimes S$ is a primitive permutation group. S is called a *Singer cycle*. In the case $n = 1$, certainly $V \rtimes S = \mathrm{AGL}(1,p) \cong C_p \rtimes C_{p-1}$. For $p = n = 2$, one obtains $V_4 \rtimes C_3 \cong A_4$ (the only subgroup of index 2 in S_4).

(ii) Theorem 6.21 shows that there is no primitive solvable group of degree 6. In particular, A_6 is not solvable.

(iii) The next theorem shows that Sylow's theorem is optimal.

Theorem 6.24 (McCarthy)**.** *Let $d \in \mathbb{N}$ not be a prime power. Then there exists a finite group G whose order is divisible by d and which has no subgroup of order d.*

Proof. By assumption, d has a prime divisor p with $d = p^a n$, $p \nmid n$ and $p^a < \sqrt{d}$. For the order e of $p + n\mathbb{Z} \in (\mathbb{Z}/n\mathbb{Z})^\times$, it holds that $p^a < \sqrt{d} < n < p^e$. Let

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

Then d is a divisor of $|G| = p^e(p^e - 1)$. Suppose $H \leq G$ has order d. Like G, H also has a normal Sylow p-subgroup P. Because $H/P \leq \mathbb{F}_{p^e}^\times$, the orbits of the conjugation action of H on $P \setminus \{1\}$ have length n. In particular, $\sqrt{d} < n < |P| = p^a$. Contradiction. □

Theorem 6.25 (Galois)**.** *Let $\alpha \in \mathbb{Q}[X]$ be irreducible with prime degree p. Then the following statements are equivalent:*

(1) α is solvable by radicals.

(2) The Galois group of α lies in $\mathrm{AGL}(1,p) \cong C_p \rtimes C_{p-1}$.

(3) For any two distinct roots $x, y \in \mathbb{C}$ of α, $\mathbb{Q}(x,y)$ is a splitting field of α.

Proof. According to the fundamental theorem of algebra, α has exactly p pairwise distinct roots $x_1, \ldots, x_p \in \mathbb{C}$. Let $G := \mathrm{Gal}(\mathbb{Q}(x_1, \ldots, x_p)|\mathbb{Q})$ be the Galois group of α. Since α is irreducible, G acts faithfully and transitively on $\{x_1, \ldots, x_p\}$. Since p is a prime number, G even acts primitively.

(1)⇒(2): Since α is solvable, G is also solvable. Therefore, (2) follows from Theorem 6.21.

(2)⇒(3): Let $G \leq \mathrm{AGL}(1,p)$. Since G acts transitively, p is a divisor of $|G|$. Thus $G = N \rtimes G_x$ with $N \cong C_p$. The action of G_x on $\{x_1, \ldots, x_p\}$ is isomorphic to the action on N. This shows $G_x \cap G_y = 1$. According to the fundamental theorem of Galois theory, $|\mathbb{Q}(x_1, \ldots, x_p) : \mathbb{Q}(x,y)| = |G_x \cap G_y| = 1$, i. e. $\mathbb{Q}(x_1, \ldots, x_p) = \mathbb{Q}(x,y)$.

(3)⇒(1): As above, $G_x \cap G_y = 1$. This shows $|G| = |G : G_x||G_x : G_x \cap G_y| = pd$ with $d \mid p-1$. By Sylow, G has a normal p-Sylow group. According to Theorem 6.21, G is solvable. Thus α is also solvable. □

Corollary 6.26. *Let $\alpha \in \mathbb{Q}[X]$ be irreducible and solvable with prime degree $p > 2$. Then α has either one or exactly p real roots.*

Proof. Since p is odd, α has at least one real root $x \in \mathbb{R}$ by the intermediate value theorem. If $y \in \mathbb{R}$ is also a root, then by Theorem 6.25 all roots lie in $\mathbb{Q}(x,y) \subseteq \mathbb{R}$. □

Definition 6.27. Let G, H be groups and Ω a G-set. As usual, $H^\Omega := \{f \colon \Omega \to H\}$ is a group with $(ff')(\omega) := f(\omega)f'(\omega)$ for $f, f' \in H^\Omega$ and $\omega \in \Omega$ (it holds that $H^\Omega \cong H^{|\Omega|}$). Obviously, G acts on H^Ω by $({}^g f)(\omega) := f({}^{g^{-1}}\omega)$ (verify). Because of

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

one obtains a homomorphism $\varphi \colon G \to \mathrm{Aut}(H^\Omega)$. One calls

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

the *wreath product* of H and G with respect to Ω.

Remark 6.28. In the case $\Omega = \{1, \ldots, n\}$, we identify H^Ω with H^n. For elements $(h_1, \ldots, h_n, g)$, $(h'_1, \ldots, h'_n, g') \in H \wr G$, it then holds that

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

Furthermore, $|H \wr G| = |H|^n |G|$.

Theorem 6.29. *Let G be an imprimitive permutation group on Ω with block Δ. Let $H := \{g \in G : {}^g\Delta = \Delta\}$ and let $\varphi \colon H \to \mathrm{Sym}(\Delta)$ be the action on Δ. Let $\Gamma := \{{}^g\Delta : g \in G\}$ and let $\psi \colon G \to \mathrm{Sym}(\Gamma)$ be the action on Γ. Then G is isomorphic to a subgroup of $\varphi(H) \wr \psi(G)$.*

Proof. Let $\Gamma = \{\Delta = \Delta_1, \dots, \Delta_n\}$. We choose $g_i \in G$ with ${}^{g_i}\Delta_i = \Delta$ for $i = 1, \dots, n$. For $x \in G$, let ${}^{x}\Delta_i = \Delta_{x(i)}$. Then

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

hence $g_i x g_{x^{-1}(i)}^{-1} \in H$. We define $f_x \in \varphi(H)^\Gamma$ by $f_x(\Delta_i) := \varphi(g_i x g_{x^{-1}(i)}^{-1})$ and

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

For $x, y \in G$, it now holds that

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

This shows

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

i. e. F is a homomorphism. For $x \in \operatorname{Ker}(F)$, we have $\psi(x) = 1$, i. e. x acts trivially on Γ. Furthermore, $f_x(\Delta_i) = 1$, i. e. $g_i x g_{x^{-1}(i)}^{-1} = g_i x g_i^{-1}$ acts trivially on Δ. Thus x acts trivially on ${}^{g_i^{-1}}\Delta = \Delta_i$ for $i = 1, \dots, n$. Overall, x acts trivially on Ω and it follows that $x = 1$. Therefore F is injective and the assertion follows. □

Example 6.30. The dihedral group D_8 acts imprimitively on the four vertices of the square (two diagonally opposite vertices form a block). Theorem 6.29 shows $D_8 \cong C_2 \wr C_2 \cong C_2^2 \rtimes C_2$. According to Example 5.11, $D_8 \cong C_4 \rtimes C_2$ also holds. In contrast to direct products, the factors of a semidirect product are therefore in general not uniquely determined.

Definition 6.31. An action $G \to \operatorname{Sym}(\Omega)$ is called *k-transitive* if $|\Omega| \geq k$ and for every two k-tuples $(\alpha_1, \dots, \alpha_k), (\beta_1, \dots, \beta_k) \in \Omega^k$ of pairwise distinct elements, there exists a $g \in G$ with ${}^{g}\alpha_i = \beta_i$ for $i = 1, \dots, k$.

Example 6.32.

(i) The 1-transitive actions are exactly the transitive actions.

(ii) Every k-transitive action is obviously also l-transitive for $1 \leq l \leq k$.

(iii) S_n is n-transitive (on $\{1, \dots, n\}$).

(iv) Let $n \geq 3$ and $k := n - 2$. For k-tuples $(\alpha_1, \dots, \alpha_k), (\beta_1, \dots, \beta_k) \in \{1, \dots, n\}^k$ with pairwise distinct elements, let $\{x, y\} = \{1, \dots, n\} \setminus \{\alpha_1, \dots, \alpha_k\}$ and $\{x', y'\} = \{1, \dots, n\} \setminus \{\beta_1, \dots, \beta_k\}$. Then exactly one of the two permutations

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

is in A_n. Thus A_n is $(n-2)$-transitive.

(v) For a prime power q and $n \geq 2$, $\mathrm{GL}(n, q)$ acts 2-transitively on the set of one-dimensional subspaces of $\mathbb{F}_q^n$ (linear algebra).

Lemma 6.33. *Let $\varphi \colon G \to \operatorname{Sym}(\Omega)$ be a transitive action, $\omega \in \Omega$ and $k \geq 2$. Then φ is k-transitive if and only if G_ω acts $(k-1)$-transitively on $\Omega \setminus \{\omega\}$.*

Proof. Let G be k-transitive and let $(\alpha_1, \ldots, \alpha_{k-1}), (\beta_1, \ldots, \beta_{k-1}) \in (\Omega \setminus \{\omega\})^{k-1}$ with pairwise distinct elements. Then there exists a $g \in G$ with ${}^g\alpha_i = \beta_i$ for $i = 1, \ldots, k-1$ and ${}^g\omega = \omega$. Thus $g \in G_\omega$ and G_ω is $(k-1)$-transitive on $\Omega \setminus \{\omega\}$.

Now let G_ω be $(k-1)$-transitive on $\Omega \setminus \{\omega\}$. Let $(\alpha_1, \ldots, \alpha_k), (\beta_1, \ldots, \beta_k) \in \Omega^k$ with pairwise distinct elements. Since φ is transitive, there exist $x, y \in G$ with ${}^x\alpha_k = \omega = {}^y\beta_k$. Then ${}^x\alpha_i, {}^y\beta_i \in \Omega \setminus \{\omega\}$ for $i = 1, \ldots, k-1$. Thus there exists an $h \in G_\omega$ with ${}^{hx}\alpha_i = {}^y\beta_i$ for $i = 1, \ldots, k$. For $g := y^{-1}hx \in G$ it follows that ${}^g\alpha_i = \beta_i$ for $i = 1, \ldots, k$. Thus G is k-transitive. □

Lemma 6.34. *If $G \to S_n$ is k-transitive, then $n(n-1)\ldots(n-k+1) \mid |G|$.*

Proof. Induction on k: In the case $k = 1$, G is transitive and the orbit equation yields $n \mid |G|$. Now let $k \geq 2$. Then G is transitive and by Lemma 6.33, G_1 is $(k-1)$-transitive on $\{2, \ldots, n\}$. By induction, $(n-1)\ldots(n-k+1) \mid |G_1|$. Because of $|G : G_1| = n$, the assertion follows. □

Theorem 6.35. *Every 2-transitive action is primitive.*

Proof. Let $\varphi\colon G \to \mathrm{Sym}(\Omega)$ be a 2-transitive action. Suppose that there exists a block $\Delta \subseteq \Omega$. Let $\alpha, \beta \in \Delta$ with $\alpha \neq \beta$ and $\gamma \in \Omega \setminus \Delta$. By assumption, there exists a $g \in G$ with ${}^g\alpha = \alpha$ and ${}^g\beta = \gamma$. In particular, $\varnothing \neq \Delta \cap {}^g\Delta \neq \Delta$. Contradiction. □

Theorem 6.36. *Let $1 \neq N \trianglelefteq G$ and $\varphi\colon G \to \mathrm{Sym}(N \setminus \{1\})$ be the action by conjugation. Then:*

(i) If φ is transitive, then N is an elementary abelian p-group.

(ii) If φ is even 2-transitive, then $p = 2$ or $|N| = 3$.

(iii) If φ is even 3-transitive, then $|N| = 4$.

(iv) φ is never 4-transitive.

Proof. Let p be a prime divisor of $|N|$ and $x \in N$ an element of order p (Cauchy). If φ is transitive, then every non-trivial element of N is conjugate to x. In particular, $y^p = 1$ for all $y \in N$. Thus N is a p-group and therefore solvable. Furthermore, N is a minimal normal subgroup. From Theorem 2.27 follows (i).

Now let φ be 2-transitive and $p \neq 2$. Then $x^{-1} \neq x$. Let $y \in N \setminus \{1, x\}$. Then there exists a $g \in G$ with $gxg^{-1} = x$ and $gx^{-1}g^{-1} = y$. This shows $y = x^{-1}$ and $N = \{1, x, x^{-1}\}$. Thus (ii) holds. If φ is 3-transitive, then $p = 2$ must hold, since $|N \setminus \{1\}| \geq 3$. Let $U := \{1, a, b, c\} \leq N$. Then $c = ab$. For a $g \in G$ with $gag^{-1} = a$ and $gbg^{-1} = b$, it must also hold that $gcg^{-1} = c$. This shows $U = N$ and (iii) follows. If the action were 4-transitive, then $|N \setminus \{1\}| \geq 4$ would hold, in contradiction to (iii). □

Example 6.37. Let $G = S_4$ and $N = V_4$. As is well known, N acts regularly on $\{1, 2, 3, 4\}$. According to Lemma 6.19, the action of $G_4 = S_3$ on $\{1, 2, 3\}$ is isomorphic to the action of G_4 on $N \setminus \{1\}$. Therefore, G_4 and G actually act 3-transitively on $N \setminus \{1\}$.

Theorem 6.38. *For $n \geq 5$, A_n is simple.*

Proof. Let $1 \neq N \trianglelefteq G := A_n$. According to Example 6.15, A_n acts faithfully and primitively on $\Omega := \{1, \ldots, n\}$. Therefore, N acts transitively on Ω according to Lemma 6.20. We now argue by induction on n. Let $n = 5$ (cf. Example 5.34). Then $5 \mid |N|$. Since $|G/N|$ is no longer divisible by 5, N must contain all elements of order 5, i. e. all 5-cycles. Every 5-cycle can be uniquely written in the form $(1, a, b, c, d)$ with $\{a, b, c, d\} = \{2, 3, 4, 5\}$. Thus there are exactly $4! = 24$ such elements and we obtain $|N| \geq 24$. Due to $|N| \mid |G|$, only the possibilities $|N| \in \{30, 60\}$ remain. Thus $|G/N|$ is also no longer divisible by 3 and N must also contain all 3-cycles. There are $\binom{5}{3} \cdot 2! = 20$ of these. Thus $|N| \geq 24 + 20 = 44$ and hence $N = G$.

Now let $n \geq 6$ and assume the claim has already been shown for $n - 1$. The stabilizer $G_n = A_{n-1}$ is simple by induction. According to the Frattini argument, $G = NG_n$. We can therefore assume $G_n \not\subseteq N$. In particular, $N \cap G_n \lhd G_n$ and thus $N_n = N \cap G_n = 1$. Thus N acts regularly on Ω and $|N| = n$. According to Example 6.32, G_n acts $(n-3)$-transitively on $\Omega \setminus \{n\}$. According to Lemma 6.19, this action is isomorphic to the action on $N \setminus \{1\}$ by conjugation. Theorem 6.36 now yields $n = 6$ and $|N| = 4$. However, this contradicts $|N| = n$. □

Theorem 6.39. *For $n \geq 5$, 1, A_n and S_n are the only normal subgroups of S_n. In particular, $S_n' = A_n$.*

Proof. Let $1 \neq N \lhd S_n$. Then $N \cap A_n \trianglelefteq A_n$. From Theorem 6.38 it follows that $N \cap A_n \in \{1, A_n\}$. In the second case, $N = A_n$. In the first case, $|S_n| = |A_n N| = |A_n||N|$ and $|N| = 2$. However, this contradicts Lemma 6.20. □

Theorem 6.40. *If G is a simple group of order 60, then $G \cong A_5$.*

Proof. We first construct a subgroup $H \leq G$ of index 5. Let $P \in \mathrm{Syl}_2(G)$. Obviously $\mathrm{N}_G(P) < G$. In the case $|G : \mathrm{N}_G(P)| = 3$, there would be a non-trivial homomorphism $G \to S_3$ in contradiction to the simplicity of G. We can therefore assume $\mathrm{N}_G(P) = P$ (otherwise set $H := \mathrm{N}_G(P)$). If any two distinct 2-Sylow subgroups intersect trivially, then the union of all 2-Sylow subgroups has 46 elements. On the other hand, according to Sylow, there must be at least six 5-Sylow subgroups, which also intersect trivially. This contradiction shows that there exists a $Q \in \mathrm{Syl}_2(G)$ with $|P \cap Q| = 2$. Then $P, Q \leq \mathrm{N}_G(P \cap Q)$. As above, $|G : \mathrm{N}_G(P \cap Q)| = 3$ is excluded. One can therefore choose $H := \mathrm{N}_G(P \cap Q)$.

The action on the cosets G/H now yields a monomorphism $G \to S_5$. Since A_5 is the only subgroup of order 60 in S_5 (Theorem 6.39), it follows that $G \cong A_5$. □

Remark 6.41. With the help of the CFSG, one can show that every 4-transitive permutation group belongs to one of the following families:

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

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

(iii) M_{11}, M_{12}, M_{23}, M_{24} (sporadic simple *Mathieu groups*[17]).

[17] See lecture notes on combinatorial group theory

7 Transfer and Normal Complements

Definition 7.1. For a prime p, G is called *p-nilpotent* if there exists a p'-normal subgroup $N \trianglelefteq G$ with p-factor group G/N.

Remark 7.2.

(i) In the situation of Definition 7.1, it is clear that $N = \mathrm{O}_{p'}(G) = \mathrm{O}^p(G)$. Conversely, every group G with $\mathrm{O}_{p'}(G) = \mathrm{O}^p(G)$ is certainly p-nilpotent. If $P \in \mathrm{Syl}_p(G)$, then in this case $G = \mathrm{O}_{p'}(G)P$ and $\mathrm{O}_{p'}(G) \cap P = 1$. Thus $G = \mathrm{O}_{p'}(G) \rtimes P$. Furthermore, $\mathrm{O}_{p'}(G)$ is then the set of p'-elements of G.

(ii) If G is p-nilpotent for a $p \mid |G| \neq p$, then G is not simple.

Example 7.3. Because of $A_3 \trianglelefteq S_3$, S_3 is 2-nilpotent, but not 3-nilpotent. On the other hand, A_4 is 3-nilpotent, but not 2-nilpotent.

Theorem 7.4. *G is nilpotent if and only if G is p-nilpotent for every prime p.*

Proof. If G is nilpotent and p is a prime, then $\mathrm{O}_{p'}(G) = \bigoplus_{q \neq p} \mathrm{O}_q(G)$ by Theorem 4.10. Thus $G/\mathrm{O}_{p'}(G)$ is a p-group and G is p-nilpotent. Conversely, let G be p-nilpotent for every prime p. Then

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

is nilpotent by Theorem 4.10. On the other hand, the homomorphism $G \to D$, $g \mapsto (g\mathrm{O}_{p'}(G))_{p \mid |G|}$ has kernel $\bigcap_{p \mid |G|} \mathrm{O}_{p'}(G) = 1$. Because of $|G| = |D|$, G is isomorphic to the nilpotent group D. □

Lemma 7.5. *Subgroups and factor groups of p-nilpotent groups are again p-nilpotent.*

Proof. Let G be p-nilpotent and $H \leq G$. Then $\mathrm{O}_{p'}(G) \cap H \leq \mathrm{O}_{p'}(H)$ and

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

is already a p-group. Thus H is p-nilpotent. Now let $N \trianglelefteq G$. Then $\mathrm{O}_{p'}(G)N/N \leq \mathrm{O}_{p'}(G/N)$ and

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

is a p-group. Thus G/N is also p-nilpotent. □

Definition 7.6. Let $K \trianglelefteq H \leq G$ with abelian factor group H/K and let R be a transversal for G/H. For $g \in G$ let $\overline{g} \in R$ with $gH = \overline{g}H$. The map

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

is called the *transfer* (German: *Verlagerung*) from G to H/K. Since H/K is abelian, the order of the factors in the product does not matter.

Lemma 7.7. *The transfer does not depend on the choice of R and is a homomorphism.*

Proof. For transversals R and S of G/H we define

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

similarly to Definition 5.17. Then $V_{H/K}(g) = (gR|R)$ for $g \in G$. As in Lemma 5.18 one shows

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

Thus $V_{H/K}$ does not depend on the choice of R. For $g, h \in G$ we have

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

Remark 7.8. We seek a transversal R such that $V_{H/K}$ is easy to calculate. Let $g \in G$ and let $x_1H, \ldots, x_nH$ be representatives for the orbits of $\langle g\rangle$ on G/H by left multiplication. Then $R := \{g^j x_i : i = 1, \ldots, n,\ j = 0, \ldots, t_i - 1\}$ is a transversal for G/H, where t_i is the orbit length of x_iH under $\langle g\rangle$. In the case $0 \le j < t_i - 1$ we have $(\overline{g(g^j x_i)})^{-1}g(g^j x_i) = 1$ (with respect to R). Thus

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

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

Example 7.9. For $g \in \mathrm{Z}(G)$ we thus have $V_{H/K}(g) = g^{|G:H|}K$. Furthermore, for $H = \mathrm{Z}(G)$ and $K = 1$ one obtains a homomorphism $G \to \mathrm{Z}(G)$, $g \mapsto g^{|G:\mathrm{Z}(G)|}$.

Definition 7.10. For $H \le G$ one calls

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

the *focal group* of H in G.

Remark 7.11. Clearly $H' \le F := \mathrm{Foc}_G(H) \le H \cap G'$ and $F \trianglelefteq H$ with abelian factor group H/F. For $g \in G$ and $h \in H$ with $[g,h] \in H$ we have $ghg^{-1}F = ghg^{-1}h^{-1}Fh = [g,h]Fh = Fh = hF$. This shows $V_{H/F}(h) = h^{|G:H|}F$ for all $h \in H$ by Remark 7.8.

Theorem 7.12. *Let $H \le G$ and $F := \mathrm{Foc}_G(H)$ with $\gcd(|G:H|, |H:F|) = 1$. For $N := \mathrm{Ker}(V_{H/F}) \trianglelefteq G$ it then holds that*

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

(ii) $HN = G$.

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

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

Proof.

(i) Since G/N is isomorphic to a subgroup of the abelian group H/F, it holds that $G' \leq N$ and $F \leq H \cap G' \leq H \cap N$. For $h \in H \cap N$, we have $1 = V_{H/F}(h) = h^{|G:H|}F$ and $h^{|G:H|} \in F$. On the other hand, $h^{|H:F|} \in F$ also holds. Because of $\gcd(|G:H|, |H:F|) = 1$, there exist $a, b \in \mathbb{Z}$ with $a|G:H| + b|H:F| = 1$. It follows that

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

Thus $H \cap N \leq F$ holds.

(ii) According to (i), $|G/N| \geq |HN/N| = |H/H \cap N| = |H/F| \geq |G/N|$ and therefore $G = HN$.

(iii) According to (ii), $G/G' = HN/G' = (HG'/G')(N/G')$ and according to (i), $HG' \cap N = G'(H \cap N) = G'F = G'$.

(iv) The proof of (ii) shows that $V_{H/F}$ is surjective. □

Remark 7.13. The assumption $\gcd(|G:H|, |H:F|) = 1$ in Theorem 7.12 is satisfied, for example, for π-Hall subgroups H. According to Exercise 34, HG'/G' is then a π-Hall subgroup of G/G'. According to Theorem 7.12(iii), N is then the smallest normal subgroup with an abelian π-factor group. This shows $N = \mathrm{O}^\pi(G)G'$.

Corollary 7.14 (Higman's Focal Subgroup Theorem)**.** *For $P \in \mathrm{Syl}_p(G)$, it holds that* $\mathrm{Foc}_G(P) = G' \cap P \in \mathrm{Syl}_p(G')$.

Proof. Choose $H = P$ in Theorem 7.12. □

Theorem 7.15 (Taunt)**.** *Let $H \leq G$ with* $\gcd(|G:H|, |H:H'|) = 1$. *Then* $G' \cap \mathrm{Z}(G) \cap H \leq H'$.

Proof. As usual, G' lies in the kernel of $V_{H/H'}$. For $x \in G' \cap \mathrm{Z}(G) \cap H$, it therefore holds that $V_{H/H'}(x) = 1$. On the other hand, because $x \in \mathrm{Z}(G)$, we have $V_{H/H'}(x) = x^{|G:H|}H'$ according to Example 7.9, so $x^{|G:H|} \in H'$. From $x \in H$, it also follows that $x^{|H:H'|} \in H'$. With $\gcd(|G:H|, |H:H'|) = 1$, it follows that $x \in H'$. □

Theorem 7.16 (Alperin's Fusion Theorem)**.** *Let $P \in \mathrm{Syl}_p(G)$. Let $\mathcal{P}$ be the set of all subgroups $Q \leq P$ with the following properties:*

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

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

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

Then it holds that

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

Proof. Obviously $F := \langle [\mathrm{N}_G(Q), Q] : Q \in \mathcal{P} \rangle \leq G' \cap P$. For the reverse inclusion, we show more generally: If $A \leq P$ and $g \in G$ with ${}^gA \leq P$, then

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

With Higman's focal subgroup theorem, it then follows that $G' \cap P = \mathrm{Foc}_G(P) \leq F$.

We argue by induction on $|P : A|$. In the case $P = A$, we have $g \in \mathrm{N}_G(P)$ and the claim holds because $P \in \mathcal{P}$. Now let $A < P$. By Theorem 3.14, $A < \mathrm{N}_P(A) \leq A_1 \in \mathrm{Syl}_p(\mathrm{N}_G(A))$. By Sylow, there exists $x \in G$ with ${}^xA_1 \leq P$. For $Q := {}^xA$, on the one hand

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

and on the other hand ${}^xA_1 \in \mathrm{Syl}_p(\mathrm{N}_G(Q))$. This shows ${}^x\mathrm{N}_P(A) \leq \mathrm{N}_P(Q) \in \mathrm{Syl}_p(\mathrm{N}_G(Q))$. Thus (i) holds for Q and by induction $[x, A] \leq [x, \mathrm{N}_P(A)] \leq F$. Because ${}^{xg^{-1}}\mathrm{N}_P({}^gA) \leq \mathrm{N}_G(Q)$, there exists $y \in \mathrm{N}_G(Q)$ with ${}^{yxg^{-1}}\mathrm{N}_P({}^gA) \leq \mathrm{N}_P(Q)$ by Sylow. One obtains $[yxg^{-1}, {}^gA] \leq [yxg^{-1}, \mathrm{N}_P({}^gA)] \leq F$ by induction.

If (ii) and (iii) are satisfied for Q, then $[y, Q] \leq [\mathrm{N}_G(Q), Q] \leq F$ by construction. Now let

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

Then $y \in \mathrm{N}_G(\tilde{Q})$ and inductively it follows that $[y, Q] \leq [y, \tilde{Q}] \leq F$. Finally, let $\tilde{Q} := Q\mathrm{C}_P(Q) > Q$. Because $\mathrm{C}_P(Q) = \mathrm{N}_P(Q) \cap \mathrm{C}_G(Q) \in \mathrm{Syl}_p(\mathrm{C}_G(Q))$, there exists $z \in \mathrm{C}_G(Q)$ with ${}^{zy}\mathrm{C}_P(Q) = \mathrm{C}_P(Q)$. Now $zy \in \mathrm{N}_G(\tilde{Q})$ and $[y, Q] \leq [zy, \tilde{Q}] \leq F$ by induction. In any case, it follows that $[y, Q] \in F$. For $a \in A$ it follows that

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

Theorem 7.17 (Puig's hyperfocal subgroup theorem)**.** *For $P \in \mathrm{Syl}_p(G)$ we have*

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

Proof. Let

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

Let $x \in Q \leq P$ and $g \in \mathrm{O}^p(\mathrm{N}_G(Q))$. According to Remark 4.6, g is a product of p'-elements $g_1, \ldots, g_n \in \mathrm{N}_G(Q)$. For $n = 1$, we have $[g, x] \in T$. Now let $n \geq 2$ and assume $[g_2 \ldots g_n, x] \in T$ has already been shown. Because $[g_2 \ldots g_n, x] \in Q \leq P$, it follows that $[g_1, g_2 \ldots g_n, x] \in T$. It follows that

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

This shows $S \leq T$.

Every p'-element $g \in G$ lies in $\mathrm{O}^p(G)$. For $x, [g, x] \in P$, we therefore have $[g, x] = g(xg^{-1}x^{-1}) \in \mathrm{O}^p(G) \cap P$. Thus $T \leq \mathrm{O}^p(G) \cap P$ holds and it remains to show $\mathrm{O}^p(G) \cap P \leq S$. For $H := \mathrm{O}^p(G)$, we have $H \cap P \in \mathrm{Syl}_p(H)$. For $Q \leq H \cap P$, we have $\mathrm{O}^p(\mathrm{N}_H(Q)) \leq \mathrm{O}^p(\mathrm{N}_G(Q))$ according to Remark 4.6. We may therefore assume $G = H$. Then $P \leq G'$ and Alperin shows

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

For $Q \in \mathcal{P}$, we have $\mathrm{N}_P(Q) \in \mathrm{Syl}_p(\mathrm{N}_G(Q))$ and $\mathrm{N}_G(Q) = \mathrm{N}_P(Q)\mathrm{O}^p(\mathrm{N}_G(Q))$. For $x \in Q$, $y \in \mathrm{N}_P(Q)$ and $g \in \mathrm{O}^p(\mathrm{N}_G(Q))$, we have

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

Overall, we now have $P = SP' = S\Phi(P) = S$ according to Lemma 4.15. $\square$

Theorem 7.18 (Frobenius' Transfer Theorem)**.** *Let $P \in \mathrm{Syl}_p(G)$ such that $\mathrm{N}_G(Q)/\mathrm{C}_G(Q)$ is a p-group for all $Q \leq P$. Then G is p-nilpotent.*

Proof. By assumption, $[\mathrm{O}^p(\mathrm{N}_G(Q)), Q] \leq [\mathrm{C}_G(Q), Q] = 1$ for all $Q \leq P$. From Puig's Theorem, it follows that $\mathrm{O}^p(G) \cap P = 1$. Therefore, $\mathrm{O}^p(G)$ is a normal complement of P. □

Remark 7.19.

(i) In Theorem 7.18, it suffices to consider the subgroups $Q \in \mathcal{P}$ from Alperin's Fusion Theorem. In that case, $G' \cap P = P'$ holds and the assertion follows from Theorem 7.38.

(ii) For $p > 2$, Thompson and Glauberman have proven that G is already p-nilpotent if $\mathrm{N}_G(K(P))/\mathrm{C}_G(K(P))$ is a p-group, where $K(P)$ is a certain characteristic subgroup of P whose definition is complicated. The analogous statement for $p = 2$ does not hold, as there are simple groups G (such as $\mathrm{PSL}(2, 17)$, see Theorem 10.11) such that $P \in \mathrm{Syl}_2(G)$ is a maximal subgroup. For $Q \trianglelefteq P$, we then have $\mathrm{N}_G(Q) = P$.

Theorem 7.20 (Grün's First Transfer Theorem)**.** *For $P \in \mathrm{Syl}_p(G)$, we have*

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

Proof. Certainly

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

Assume $H < P \cap G'$. Since $P' \leq H$, we have $H \trianglelefteq P$. Let $x \in P \cap G' \setminus H$ be of minimal order.

To calculate the transfer $V_{P/H}(x)$ according to Remark 7.8, we decompose G into double cosets of the form PyP. Clearly PyP is a union of left cosets of P and $\langle x\rangle$ acts by left multiplication on the set of these cosets. Let $y = y_1, \ldots, y_n \in Py$ be a system of representatives of the corresponding orbits with orbit lengths $p^{a_1} \leq \ldots \leq p^{a_n}$ (if necessary, replace y by some y_i). The orbit equation yields

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

We have $x^{p^{a_i}} y_i P = y_i P$, thus $y_i^{-1} x^{p^{a_i}} y_i \in P$ and specifically $y^{-1} x^{p^{a_1}} y \in P$.

Case 1: $t > 0$.
The orbit of $y_i P$ provides the contribution $z_i H$ in $V_{P/H}(x)$ with $z_i := y_i^{-1} x^{p^{a_i}} y_i \in P$ (Remark 7.8). It holds that

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

Since $a_i \geq a_1$, $y^{-1} x^{p^{a_i}} y$ is a power of $y^{-1} x^{p^{a_1}} y \in P$. This shows

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

One can therefore replace the contribution $z_i H$ in $V_{P/H}(x)$ by $y^{-1} x^{p^{a_i}} y H$. All these contributions together yield $y^{-1} x^{p^t} y H$. Since $x \in G'$, we have $y^{-1} x^{p^t} y \in P \cap G'$ and the choice of x shows $y^{-1} x^{p^t} y \in H$. These double cosets thus provide no contribution to $V_{P/H}(x)$.

Case 2: $t = 0$.
Here $P = yPy^{-1}$, so $y \in \mathrm{N}_G(P)$. The contribution of $yP = y_1 P$ in $V_{P/H}(x)$ is

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

(note: $a_1 = 0$). The number of these double cosets $PyP = yP$ is $k := |\mathrm{N}_G(P) : P| \not\equiv 0 \pmod{p}$. In total, we obtain $V_{P/H}(x) = x^k H$. As is well known, $x \in G' \subseteq \mathrm{Ker}(V_{P/H})$ and it follows that $x^k \in H$. Since k is not divisible by p, one obtains the contradiction $x \in H$. □

Theorem 7.21 (Burnside's Transfer Theorem)**.** *Let $P \in \mathrm{Syl}_p(G)$ with $\mathrm{N}_G(P) = \mathrm{C}_G(P)$. Then G is p-nilpotent.*

Proof. Since $P \leq \mathrm{N}_G(P) = \mathrm{C}_G(P)$, P is abelian. Grün's Transfer Theorem (or Alperin's Fusion Theorem) shows $G' \cap P = [\mathrm{N}_G(P), P] = 1$. Therefore the claim follows from Theorem 7.12. □

Theorem 7.22. *Let p be the smallest prime divisor of $|G|$. If G has a cyclic p-Sylow group, then G is p-nilpotent.*

Proof. Let $P \in \mathrm{Syl}_p(G)$ be cyclic of order p^n. Then $|\mathrm{Aut}(P)| = \varphi(p^n) = p^{n-1}(p-1)$ according to Theorem 2.4. As is well known, $\mathrm{N}_G(P)/\mathrm{C}_G(P)$ is isomorphic to a subgroup of $\mathrm{Aut}(P)$. Because of $P \leq \mathrm{C}_G(P)$, it follows that $|\mathrm{N}_G(P)/\mathrm{C}_G(P)| \mid p-1$. On the other hand, by Lagrange, $|\mathrm{N}_G(P)/\mathrm{C}_G(P)| \mid |G|$. Since p is the smallest prime divisor of $|G|$, we obtain $\mathrm{N}_G(P) = \mathrm{C}_G(P)$. The assertion now follows from Theorem 7.21. □

Example 7.23.

(i) Let $|G| = 11^2 \cdot 12$. We show that G is solvable. Let $P \in \mathrm{Syl}_{11}(G)$. In the case $P \trianglelefteq G$, both P and G/P are solvable and therefore so is G. So let $P \not\trianglelefteq G$. By Sylow, $|G : \mathrm{N}_G(P)| = 12$, thus $\mathrm{N}_G(P) = P$. Because $|P| = 11^2$, P is abelian and it follows that $\mathrm{N}_G(P) = P \leq \mathrm{C}_G(P) \leq \mathrm{N}_G(P)$. By Theorem 7.21, there exists an $N \trianglelefteq G$ with $|N| = 12$. Again, N and G/N are solvable and therefore so is G.

(ii) If $|G|$ is divisible by 2 only once, then G is 2-nilpotent according to Theorem 7.22. By Feit-Thompson, G is even solvable.

Theorem 7.24 (Zassenhaus)**.** *If all Sylow subgroups of G are cyclic, then G' and G/G' are also cyclic. In particular, G is metabelian.*

Proof. We first show by induction on $|G|$ that G is solvable. Let p be the smallest prime divisor of $|G|$. By Theorem 7.22, $G/\mathrm{O}_{p'}(G)$ is a p-group and thus solvable. Obviously, the Sylow subgroups of $\mathrm{O}_{p'}(G)$ are also cyclic. By induction, $\mathrm{O}_{p'}(G)$ is therefore also solvable. The assertion now follows from Lemma 2.22.

Now G/G' is abelian and all Sylow subgroups of G/G' are cyclic. Thus G/G' is also cyclic. By the same argument, it suffices to show that G' is abelian. Let us assume indirectly that $G'' \neq 1$. Replacing G by G/G''', one can assume that G'' is abelian. Then G'' is certainly cyclic. Thus $G/\mathrm{C}_G(G'') \leq \mathrm{Aut}(G'') \cong (\mathbb{Z}/|G''|\mathbb{Z})^\times$ is abelian (Theorem 2.4). This shows $G' \leq \mathrm{C}_G(G'')$ and $G'' \leq \mathrm{Z}(G')$. Since G'/G'' is also cyclic, G' must finally be abelian (Exercise 10(a)). However, this contradicts $G'' \neq 1$. □

Remark 7.25. In the situation of Theorem 7.24, one can further show that G' is a Hall subgroup. Thus $G \cong C_m \rtimes C_n$ with $\gcd(n, m) = 1$ according to Schur-Zassenhaus.

Example 7.26. Groups of square-free order are metabelian.

Theorem 7.27. *For every abelian Hall subgroup $H \leq G$ and $N := \mathrm{N}_G(H)$, the following holds:*

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

Proof. We regard $V_{H/1}$ as a map to H and write $V_H := V_{H/1}$. Let $g \in H$ and $V_H(g) = \prod_{i=1}^n x_i^{-1} g^{t_i} x_i \in H$ as in Remark 7.8. For $i = 1, \ldots, n$ we then have $g^{t_i}, x_i^{-1} g^{t_i} x_i \in H$ and $\langle H, x_i H x_i^{-1} \rangle \leq \mathrm{C}_G(g^{t_i})$, since H is abelian. According to Theorem 5.46 (Wielandt), the nilpotent Hall groups H and $x_i H x_i^{-1}$ are conjugate in $\mathrm{C}_G(g^{t_i})$. Thus, let $c_i \in \mathrm{C}_G(g^{t_i})$ with $c_i x_i H x_i^{-1} c_i^{-1} = H$ for $i = 1, \ldots, n$. Then $c_i x_i \in N$ and

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

It follows that $V_H(g) \in g^{|G:H|}[H,N]$ and $g^{|G:H|} \in V_H(H)[H,N]$. Because of $\gcd(|H|, |G:H|) = 1$, we even have $H = V_H(H)[H,N]$.

Clearly,

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

(note: $G/\mathrm{Ker}(V_H) \cong V_H(G) \leq H$ is abelian). Therefore, $H = V_H(H)(H \cap \mathrm{Ker}(V_H))$ also holds. Since $[H,N] \leq \mathrm{Ker}(V_H)$, it follows from (7.1) that $V_H(V_H(g)) = V_H(g)^{|G:H|}$ for $g \in H$. This yields $V_H(H) \cap \mathrm{Ker}(V_H) = 1$ and it follows that

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

For reasons of order, we then also have $[H,N] = \mathrm{Foc}_G(H) = H \cap \mathrm{Ker}(V_H)$. This shows (ii) and a part of (i).

Let R be an arbitrary transversal for G/H and let $x \in N$. As in Definition 7.6, we choose $\overline{g} \in R$ with $gH = \overline{g}H$ for $g \in G$. Then Rx is also a transversal for G/H, because $rxH = sxH$ implies $rHx = sHx$ and $rH = sH$ for $r, s \in R$. For $g \in G$, let $\widetilde{g} \in Rx$ with $gH = \widetilde{g}H$. Then $\overline{gr}xH = \overline{gr}Hx = grHx = grxH = \widetilde{grx}H$ and $\overline{gr}x = \widetilde{grx}$ for $r \in R$. This shows

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

Thus $V_H(H) \leq H \cap \mathrm{Z}(N) = \mathrm{C}_H(N)$. Conversely, for $g \in \mathrm{C}_H(N)$, we have $V_H(g) = g^{|G:H|}$ by (7.1). This implies $V_H(H) = \mathrm{C}_H(N)$ and we are done. □

Remark 7.28. In the situation of Theorem 7.27, $G/\mathrm{Ker}(V_{H/F}) \cong H/F \cong \mathrm{C}_H(N)$ with $F := \mathrm{Foc}_G(H)$ holds according to Theorem 7.12. In this way, one can frequently construct normal subgroups.

Example 7.29. Let $P \cong C_4 \times C_2$ be a 2-Sylow subgroup of G and $N := \mathrm{N}_G(P)$. According to Theorem 4.18,

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

Since $\Phi(P)$ is characteristic in P, $\Phi(P) \trianglelefteq N$. Because $|\Phi(P)| = 2$, even $\Phi(P) \leq P \cap \mathrm{Z}(N) \neq 1$ holds. By Remark 7.28, there exists a $K \trianglelefteq G$ with $G/K \cong P \cap \mathrm{Z}(N)$. In particular, G is not simple. Let $1 \neq \alpha \in \mathrm{Aut}(P)$ be of odd order. By Remark 4.21, α acts non-trivially on $P/\Phi(P) \cong C_2^2$. We have $\mathrm{Aut}(C_2^2) \cong \mathrm{GL}(2,2) \cong S_3$. Thus α must transitively permute the three maximal subgroups of P. On the other hand, α must fix the characteristic subgroup $\{x \in P : x^2 = 1\} \cong C_2^2$. This contradiction shows that $\mathrm{Aut}(P)$ is a 2-group. Therefore, $N/\mathrm{C}_G(P)$ is also a 2-group. Since $P \leq \mathrm{C}_G(P)$, even $N = \mathrm{C}_G(P)$ holds. By Burnside's Transfer Theorem, G is 2-nilpotent.

Theorem 7.30. *Every subgroup $H \leq G$ with $H \cap gHg^{-1} = 1$ for all $g \in G \setminus H$ possesses a normal complement in G (cf. Exercise 35).*

Proof (Shaw). Induction on $|H|$: We can assume $H \neq 1$. Then $H' < H$. Let $h \in H$ and $V_{H/H'}(h) = \prod_{i=1}^{n} x_i^{-1} h^{t_i} x_i H'$ as in Remark 7.8. Here we can assume $x_1 = 1$. Because $hx_1H = H = x_1H$, it follows that $t_1 = 1$ and $x_1^{-1}h^{t_1}x_1 = h$. For $i > 1$, $x_i \notin H$ and $x_i^{-1}h^{t_i}x_i \in H \cap x_i^{-1}Hx_i = 1$. This shows $V_{H/H'}(h) = hH'$ for all $h \in H$. In particular, $V_{H/H'}(H) = H/H'$ and $\mathrm{Ker}(V_{H/H'}) \cap H = H'$. Let $N := \mathrm{Ker}(V_{H/H'})$. For $g \in G$, there exists an $h \in H$ with $V_{H/H'}(g) = V_{H/H'}(h)$ and $g = hh^{-1}g \in HN$. Thus $G = HN$. For $g \in N \setminus H' = N \setminus H$, $gH'g^{-1} \cap H' \subseteq gHg^{-1} \cap H = 1$. By induction, H' has a normal complement K in N. By Exercise 35, H' and K are Hall subgroups of N. In particular, K is characteristic in N and thus normal in G. We have $H \cap K = H \cap N \cap K = H' \cap K = 1$ and $G = HN = HH'K = HK$. The assertion follows. □

Remark 7.31. Frobenius showed that the solvability condition in Theorem 7.30 is redundant. However, no proof is known that does not rely on character theory.

Theorem 7.32. *Let G be a non-abelian simple group and $P \in \mathrm{Syl}_p(G)$ with $|P| = p^n > 1$. Then one of the following two statements holds:*

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

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

Proof. First, assume that P is abelian. According to Theorem 7.21, then $P \leq \mathrm{C}_G(P) < \mathrm{N}_G(P)$. Let $g \in \mathrm{N}_G(P) \setminus \mathrm{C}_G(P)$. Since P is the only Sylow p-subgroup in $\mathrm{N}_G(P)$, g is not a p-element. By replacing g with a suitable power (Lemma 2.1), one can assume that g has order $q^s \neq 1$ for a prime $q \neq p$. According to Remark 4.21, $\langle g \rangle$ acts non-trivially on $P/\Phi(P)$. Since $P/\Phi(P)$ is elementary abelian, $\mathrm{Aut}(P/\Phi(P)) \leq \mathrm{GL}(n, p)$ and $q \mid |\mathrm{GL}(n, p)| = (p^n - 1)(p^n - p) \dots (p^n - p^{n-1})$. Because $q \neq p$, it then also follows that

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

Now let P be non-abelian. In particular, then $n \geq 3$ and $\Phi(P) \neq 1$. According to Theorem 7.18, there exists a subgroup $Q \leq P$ such that $\mathrm{N}_G(Q)/\mathrm{C}_G(Q)$ is not a p-group. We again choose a prime divisor $q \neq p$ of $|\mathrm{N}_G(Q)/\mathrm{C}_G(Q)|$. Because $|Q : \Phi(Q)| \leq p^{n-1}$, one obtains as above $q \mid (p^{n-1} - 1)(p^{n-2} - 1) \dots (p^2 - 1)(p - 1)$. Because $p^2 - 1 = (p + 1)(p - 1)$, one can omit the factor $p - 1$ here. Furthermore, $q \mid |G : P|$ since $q \neq p$. In the case $q \mid |\mathrm{N}_G(P) : P|$, statement (i) holds. Thus we can assume $q \mid |G : \mathrm{N}_G(P)|$. Hence (ii) holds. □

Example 7.33. According to Theorem 4.23 and Example 7.26, the order of a non-abelian simple group is the product of at least four primes. Let G be a simple group of order $pqrs$ with primes $p \leq q \leq r \leq s$. According to Theorem 7.22, $p = q$ and according to Theorem 4.23, $q < r$. Furthermore,

$$1 \neq \gcd(rs, (p^2 - 1)(p - 1)) = \gcd(rs, p + 1)$$

according to Theorem 7.32. This shows $p = q = 2$ and $r = 3$. Let us assume $s = 3$. According to Sylow, then $\mathrm{N}_G(S) = S$ for $S \in \mathrm{Syl}_3(G)$. However, this contradicts Theorem 7.21. Thus $s \geq 5$. Let $S \in \mathrm{Syl}_s(G)$. Then $|G : \mathrm{N}_G(S)|$ is a divisor of 12 and $|G : \mathrm{N}_G(S)| \equiv 1 \pmod{s}$ according to Sylow. It follows that

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

The case $|G : \mathrm{N}_G(S)| = 12$ contradicts Theorem 7.21 as before. Thus $s = 5$ and $G \cong A_5$ according to Theorem 6.40.

Lemma 7.34 (Brandis). *Let $G = HN$ with $H \leq G$ and $N \trianglelefteq G$. Let $K := H \cap N$ and $K' \leq K_0 \leq K$ with $K_0 \trianglelefteq H$ and $\gcd(|K/K_0|, |G : H|) = 1$. Suppose the transfer $V\colon N \to K/K_0$ is trivial. Then $H = KL$ with $L \leq H$ and $K \cap L = K_0$.*

Proof. Let R be a transversal for N/K. For $x \in N$, let $\overline{x} \in R$ with $xK = \overline{x}K$. We define

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

(since K/K_0 is abelian, the order of the factors does not matter). Because of $K_0 \trianglelefteq H$, we have $R = \{\overline{r^x} : r \in R\}$. For $x, y \in H$, it holds that

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

i. e. α is a crossed homomorphism (Definition 5.20). By Lemma 5.21, $L := \mathrm{Ker}(\alpha) \leq H$. For $x \in K$, we have $r^x K = x^{-1}rK$ and

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

Due to $|N : K| = |N : N \cap H| = |HN : H| = |G : H|$ and $\gcd(|K/K_0|, |G : H|) = 1$, $\alpha_{|K}$ is surjective and $L \cap K = K_0$. For $h \in H$, there exists $x \in K$ with $\alpha(h) = \alpha(x)^{-1}$. Since K/K_0 is abelian, we have $\alpha(hx) = \alpha(h)\alpha(x) = 1$, i. e. $hx \in \mathrm{Ker}(\alpha) = L$. This shows $h = (hx)x^{-1} \in LK$ and $H = KL$. □

Theorem 7.35. *Let $P \in \mathrm{Syl}_p(G)$ and $Q = P \cap \mathrm{O}^p(G)$. Then there exists $R \leq P$ with $P = QR$ and $Q \cap R = Q'$.*

Proof. Let $H := P$, $N := \mathrm{O}^p(G)$, $K := Q$ and $K_0 := Q'$ in Lemma 7.34. Certainly $G = HN$ and $\gcd(|K/K_0|, |G : H|) = 1$ hold. Since Q' is characteristic in $Q \trianglelefteq H$, we also have $K_0 \trianglelefteq H$. Because of $\mathrm{O}^p(N) \trianglelefteq G$, we have $\mathrm{O}^p(N) = N$. In particular, the transfer $N \to K/K_0$ must be trivial. Now the claim follows from Lemma 7.34. □

Corollary 7.36 (Gaschütz). *If the Sylow p-subgroups of $\mathrm{O}^p(G)$ are abelian, then $\mathrm{O}^p(G)$ has a complement in G.*

Proof. In the situation of Theorem 7.35, we have $\mathrm{O}^p(G) \cap R = Q \cap R = Q' = 1$ and $G = P\mathrm{O}^p(G) = RQ\mathrm{O}^p(G) = R\mathrm{O}^p(G)$. □

Remark 7.37. The next theorem is a localization of Wielandt's Theorem 4.17.

Theorem 7.38. *For $P \in \mathrm{Syl}_p(G)$, the following statements are equivalent:*

(1) G is p-nilpotent.

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

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

If applicable, $G' \cap P = P'$.

Proof. If G is p-nilpotent, then

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

by Dedekind. In particular, $G' \cap P \leq \Phi(P)$ then holds. Now let $N = \mathrm{O}^p(G)G'$. By Theorem 7.12 and Remark 7.13, $G' \cap P = N \cap P$ holds. From $G' \cap P \leq \Phi(P)$ it follows that $Q := \mathrm{O}^p(G) \cap P \leq N \cap P \leq \Phi(P)$.

Finally, let $Q \leq \Phi(P)$. By Theorem 7.35 there exists $R \leq P$ with $P = QR = \Phi(P)R$ and $Q \cap R = Q'$. With Lemma 4.15 we obtain $P = R$ and $Q = Q \cap P = Q'$, thus $Q = 1$. Consequently, G is p-nilpotent. □

Corollary 7.39. *Let $P \in \mathrm{Syl}_p(G)$ such that any two elements $x, y \in P$ conjugated in G are already conjugated in P. Then G is p-nilpotent.*

Proof. Let $g \in G$ and $x, [g, x] \in P$. Then $gxg^{-1} = [g, x]x \in P$ also holds. By assumption there exists $z \in P$ with $gxg^{-1} = zxz^{-1}$. It follows that $[g, x] = [z, x] \in P'$ and $G' \cap P = \mathrm{Foc}_G(P) = P'$. The assertion follows from Theorem 7.38. □

Definition 7.40. For a prime p let

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

Remark 7.41. By Theorem 4.18, $\mathrm{A}^p(G)$ (resp. $\mathrm{E}^p(G)$) is the smallest normal subgroup of G with (elementary) abelian p-factor group. For $P \in \mathrm{Syl}_p(G)$, $G = P\mathrm{O}^p(G)$ holds and therefore $\mathrm{A}^p(G) = P'\mathrm{O}^p(G)$ as well as $\mathrm{E}^p(G) = P'\langle x^p : x \in P\rangle \mathrm{O}^p(G) = \Phi(P)\mathrm{O}^p(G)$.

Theorem 7.42 (Tate's Transfer Theorem)**.** *Let $H \leq G$ with $p \nmid |G : H|$. Then the following statements are equivalent:*

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

Proof. The implications (1)⇒(2)⇒(3) are trivial. Now let $G/\mathrm{E}^p(G) \cong H/\mathrm{E}^p(H)$ and $P \in \mathrm{Syl}_p(H)$. Because $p \nmid |G : H|$, we have $P \in \mathrm{Syl}_p(G)$ and $G = H\mathrm{O}^p(G)$. From $H/H \cap \mathrm{O}^p(G) \cong H\mathrm{O}^p(G)/\mathrm{O}^p(G) = G/\mathrm{O}^p(G)$ it follows that $\mathrm{O}^p(H) \leq \mathrm{O}^p(G)$ and analogously $\mathrm{E}^p(H) = \mathrm{E}^p(G) \cap H$. Let $\overline{H} := H/\mathrm{O}^p(H)$. We use Lemma 7.34 with $N := \mathrm{O}^p(G)$, $K := H \cap N$ and $K_0/\mathrm{O}^p(H) := \Phi(\overline{K})$. Then $K/K_0 \cong \overline{K}/\Phi(\overline{K})$ is an abelian p-group and the transfer $N \to K/K_0$ is trivial. Thus one obtains $H = KL$ with $L \leq K$ and $K \cap L = K_0$. According to Dedekind,

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

It follows that $\overline{K} = \overline{K \cap L} = \overline{K_0} = \Phi(\overline{K}) = 1$. This shows

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

Remark 7.43.

(i) Theorem 7.42 was proven by Tate in 1964 using cohomological methods, while Thompson presented a character-theoretic proof in 1970. Brandis' group-theoretic approach from 1978 is largely unknown. For instance, Isaacs writes in his 2008 book that there seems to be no "simple" proof. Gagola and Isaacs later gave a group-theoretic proof, which is however significantly more elaborate than the proof above.

(ii) The proof of Theorem 7.42 shows that the factor groups listed in (1)–(3) are already isomorphic if their orders coincide. According to Burnside's Basis Theorem, (3) then means that $G/\mathrm{O}^p(G)$ and $H/\mathrm{O}^p(H)$ possess minimal generating systems of the same cardinality.

(iii) If the equivalent statements in Theorem 7.42 hold, one says: H *controls* the transfer in G. In this case, G is p-nilpotent if and only if H is p-nilpotent. Particularly interesting is the choice $H := \mathrm{N}_G(P)$, where $P \in \mathrm{Syl}_p(G)$. If P is abelian, then $G' \cap P = [H, P] \leq H' \cap P \leq G' \cap P$ according to Grün. Because of $G/\mathrm{A}^p(G) \cong P/(G' \cap P) \cong H/\mathrm{A}^p(H)$ (Theorem 7.12), H controls the transfer in this case. This is generalized in the next theorem.

Theorem 7.44 (Grün's Second Transfer Theorem)**.** *Let $P \in \mathrm{Syl}_p(G)$. For all $g \in G$ with ${}^g\mathrm{Z}(P) \leq P$, let ${}^g\mathrm{Z}(P) = \mathrm{Z}(P)$. Then $\mathrm{N}_G(\mathrm{Z}(P))$ controls the transfer in G.*

Proof. Let $Z := \mathrm{Z}(P)$ and $H := \mathrm{N}_G(Z)$. Since Z is characteristic in P, it holds that $P \leq \mathrm{N}_G(P) \leq H$. It suffices to show $G' \cap P \leq H' \cap P$. According to Grün's first theorem, we only need to prove $R := P \cap Q' \leq H'$ for all $Q \in \mathrm{Syl}_p(G)$. Let $g \in G$ with ${}^gP = Q$. Then $Z \leq \mathrm{C}_G(P) \leq \mathrm{N}_G(R)$ and ${}^gZ \leq \mathrm{C}_G(Q) \leq \mathrm{N}_G(R)$. We choose $P_1 \in \mathrm{Syl}_p(\mathrm{N}_G(R))$ and $x \in \mathrm{N}_G(R)$ with $Z \leq P_1$ and ${}^{xg}Z \leq P_1$. By Sylow, there exists $y \in G$ with ${}^yP_1 \leq P$. It follows that ${}^yZ \leq P$. The assumption now implies $y \in H$. Analogously, $yxg \in H$ and therefore $xg \in H$. This shows $R = {}^xR \leq P \cap {}^{xg}P' \leq H'$. □

Remark 7.45.

(i) Yoshida's transfer theorem states that $\mathrm{N}_G(P)$ controls the transfer if P has no factor group isomorphic to $C_p \wr C_p$ (where C_p acts regularly on itself). In particular, this holds if $|P| < |C_p \wr C_p| = p^{p+1}$ or if the nilpotency class of P is less than p (Exercise 46).

(ii) The next theorem has similarities with Lemma 5.14.

Theorem 7.46 (Roquette)**.** *Let $G = HN$ with $H \leq G$ and $N \trianglelefteq G$. Let $H \cap N \leq \Phi(H)$ and $\gcd(|H \cap N|, |G : H|) = 1$. Then H has a normal complement in G.*

Proof. We can assume that N is minimal as a normal subgroup with respect to the property $G = HN$. Let $K := H \cap N$ and π be the set of prime divisors of $|K|$. Then $M := \mathrm{O}^\pi(N)$ is characteristic in N and normal in G. Now $\gcd(|K|, |N : K|) = \gcd(|K|, |G : H|) = 1$ and $N = KM$ according to Lemma 1.9(vi). It follows that $HM = HKM = HN = G$ and the minimality of N shows $N = M$. Thus N has no proper π-factor groups. In particular, the transfer $N \to K/K'$ is trivial. Lemma 7.34 with $K_0 = K'$ yields $L \leq H$ with $H = KL$ and $K \cap L = K_0$. By assumption $H = KL = \Phi(H)L = L$ and therefore $K = K_0 = K'$. By Frattini, $\Phi(H)$ and thus also K is nilpotent. One obtains $K = 1$, i. e. N is a normal complement of H. □

Theorem 7.47 (Shemetkov)**.** *Let $N \trianglelefteq G$. Let π be a set of prime numbers p with the following property: There exists $P \in \mathrm{Syl}_p(G)$ such that $P \cap N$ is abelian and has a complement in P. Then there exists $H \leq G$ with $G = HN$ such that $H \cap N$ is a π'-group.*

Proof. We argue by induction on $|G| + |N| + |\pi|$.

Case 1: $N' < N$.
Let p be a prime with $M := \mathrm{O}^p(N) < N$. In the case $M = 1$, the claim follows with $G = H$ if $p \notin \pi$ or with Theorem 5.23 if $p \in \pi$. So let $M \neq 1$ and $\overline{G} := G/M$. Let $q \in \pi$. By assumption, there exists a q-Sylow subgroup $G_q = N_q \rtimes R$ of G, where $N_q \in \mathrm{Syl}_q(N)$ is abelian. Obviously, $\overline{N_q} \leq \overline{G_q}$ are Sylow

subgroups of $\overline{N}$ and $\overline{G}$ respectively, and $\overline{N_q}$ is abelian. Because of $R \cap N \leq R \cap G_q \cap N = R \cap N_q = 1$, we have $N_q M \cap RM = (N_q M \cap R)M = M$ and $\overline{G_q} = \overline{N_q} \rtimes \overline{R}$. By induction, there exists $K/M \leq \overline{G}$ with $G = KN$ such that $(K \cap N)/M$ is a π'-group.

For $q \neq p$, every q-Sylow subgroup of M is also a q-Sylow subgroup of N and therefore possesses a complement in K. Now let $q = p$ and $K_p \in \mathrm{Syl}_p(K)$. By Corollary 7.36, $M = \mathrm{O}^p(K_p M)$ possesses a complement R in $K_p M$. It holds that

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

By Sylow, R must normalize a Sylow p-subgroup M_p of M, because their number is 1 modulo p. Now R is a complement of M_p in the Sylow subgroup $M_p \rtimes R$ of K. Because of $M < N$, the claim holds for $M \leq K$ by induction, i. e. there exists $H \leq K$ with $K = HM$ such that $H \cap M$ is a π'-group. Then $G = KN = HMN = HN$ and because of

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

$H \cap N$ is also a π'-group.

Case 2: $N = N'$.
In the case $\pi = \varnothing$, the claim holds with $H = G$. So let $p \in \pi$ and $\tau := \pi \setminus \{p\}$. By induction, there exists $K \leq G$ with $G = KN$ such that $K \cap N$ is a τ'-group. We can assume that $K \cap N$ is not a π'-group, i. e. p divides $|K \cap N|$. Let $P \in \mathrm{Syl}_p(K \cap N)$. By Lemma 5.14, we may assume $K \cap N \leq \Phi(K)$. In particular, $K \cap N \trianglelefteq K$ is nilpotent and $P = \mathrm{O}_p(K \cap N) \trianglelefteq K \leq \mathrm{N}_G(P)$. We consider

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

By assumption, there exists an abelian Sylow p-subgroup N_p of N containing P. Certainly $N_p \in \mathrm{Syl}_p(\mathrm{C}_N(P))$ and N_p possesses a complement in L. Now let $q \in \tau$. A q-Sylow subgroup K_q of K normalizes a $\mathrm{C}_N(P)_q \in \mathrm{Syl}_q(\mathrm{C}_N(P))$. Since $K \cap N$ is a τ'-group, $K_q \cap \mathrm{C}_N(P)_q = 1$ and $\mathrm{C}_N(P)_q \rtimes K_q \in \mathrm{Syl}_q(L)$. By Taunt, $N_p \cap \mathrm{Z}(N) = N_p \cap \mathrm{Z}(N) \cap N' = 1$. In particular, $\mathrm{C}_N(P) < N$ and we can apply induction to $\mathrm{C}_N(P) \trianglelefteq L$. This yields $H \leq L$ with $L = H\mathrm{C}_N(P)$ such that $H \cap \mathrm{C}_N(P)$ is a π'-group. Then $G = KN = K\mathrm{N}_N(P)N = LN = HN$. Because $|N : \mathrm{C}_N(P)| \not\equiv 0 \pmod{p}$,

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

is a p'-group. On the other hand,

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

is a τ'-group. Overall, $H \cap N$ is a π'-group. □

Corollary 7.48. *Let $N \trianglelefteq G$. For every prime divisor p of $|G : N|$, let N possess an abelian Sylow p-subgroup with a complement in a Sylow subgroup of G. Then N possesses a complement in G.*

Proof. Let π be the set of all prime divisors of $|G : N|$. Theorem 7.47 yields $H \leq G$ with $G = HN$, such that $H \cap N$ is a π'-group. With Lemma 5.14 we can, on the other hand, achieve that $H \cap N$ is a π-group (see proof of Corollary 5.31). Thus $H \cap N = 1$. □

8 Generators and Relations

In this chapter, we again allow G to be an infinite group.

Definition 8.1. An *alphabet* shall be an arbitrary set A, whose elements we call *letters*. A *word* w is a sequence of the form $w = a_1^{\epsilon_1} \dots a_n^{\epsilon_n}$ with $a_1, \dots, a_n \in A$ and $\epsilon_1, \dots, \epsilon_n \in \{\pm 1\}$. Here, the *empty word* with $n = 0$ is also allowed. If $a_i \neq a_{i+1}$ or $\epsilon_i = \epsilon_{i+1}$ for $i = 1, \dots, n-1$, then w is called *reduced*. Obviously, one can transform every word w into a reduced word $\overline{w}$ by successively deleting parts of the form aa^{-1} or $a^{-1}a$ (according to Exercise 60, $\overline{w}$ is uniquely determined). On the set W of all words, $w \sim v :\Longleftrightarrow \overline{w} = \overline{v}$ defines an equivalence relation. The set of equivalence classes $F_A := \{[w] : w \in W\}$ then forms a group with respect to concatenation, i. e.

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

The identity element is the equivalence class of the empty word []. The inverse of $[a_1^{\epsilon_1} \dots a_n^{\epsilon_n}]$ is $[a_n^{-\epsilon_n} \dots a_1^{-\epsilon_1}]$. One calls F_A the *free group over the alphabet* A.

Remark 8.2.

(i) By means of the injection $A \to F_A$, $a \mapsto [a]$, we can regard A as a subset of F_A. Then $F_A = \langle A \rangle$ holds.

(ii) For $A = \varnothing$, $F_A = 1$. In the case $|A| = 1$, obviously $F_A \cong \mathbb{Z}$. For $|A| \geq 2$, F_A is non-abelian, because $\overline{aba^{-1}b^{-1}} = aba^{-1}b^{-1}$ for $a, b \in W$, $a \neq b$.

(iii) Let $w = a_1^{\epsilon_1} \dots a_n^{\epsilon_n} \in F_A \setminus \{1\}$ with finite order. After possible conjugation with $a_1^{-\epsilon_1}$, we can assume $a_1^{\epsilon_1} \neq a_n^{-\epsilon_n}$. Then, however, all powers w^n with $n \in \mathbb{N}$ would be reduced. This contradiction shows that F_A is torsion-free.

Theorem 8.3 (Universal property of free groups)**.** *Every map $A \to G$ can be extended to exactly one homomorphism $F_A \to G$.*

Proof. Let $f \colon A \to G$ be given. For $w = a_1^{\epsilon_1} \dots a_n^{\epsilon_n} \in W$ we define $\widehat{f}(w) := f(a_1)^{\epsilon_1} \dots f(a_n)^{\epsilon_n} \in G$. Obviously $\widehat{f}(\overline{w}) = \widehat{f}(w)$. Thus $\widehat{f}$ induces a well-defined map $F_A \to G$, which we also denote by $\widehat{f}$. Because of $\widehat{f}(wv) = \widehat{f}(w)\widehat{f}(v)$ for $w, v \in W$, $\widehat{f}$ is a homomorphism. Because of $F_A = \langle A \rangle$, $\widehat{f}$ is uniquely determined by f. □

Theorem 8.4. *For finite alphabets A and B, F_A and F_B are isomorphic if and only if $|A| = |B|$ holds.*

Proof. First let $f \colon A \to B$ be a bijection. Because of $B \subseteq F_B$, there exists a homomorphic extension $\widehat{f} \colon F_A \to F_B$ of f according to Theorem 8.3. Analogously, f^{-1} also has a homomorphic extension $\widehat{f^{-1}} \colon F_B \to F_A$. Because of $F_A = \langle A \rangle$ and $F_B = \langle B \rangle$, $\widehat{f} \circ \widehat{f^{-1}} = 1$ and $\widehat{f^{-1}} \circ \widehat{f} = 1$. Thus F_A and F_B are isomorphic (the finiteness of A and B is not used for this direction).

Conversely, assume now that F_A and F_B are isomorphic. Since there are exactly $2^{|A|}$ maps of the form $A \to C_2$, there exist, according to Theorem 8.3, exactly that many homomorphisms $F_A \to C_2$. Because of $F_A \cong F_B$, there exist exactly $2^{|A|}$ homomorphisms of the form $F_B \to C_2$. This shows $|A| = |B|$. □

Definition 8.5. In the situation of Theorem 8.4, $\operatorname{rk} F_A := |A|$ is called the *rank* of F_A. A free group of rank $k \in \mathbb{N}$ is denoted by F_k.

Theorem 8.6. *Let X be a generating set of G with the property that every map from X into a group H has a homomorphic extension $G \to H$. Then $G \cong F_X$.*

Proof. By assumption, there exists a homomorphism $f\colon G \to F_X$ with $f(x) = x$ for $x \in X$. According to Theorem 8.3, there also exists a homomorphism $g\colon F_X \to G$ with $g(x) = x$ for $x \in X$. Obviously then $f \circ g = \mathrm{id}_{F_X}$ and $g \circ f = \mathrm{id}_G$. This shows that f is an isomorphism. □

Theorem 8.7. *Every group G is isomorphic to a factor group of a free group F. If G can be generated by n elements, then one can choose* $\operatorname{rk} F = n$.

Proof. Let X be a generating set of G. According to Theorem 8.3, there exists a homomorphism $f\colon F_X \to G$ with $f(x) = x$. Obviously f is surjective and the claim follows from the homomorphism theorem. □

Remark 8.8.

(i) Let X be a generating set for G and $f\colon F_X \to G$ with $f(x) = x$ as in Theorem 8.7. The elements in $\operatorname{Ker}(f)$ are called *relators* for G w.r.t. X. For $x_1^{\epsilon_1} \dots x_n^{\epsilon_n} \in \operatorname{Ker}(f)$, the equation $x_1^{\epsilon_1} \dots x_n^{\epsilon_n} = 1$ holds in G. An equation of this form is called a *relation* for G w.r.t. X.

(ii) Conversely, let F_A be a free group and $X \subseteq F_A$. Let $N := \langle gXg^{-1} : g \in F_A \rangle \trianglelefteq F_A$ be the normal closure of X in F_A. We set

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

One often identifies letters $a \in A$ with their cosets $aN \in \langle A \mid X \rangle$ (in general not injective!). If $|A| + |X| < \infty$, then $\langle A \mid X \rangle$ is called *finitely presented*. In this way, every group can be described, but in general it is difficult to determine the properties of $\langle A \mid X \rangle$. For example, there exist finitely presented groups for which it cannot be algorithmically decided whether they are trivial!

Example 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) Let $G := \langle x, y, z \mid xyx^{-1} = y^2, yzy^{-1} = z^2, zxz^{-1} = x^2 \rangle$. For $a, b \in \mathbb{N}$ we have

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

By cyclic permutation of x, y, z one obtains analogous equations. It follows that

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

and $x = z^{-1} y^{-16} z^2 y^2 \in \langle y, z \rangle$. Thus $G = \langle y, z \rangle$. Because $N := \langle z \rangle \trianglelefteq G$ and $G/N = \langle yN \rangle$, G is solvable. On the other hand, $y = xyx^{-1}y^{-1} \in G'$ and analogously $x, z \in G'$. This shows $G = 1$ (otherwise $G = G' < G$ would hold).

Theorem 8.10 (von Dyck)**.** *Let $G = \langle x_i : i \in I \rangle$ and $H = \langle y_i : i \in I \rangle$ be groups such that for every relation $x_{i_1}^{\epsilon_1} \dots x_{i_n}^{\epsilon_n} = 1$ in G, the relation $y_{i_1}^{\epsilon_1} \dots y_{i_n}^{\epsilon_n} = 1$ also holds in H. Then there exists an epimorphism $f\colon G \to H$ with $f(x_i) = y_i$ for $i \in I$.*

Proof. By Theorem 8.3, there exist epimorphisms $f_G\colon F_I \to G$ and $f_H\colon F_I \to H$ with $f_G(i) = x_i$ and $f_H(i) = y_i$ for $i \in I$. By assumption, $\mathrm{Ker}(f_G) \leq \mathrm{Ker}(f_H)$ holds. Thus

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

is the desired epimorphism. □

Example 8.11.

(i) Let $G := \langle x_1, \ldots, x_n \mid [x_i, x_j] = 1\ \forall i, j\rangle$. Apparently G is abelian and every element in G has the form $x_1^{a_1} \ldots x_n^{a_n}$ with $a_1, \ldots, a_n \in \mathbb{Z}$. Now let $H := \langle y_1\rangle \oplus \ldots \oplus \langle y_n\rangle \cong C_\infty^n$. According to Theorem 8.10 there exists an epimorphism $f\colon G \to H$ with $f(x_i) = y_i$ for $i = 1, \ldots, n$. Apparently f is also injective and $G \cong H \cong C_\infty^n$. This explains the term *free abelian group*. In general, every abelian group is apparently isomorphic to a factor group of $\langle (x_i)_{i\in I} : [x_i, x_j] = 1\ \forall i, j \in I\rangle$.

(ii) Let $G := \langle x, y \mid x^n = y^2 = (xy)^2 = 1\rangle$ for $n \geq 2$. Because of $xyxy = 1$ and $y^2 = 1$ we have $xy = y^{-1}x^{-1} = yx^{-1}$. In this way, one can write every element in G in the form $x^i y^j$ with $i, j \in \mathbb{Z}$. Because of $x^n = y^2 = 1$ one can assume $i \in \{0, \ldots, n-1\}$ and $j \in \{0, 1\}$. In particular, $|G| \leq 2n$ holds. Now let $H \cong D_{2n}$. Then there exist elements $\widetilde{x}, \widetilde{y} \in H$ with $H = \langle\widetilde{x}\rangle \rtimes \langle\widetilde{y}\rangle$. In particular $\widetilde{x}^n = \widetilde{y}^2 = 1$. Furthermore $\widetilde{y}\widetilde{x}\widetilde{y}^{-1} = \widetilde{x}^{-1}$ holds, thus $(\widetilde{x}\widetilde{y})^2 = 1$. According to Theorem 8.10 there is an epimorphism $G \to H$. Because of $|H| = 2n \geq |G|$, it follows that $G \cong H \cong D_{2n}$.

Remark 8.12 (Coxeter-Todd algorithm)**.** To estimate the size of a group $G = \langle X \mid R\rangle$ from above, one first looks for a "known" subgroup $H \leq G$ (for example $H = \langle x\rangle$ for an $x \in X$). Then one chooses a list L of left cosets modulo H, such that G permutes the elements of L by left multiplication. Since in general G acts transitively on G/H, L must already contain all cosets modulo H. This shows $|G| \leq |L||H|$ (cosets may appear multiple times in L).

Theorem 8.13 (Carmichael)**.** *For $n \geq 2$ we have*

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

Proof. Let G be the group on the right side. For $n = 2$, $A_2 = 1 = \langle\varnothing\rangle = G$. Therefore, let $n \geq 3$ and $m := n - 2$. Let $H := \langle x_1, \ldots, x_{m-1}\rangle \leq G$. By von Dyck, H is a factor group of A_{n-1}. In particular, $|H| \leq \frac{1}{2}(n-1)!$. For $i \neq j$, $x_i x_j = (x_i x_j)^{-1} = x_j^{-1} x_i^{-1} = x_j^2 x_i^2$ holds in G. We consider the n cosets

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

For $i, j < m$ with $i \neq j$, we have

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

This shows that G acts on L by left multiplication. One obtains $|G| \leq n|H| \leq n!/2$.

Conversely, the elements $x_i := (1, 2, i+2)$ for $i = 1, \ldots, n-2$ in A_n satisfy the given relations, because $x_i x_j = (1, i+2)(2, j+2)$ for $i \neq j$. By Theorem 8.10, there exists an isomorphism $G \to A_n$. □

Theorem 8.14 (Gauss)**.** *For every prime p and $n \geq 1$,*

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

Proof. By Theorem 2.4, $\mathrm{Aut}(C_{p^n}) \cong (\mathbb{Z}/p^n\mathbb{Z})^\times =: G$.

First let $p > 2$. We must show that G is cyclic. In the case $n = 1$, $G = \mathbb{F}_p^\times$ and the claim holds (Algebra or Theorem 9.8). Now let $n \geq 2$. Then $|G| = \varphi(p^n) = p^{n-1}(p-1)$. The canonical map $\Psi\colon G \to (\mathbb{Z}/p\mathbb{Z})^\times$, $a + p^n\mathbb{Z} \mapsto a + p\mathbb{Z}$ is clearly an epimorphism. In particular, $P := \mathrm{Ker}(\Psi) \in \mathrm{Syl}_p(G)$ and $G/P \cong C_{p-1}$. By Theorem 2.11, it suffices to show that P is cyclic. We show more precisely that P is generated by $1 + p + p^n\mathbb{Z} \in P$. For this, one calculates

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

Now let $p = 2$ and wlog. $n \geq 2$. Then $|G| = 2^{n-1}$. Because of $(-1 + 2^n\mathbb{Z})^2 = 1 + 2^n\mathbb{Z}$, it suffices to show

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

The case $n = 2$ is clear. So let $n \geq 3$. One calculates

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

and

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

Thus $|\langle 5+2^n\mathbb{Z} \rangle| = 2^{n-2}$. Because of $-1 \not\equiv 1+2^{n-1} \pmod{2^n}$, we also have $\langle -1+2^n\mathbb{Z} \rangle \cap \langle 5+2^n\mathbb{Z} \rangle = 1$. □

Theorem 8.15. *Let P be a p-group of order p^n with a cyclic subgroup of order p^{n-1}. Then one of the following statements holds:*

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

(ii) $n \geq 3$ *and* $P \cong M_{p^n} := \langle x, y \mid x^{p^{n-1}} = y^p = 1,\ yxy^{-1} = x^{1+p^{n-2}} \rangle$ (modular group[18]).

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

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

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

Proof. If P is abelian, then (i) obviously holds by Theorem 2.11. Now let P be non-abelian. Then $n \geq 3$. Let $x \in P$ with $|\langle x \rangle| = p^{n-1}$. Then $\langle x \rangle \trianglelefteq P$ by Theorem 4.10. Let us first assume that $\langle x \rangle$ has a complement in P, i. e. $P = \langle x \rangle \rtimes \langle y \rangle$ for some $y \in P$ with $y^p = 1$. If $p > 2$, then $\mathrm{Aut}(\langle x \rangle)$ is cyclic by Theorem 8.14. By replacing y with a power if necessary, one achieves $yxy^{-1} = x^{1+p^{n-2}}$, because $(1 + p^{n-2})^p \equiv 1 \pmod{p^{n-1}}$. By Theorem 8.10 there exists an epimorphism $M_{p^n} \to P$. Obviously $|M_{p^n}| \leq p^n$ holds and it follows that $P \cong M_{p^n}$.

[18] *Modular* means that a generalization of the Dedekind identity holds: $U \leq W \Rightarrow \langle U, V \rangle \cap W = \langle U, V \cap W \rangle$ for all $U, V, W \leq G$. For $G = M_{p^n}$, even $\langle U, V \rangle = UV$ holds, i. e. $UV = VU$ for all $U, V \leq M_{p^n}$ (Exercise 66)

Now let $p = 2$. In the case $n = 3$, $\mathrm{Aut}(\langle x\rangle)$ is still cyclic and one again obtains $P \cong M_8 \cong D_8$. So let $n \geq 4$. By Theorem 8.14, $\mathrm{Aut}(\langle x\rangle)$ has exactly three involutions (=elements of order 2): $x \mapsto x^{-1}$, $x \mapsto x^{1+2^{n-2}}$ and $x \mapsto x^{-1+2^{n-2}}$. The first case leads to $P \cong D_{2^n}$, the second to $P \cong M_{2^n}$ and the third to $P \cong SD_{2^n}$.

In the following we can assume that $\langle x\rangle$ has no complement in P. Let $y \in P \setminus \langle x\rangle$. Then $y^p \in \langle x\rangle = \mathrm{C}_P(x)$. The action of $\langle y\rangle$ on $\langle x\rangle$ thus still induces an automorphism of order p. In the case $y^p \notin \langle x^p\rangle$, $P = \langle y\rangle$ would be abelian. So let $i \in \mathbb{Z}$ with

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

In the case $yxy^{-1} = x^{1+p^{n-2}}$, we have $[y, x] = x^{1+p^{n-2}}x^{-1} = x^{p^{n-2}} \in \mathrm{Z}(P)$ and Exercise 18(b) yields

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

But then $\langle x^i y\rangle$ would be a complement of $\langle x\rangle$. Thus $p = 2$ and $yxy^{-1} \in \{x^{-1}, x^{-1+2^{n-2}}\}$, where in the second case $n \geq 4$ holds. In both cases $y^2 = yy^2y^{-1} = yx^{2k}y^{-1} = x^{-2k} = y^{-2}$ and $y^4 = 1$. This shows $y^2 = x^{2^{n-2}}$. If now $yxy^{-1} = x^{-1+2^{n-2}} = x^{-1}y^2$, then $(xy)^2 = x(yxy^{-1})y^2 = y^4 = 1$. Then $\langle xy\rangle$ would be a complement of $\langle x\rangle$. Thus $yxy^{-1} = x^{-1}$ and there is an epimorphism $Q_{2^n} \to P$. It is easy to see that $|Q_{2^n}| \leq 2^n$ holds. Thus $P \cong Q_{2^n}$. □

Theorem 8.16. *The groups M_{p^n}, D_{2^n}, Q_{2^n} and SD_{2^n} have order p^n (resp. 2^n) and are pairwise non-isomorphic.*

Proof. It is clear that one can construct semidirect products $C_{p^{n-1}} \rtimes C_p$ with suitable operations. Thus Theorem 8.15 shows that M_{p^n}, D_{2^n} and SD_{2^n} have the "correct" order. Now let $\zeta := e^{2\pi\mathrm{i}/2^{n-1}} \in \mathbb{C}$ and $Q = \langle x, y\rangle \leq \mathrm{GL}(2, \mathbb{C})$ with

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

Apparently $x^{2^{n-1}} = 1$, $y^2 = x^{2^{n-2}}$ and $yxy^{-1} = x^{-1}$ holds. Thus every element in Q has the form $x^i y^j$ with $i \in \{0, \ldots, 2^{n-1} - 1\}$ and $j \in \{0, 1\}$. Because of $y \notin \langle x\rangle$, $|Q| = 2^n$. According to Theorem 8.15, $Q \cong Q_{2^n}$ holds.

It remains to show that the groups M_{2^n}, D_{2^n}, Q_{2^n} and SD_{2^n} are pairwise non-isomorphic (with the exception $M_8 \cong D_8$). The semidirect products M_{2^n}, D_{2^n} and SD_{2^n} possess at least two involutions. In Q_{2^n}, on the other hand, $(x^i y)^2 = x^i yx^i y^{-1}y^2 = y^2 \neq 1$ for $i \in \mathbb{Z}$. Therefore Q_{2^n} possesses only one involution and $Q_{2^n} \ncong M_{2^n}$, $Q_{2^n} \ncong D_{2^n}$ and $Q_{2^n} \ncong SD_{2^n}$ holds. We can now assume $n \geq 4$. In the group M_{2^n}, $\langle [x, y]\rangle = \langle x(yx^{-1}y^{-1})\rangle = \langle x^{2^{n-2}}\rangle \trianglelefteq M_{2^n}$ holds. Since $M_{2^n}/\langle [x, y]\rangle$ is abelian, $M'_{2^n} = \langle [x, y]\rangle \cong C_2$ holds. In D_{2^n}, on the other hand, $[x, y] = x^2$ holds and thus $|D'_{2^n}| \geq 2^{n-2}$. In SD_{2^n}, analogously $[x, y] = x^{2+2^{n-2}}$ and $|SD'_{2^n}| \geq 2^{n-2}$. This shows $M_{2^n} \ncong D_{2^n}$ and $M_{2^n} \ncong SD_{2^n}$. Finally, we still have to distinguish D_{2^n} from SD_{2^n}. According to Burnside's Basis Theorem,

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

The maximal subgroups of D_{2^n} are therefore $\langle x\rangle \cong C_{2^{n-1}}$, $\langle x^2, y\rangle \cong D_{2^{n-1}}$ and $\langle x^2, xy\rangle \cong D_{2^{n-1}}$. The maximal subgroups of SD_{2^n} are on the other hand $\langle x\rangle \cong C_{2^{n-1}}$, $\langle x^2, y\rangle \cong D_{2^{n-1}}$ and $\langle x^2, xy\rangle \cong Q_{2^{n-1}} \ncong D_{2^{n-1}}$. Thus $D_{2^n} \ncong SD_{2^n}$. □

9 Central Products and the Generalized Fitting Group

Remark 9.1. Let P be a non-abelian p-group of order p^n. Since P is not cyclic, $|P : P'| \geq |P : \Phi(P)| \geq p^2$ holds. This shows that the nilpotency class of P is at most $n-1$ (Theorem 3.9). If equality holds, one says: P has *maximal class*. In this case $|P : P^{[k]}| = p^k$ for $k \geq 2$.

Lemma 9.2. *Let P be a p-group of order p^n with maximal class. Let $N \trianglelefteq P$ with $|N| = p^k \leq p^{n-2}$. Then $N = \mathrm{Z}_k(P) = P^{[n-k]}$.*

Proof. Induction on n: For $n = 3$, the claim follows from Example 4.22. So let $n \geq 4$ and $N \neq 1$. Since $P/\mathrm{Z}(P)$ also has maximal class, it holds that $|\mathrm{Z}(P)| = p$. According to Theorem 3.14, $\mathrm{Z}(P) \leq N$. Induction therefore implies $N/\mathrm{Z}(P) = \mathrm{Z}_{k-1}(P/\mathrm{Z}(P)) = \mathrm{Z}_k(P)/\mathrm{Z}(P)$ and $N = \mathrm{Z}_k(P)$. According to Remark 9.1, $P^{[n-k]}$ is also a normal subgroup of order p^k. Thus $P^{[n-k]} = \mathrm{Z}_k(P) = N$. □

Theorem 9.3 (Taussky)**.** *For every non-abelian 2-group P, the following statements are equivalent:*

(1) P has maximal class.

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

(3) P is a dihedral group, a quaternion group, or a semi-dihedral group.

Proof. The implication (1)⇒(2) follows from Remark 9.1. Now let $|P : P'| = 4$. Let $2^n := |P|$ be minimal such that (3) is not satisfied. We have already seen in Theorem 8.16 that $|M'_{2^n}| = 2$ holds. According to Theorem 8.15, it follows that $\exp(P) \leq 2^{n-2}$. Let $Z \leq \mathrm{Z}(P) \cap P'$ with $|Z| = 2$ (Theorem 3.14). Then $|P/Z : (P/Z)'| = |P/P'| = 4$. By the choice of P, $P/Z \in \{D_{2^{n-1}}, Q_{2^{n-1}}, SD_{2^{n-1}}\}$. So let $x \in P$ with $|P : \langle x\rangle Z| = 2$. Because of $Z \leq \mathrm{Z}(P)$ and $\exp(P) \leq 2^{n-2}$, $\langle x\rangle Z \cong C_{2^{n-2}} \times C_2$. From Exercise 28 it follows that $\mathrm{Z}(P) = Z$. For $y \in P \setminus \langle x\rangle Z$, it holds that $yxy^{-1} \in x^{-1}Z \cup x^{-1+2^{n-3}}Z$ and $yx^2y^{-1} = x^{-2}$. This yields the contradiction $x^{2^{n-3}} \in \mathrm{Z}(P) = Z$. Thus (3) must hold.

Now let $P \in \{D_{2^n}, Q_{2^n}, SD_{2^n}\}$. We show (1) by induction on n (cf. Exercise 19). In the case $n = 3$, D_8 and Q_8 are non-abelian and therefore of maximal class. Now let $n \geq 4$. Then $[x, y] \in \{x^2, x^{2+2^{n-2}}\}$ and $P' = \langle x^2\rangle$. From Exercise 28 it follows that $\mathrm{Z}(P) = \langle x^{2^{n-2}}\rangle$. By induction, $P/\mathrm{Z}(P) \cong D_{2^{n-1}}$ has maximal class and therefore so does P. □

Remark 9.4. For $p > 2$, there are non-abelian p-groups P with $|P : P'| = p^2$ that do not have maximal class. Blackburn has classified all 3-groups with maximal class. On the other hand, the p-groups of maximal class for $p > 3$ are not known.

Theorem 9.5. *Let P be a non-cyclic p-group in which every abelian normal subgroup is cyclic. Then $p = 2$ and P has maximal class.*

Proof. Let $A \trianglelefteq P$ be a maximal abelian normal subgroup (i. e. there is no abelian normal subgroup of P that properly contains A). By assumption, A is cyclic and therefore $A < P$. Furthermore, $A \leq \mathrm{C}_P(A) \trianglelefteq P$. Let us assume $A < \mathrm{C}_P(A)$. Since the chief factors of P all have order p (Example 3.8), there exists a normal subgroup $N \trianglelefteq P$ with $A < N \leq \mathrm{C}_P(A)$ and $|N : A| = p$. Then $A \leq \mathrm{Z}(\mathrm{C}_P(A)) \cap N \leq \mathrm{Z}(N)$ and $N/\mathrm{Z}(N)$ is cyclic. Thus N is abelian, contradicting the choice of A. This shows $\mathrm{C}_P(A) = A$ and $P/A \leq \mathrm{Aut}(A)$. In the case $|A| = p$, we would have $p \nmid |\mathrm{Aut}(A)|$. Thus $|A| \geq p^2$. Let $B \leq A$ with $|B| = p^2$. Since A is cyclic, $B \trianglelefteq P$ holds. For $C := \mathrm{C}_P(B) \trianglelefteq P$, we have $P/C \leq \mathrm{Aut}(B) \cong C_{p(p-1)}$ and therefore $|P : C| \leq p$.

Let us assume $A < C$. As usual, there exists an $N \trianglelefteq P$ with $A < N \leq C$ and $|N : A| = p$. By the choice of A, N is non-abelian and we can apply Theorem 8.15. Because of $B \leq \mathrm{Z}(N)$, according to Taussky, only $N \cong M_{p^n}$ is possible. It holds that $M'_{p^n} = \langle x^{p^{n-2}} \rangle \cong C_p$ and $M_{p^n}/M'_{p^n} \cong C_{p^{n-2}} \times C_p$. Every element of order p in M_{p^n} thus lies in $\langle x^{p^{n-3}}, y \rangle$. Since $x^{p^{n-3}}$ has order p^2, the elements of order p in M_{p^n} form the characteristic subgroup $E := \langle x^{p^{n-2}}, y \rangle \cong C_p \times C_p$. But then E is a non-cyclic, abelian normal subgroup of P. This contradiction shows $A = C$.

Thus $|P : A| = p$. Again, Theorem 8.15 can be applied. The case $P \cong M_{p^n}$ is excluded as before. This shows the claim. □

Theorem 9.6. *For every p-group P, the following statements are equivalent:*

(1) P possesses only one subgroup of order p.

(2) Every abelian subgroup of P is cyclic.

(3) P is cyclic or a quaternion group.

Proof. The implication (1)⇒(2) follows from Theorem 2.11. If (2) holds, then P is cyclic, a dihedral group, a quaternion group, or a semi-dihedral group by Theorem 9.5. In (semi-)dihedral groups, the abelian subgroup $\langle x^{2^{n-2}}, y \rangle$ is not cyclic. This shows (3). Now let us assume (3). If P is cyclic, then (1) follows from Theorem 2.4. For quaternion groups, we had already seen in Theorem 8.16 that only one involution exists. □

Lemma 9.7. *For every prime p, there exist $\lambda, \mu \in \mathbb{F}_p$ with $\lambda^2 + \mu^2 = -1$.*

Proof. For $p = 2$ choose $\lambda = 1$ and $\mu = 0$. Let therefore $p > 2$. From $\lambda^2 = \mu^2$ it follows that $(\lambda + \mu)(\lambda - \mu) = 0$ and $\lambda = \pm\mu$. This shows $|\{\lambda^2 + 1 : \lambda \in \mathbb{F}_p\}| = |\{-\mu^2 : \mu \in \mathbb{F}_p\}| \geq \lceil p/2 \rceil > p/2$. By the pigeonhole principle,

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

Theorem 9.8 (Wedderburn)**.** *Every finite skew field is a field with a cyclic multiplicative group.*

Proof (Kaczynski). Let K be a finite skew field and $p \in \mathbb{N}$ the order of 1 in $(K, +)$. Assume p is not a prime number, say $p = ab$ with $a, b > 1$. Then

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

Since K is a skew field, one obtains the contradiction $\sum_{i=1}^{a} 1 = 0$ or $\sum_{i=1}^{b} 1 = 0$. Therefore p is a prime number and K is an $\mathbb{F}_p$-vector space. For a subgroup $H \leq G := K^\times$ let

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

By the distributive law, $L(H)$ is closed under multiplication. Since every element in G has finite order, $L(H)$ is also closed under division, i. e. $L(H)$ is itself a skew field. Suppose that H is an elementary abelian q-group of rank 2. Then $L(H)$ is a field in which the polynomial $X^q - 1$ has more than q roots. This contradiction shows that every abelian subgroup of G is cyclic. By Theorem 9.6, every Sylow subgroup of G is cyclic or a quaternion group.

Suppose that a 2-Sylow subgroup P of G is indeed a quaternion group. Because $|G| = |K| - 1$, then $p > 2$. Let $x, y \in P$ be of order 4 with $xy = yx^{-1}$. In the field $L(\langle x \rangle)$, $x^2 \neq 1$ is a root of $X^2 - 1$, so $x^2 = -1$ and $xy = -yx$. Analogously $y^2 = -1$. Let $\lambda, \mu \in \mathbb{F}_p$ be as in Lemma 9.7. Then

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

Thus $y = -\lambda x \pm \mu$ and one has the contradiction $xy = yx = -xy$. Now all Sylow subgroups of G are cyclic. It suffices to show that G is abelian.

By Theorem 7.24, G is at least solvable. Assume $G \neq \mathrm{Z}(G)$. Let $A/\mathrm{Z}(G)$ be a minimal normal subgroup of $G/\mathrm{Z}(G)$. Then $A/\mathrm{Z}(G)$ is an elementary abelian q-group. Since the q-Sylow subgroups of G and $G/\mathrm{Z}(G)$ are cyclic, $|A/\mathrm{Z}(G)| = q$. By Exercise 10, A is abelian. Let $g \in G$ and $x \in A$ be arbitrary. Because $A \trianglelefteq G$, there exists $y \in A$ with $(1 + g)x = y(1 + g)$ (even if $1 + g = 0$). It follows

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

In the case $x - y = y - gxg^{-1} = 0$, then $x = y = gxg^{-1}$, i. e. $g \in \mathrm{C}_G(x)$. Otherwise it follows $g = (y - gxg^{-1})^{-1}(x - y) \in \mathrm{C}_G(x)$, since A is abelian. Since $g \in G$ and $x \in A$ were arbitrary, the contradiction $A \leq \mathrm{Z}(G)$ follows. Thus $K^\times = G = \mathrm{Z}(G)$ is abelian and cyclic. □

Theorem 9.9. *For a prime p, there are up to isomorphism exactly five groups of order p^3. These are given by:*

(i) C_{p^3}.

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

(iii) C_p^3.

(iv) M_{p^3}.

(v) Q_8 *for* $p = 2$.

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

Proof. Let $|P| = p^3$. We can certainly assume that P is non-abelian. According to Theorem 8.15, we may also assume $\exp(P) = p$. Then $p > 2$, because otherwise $xy = (xy)^{-1} = y^{-1}x^{-1} = yx$ for $x, y \in P$. Since $|P : \Phi(P)| = p^2$, P can be generated by two elements x, y. Then certainly $x^p = y^p = 1$ and $[x, x, y], [y, x, y] \in P^{[3]} = 1$. According to Theorem 8.10, there is an epimorphism $p_+^{1+2} \to P$. We must now show that $|p_+^{1+2}| \leq p^3$ holds. For this, let $z := [x, y]$. According to Exercise 18, $z^p = [x^p, y] = 1$. Because $xy = [x, y]yx = zyx = yxz$, every element in p_+^{1+2} can be written in the form $x^i y^j z^k$ with $i, j, k \in \{0, \ldots, p - 1\}$. This shows $P \cong p_+^{1+2}$.

It remains to show that the last case actually occurs. For this, we consider the group $P \leq \mathrm{GL}(3, p)$ of upper triangular matrices with ones on the main diagonal. Then $|P| = p^3$. Because

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

P is non-abelian. According to the binomial formula, $x^p - 1 = (x - 1)^p = (x - 1)^3(x - 1)^{p-3} = 0$ for all $x \in P$, because

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

This shows $\exp(P) = p$. □

Definition 9.10. A p-group P is called *extraspecial*, if $P' = \Phi(P) = \mathrm{Z}(P) \cong C_p$ holds.

Example 9.11. According to Example 4.22, every non-abelian group of order p^3 is extraspecial.

Lemma 9.12. *Let P be extraspecial and $\alpha \in \mathrm{Aut}(P)$ with $\alpha(x)\mathrm{Z}(P) = x\mathrm{Z}(P)$ for all $x \in P$. Then $\alpha \in \mathrm{Inn}(P)$.*

Proof. Let $|P/\mathrm{Z}(P)| = p^n$. Then there exists a generating system $x_1, \ldots, x_n \in P$ of P. We have $\alpha(x_i) \in x_i\mathrm{Z}(P)$ for $i = 1, \ldots, n$ and α is uniquely determined by these images. Thus there are at most p^n many automorphisms with the specified property. On the other hand, every inner automorphism satisfies the condition. Because $|\mathrm{Inn}(P)| = |P/\mathrm{Z}(P)| = p^n$, the claim follows. □

Lemma 9.13. *Let P be an extraspecial subgroup of a group G with $[G, P] \leq \mathrm{Z}(P)$. Then $G = P\mathrm{C}_G(P)$.*

Proof. Because of $[G, P] \leq \mathrm{Z}(P) \leq P$, we have $P \trianglelefteq G$. For $g \in G$, $\alpha(x) := gxg^{-1}$ $(x \in P)$ defines an automorphism on P. Here, $\alpha(x)\mathrm{Z}(P) = gxg^{-1}x^{-1}x\mathrm{Z}(P) = [g, x]x\mathrm{Z}(P) = x\mathrm{Z}(P)$ holds. According to Lemma 9.12, α is an inner automorphism on P. Therefore, there exists an $x \in P$ with $gyg^{-1} = \alpha(y) = xyx^{-1}$ for all $y \in P$. It follows that $g = xx^{-1}g \in P\mathrm{C}_G(P)$. □

Definition 9.14. A group G is called a *central product* of subgroups $N_1, \ldots, N_k \leq G$ if:

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

We write $G = N_1 * \ldots * N_k$.

Remark 9.15. Because of $[N_i, N_j] = 1$, we have $N_i \trianglelefteq G = N_1 * \ldots * N_k$ for $i = 1, \ldots, k$. Thus, the direct sum $N_1 \oplus \ldots \oplus N_k$ is also a central product. As with the direct sum, $N * M = M * N$ and $(N_1 * N_2) * N_3 = N_1 * (N_2 * N_3)$ hold (cf. Remark 2.8).

Example 9.16. It holds that $C_2 \cong C_2 * C_2$, but also $C_2^2 \cong C_2 * C_2$. The notation $N_1 * \ldots * N_k$ is therefore generally not unique.

Theorem 9.17. *Let $G = N_1 * \ldots * N_k$ with $k \geq 2$. Then $\bigcap_{i=1}^k N_i \leq \mathrm{Z}(G)$ and*

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

Proof. Because of $[N_i, N_j] = 1$, we have $\bigcap_{i=1}^k N_i \leq \mathrm{Z}(\langle N_1, \ldots, N_k \rangle) = \mathrm{Z}(G)$ and $N_i\mathrm{Z}(G)/\mathrm{Z}(G) \cong N_i/N_i \cap \mathrm{Z}(G) = N_i/\mathrm{Z}(N_i)$. It thus suffices to show $G/\mathrm{Z}(G) = N_1\mathrm{Z}(G)/\mathrm{Z}(G) \oplus \ldots \oplus N_k\mathrm{Z}(G)/\mathrm{Z}(G)$. It holds that $N_i\mathrm{Z}(G) \cap \prod_{j \neq i} N_j\mathrm{Z}(G) = \mathrm{Z}(G)$. The claim follows. □

Remark 9.18. Analogous to the direct product (vs. direct sum), we now construct an "outer" central product.

Theorem 9.19. *Let $G_1, \ldots, G_k$ be groups with $Z_i \leq \mathrm{Z}(G_i)$ and $Z_1 \cong \ldots \cong Z_k$ with $k \geq 2$. Then there exists a central product of the form $G = N_1 * \ldots * N_k$ with $N_i \cong G_i$ $(i = 1, \ldots, k)$ and $\bigcap_{i=1}^k N_i \cong Z_1$.*

Proof. We choose isomorphisms $\varphi_i\colon Z_1 \to Z_i$ for $i = 2, \ldots, k$. Then

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

Let $G := (G_1 \times \ldots \times G_k)/Z$. Then G is generated by the normal subgroups

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

Here, $[N_i, N_j] = [G_iZ/Z, G_jZ/Z] = [G_i, G_j]Z/Z = 1$ holds for $i \neq j$. Thus $G = N_1 * \ldots * N_k$. For $z_1 \in Z_1$ and $i \in \{1, \ldots, k\}$, we have $z_1Z = z_1z_1^{-1}\varphi_i(z_1)Z = \varphi_i(z_1)Z$. This shows

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

Now let $g_1Z = \ldots = g_kZ \in \bigcap_{i=1}^{k} N_i$ with $g_i \in G_i$. Then $g_1^{-1}g_i \in Z \leq Z_1 \times \ldots \times Z_k$ and it follows that $g_i \in Z_i$ for $i = 1, \ldots, k$. Thus $\bigcap_{i=1}^{k} N_i = Z_1Z/Z \cong Z_1$. □

Theorem 9.20. *Every extraspecial p-group P has the form $P = E_1 * \ldots * E_k$ with $E_i \in \{D_8, Q_8\}$ (if $p = 2$) or $E_i \in \{M_{p^3}, p_+^{1+2}\}$ (if $p > 2$) for $i = 1, \ldots, k$. Here $\bigcap_{i=1}^{k} E_i = \mathrm{Z}(P)$, if $k \geq 2$. In particular, $|P| = p^{2k+1}$ holds.*

Proof. Let P be extraspecial of order p^n. We argue by induction on n. Let $x_1, y_1 \in P$ with $[x_1, y_1] \neq 1$. Then $P' = \langle [x_1, y_1]\rangle \leq \langle x_1, y_1\rangle =: E_1 \trianglelefteq P$. According to Lemma 4.15, $\Phi(E_1) \leq \Phi(P) = P'$. From Burnside's Basis Theorem it follows therefore that $|E_1| = p^3$ and $E_1 \in \{D_8, Q_8\}$ (or $E_1 \in \{M_{p^3}, p_+^{1+2}\}$). In the case $P = E_1$ we are finished. So let $E_1 < P$.

According to Lemma 9.13, $P = E_1Q$ with $Q := \mathrm{C}_P(E_1)$. It holds that $\mathrm{Z}(Q) \leq \mathrm{C}_P(E_1Q) = \mathrm{Z}(P) = \mathrm{Z}(E_1)$. In particular, Q is non-abelian and therefore $1 \neq \Phi(Q) \leq Q' \leq P'$ and $\Phi(Q) = Q' = \mathrm{Z}(Q) = P' \cong C_p$. This shows that Q is extraspecial. By induction, $Q = E_2 * \ldots * E_k$ has the desired form with $\mathrm{Z}(Q) \leq \bigcap_{i=2}^{k} E_i$. Thus $P = E_1 * Q = E_1 * \ldots * E_k$ also holds with $\bigcap_{i=1}^{k} E_i = E_1 \cap Q = \mathrm{Z}(E_1) = \mathrm{Z}(P)$. From Theorem 9.17 it follows

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

Remark 9.21. We now concern ourselves with the uniqueness in Theorem 9.20.

Lemma 9.22. *Let P be non-abelian of order p^3 and $a, b \in P' \setminus \{1\}$. Then there exists an $\alpha \in \mathrm{Aut}(P)$ with $\alpha(a) = b$.*

Proof. In the case $p = 2$, $a = b$ and $\alpha = 1$ satisfies the claim. Therefore let $p > 2$. First let $P = \langle x, y\rangle \cong M_{p^3}$. Then $P' = \langle x^p\rangle$ and there exist $i, j \in \mathbb{Z} \setminus p\mathbb{Z}$ with $a = x^{ip}$ and $b = x^{jp}$. It holds that $(x^i)^{p^2} = 1 = y^p$ and $y(x^i)y^{-1} = x^{i(1+p)} = (x^i)^{1+p}$. Thus the generators x^i and y of P satisfy the same relations as x and y. Analogously, x^j and y also satisfy these relations. According to Theorem 8.10, there is an $\alpha \in \mathrm{Aut}(P)$ with $\alpha(x^i) = x^j$. It follows that $\alpha(a) = \alpha(x^i)^p = x^{jp} = b$.

Now let $P = \langle x, y\rangle \cong p_+^{1+2}$. Then $a = [x, y]^i$ and $b = [x, y]^j$ for $i, j \in \mathbb{Z} \setminus p\mathbb{Z}$. As before, there exists an $\alpha \in \mathrm{Aut}(P)$ with $\alpha(x^i) = x^j$ and $\alpha(y) = y$. According to Exercise 18,

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

Theorem 9.23. *For $k \geq 1$ there are, up to isomorphism, exactly two extraspecial groups of order p^{2k+1}:*

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

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

Proof. Let $P = E_1 * \ldots * E_k$ be extraspecial as in Theorem 9.20. We first show that the isomorphism type of P is uniquely determined by the E_i. So let $Q = F_1 * \ldots * F_k$ with $E_i \cong F_i$ for $i = 1, \ldots, k$. Furthermore, let $\bigcap_{i=1}^k E_i \neq 1 \neq \bigcap_{i=1}^k F_i$ and thus $|P| = |Q|$ according to Theorem 9.17. We choose isomorphisms $\varphi_i \colon E_i \to F_i$. According to Lemma 9.22, we can assume $\varphi_i(z) = \varphi_1(z)$ for $i = 2, \ldots, k$ and $z \in \mathrm{Z}(E_i) = \mathrm{Z}(P)$. Every element in P has the form $x_1 \ldots x_k$ with $x_i \in E_i$ for $i = 1, \ldots, k$. In the case $x_1 \ldots x_k = 1$, it holds that $x_i = (x_1 \ldots x_{i-1} x_{i+1} \ldots x_k)^{-1} \in \mathrm{Z}(E_i)$. Thus

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

Thus the map $\Psi \colon P \to Q$, $x_1 \ldots x_k \mapsto \varphi_1(x_1) \ldots \varphi_k(x_k)$ is well-defined and injective. Because of $|P| = |Q|$, Ψ is also bijective. Obviously, Ψ is also an isomorphism.

We now show $P := M_{p^3} * M_{p^3} \cong M_{p^3} * p_+^{1+2}$ for $p > 2$. Let $P = \langle x, y, a, b \rangle$ with $\langle x, y \rangle \cong \langle a, b \rangle \cong M_{p^3}$ and $[y, x] = x^p = a^p = [b, a]$. We define $P_1 := \langle x, yb \rangle \cong M_{p^3}$ and $P_2 := \langle xa^{-1}, b \rangle$. Because of $(xa^{-1})^p = x^p a^{-p} = 1$, $[xa^{-1}, b]^p = [a^{-1}, b]^p = 1$ and $[xa^{-1}, xa^{-1}, b] = 1 = [b, xa^{-1}, b]$, it follows that $P_2 \cong p_+^{1+2}$. Finally, $[x, xa^{-1}] = 1 = [x, b]$ and

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

and $[xb, b] = 1$. Thus $P = P_1 * P_2 \cong M_{p^3} * p_+^{1+2}$. In the case $p > 2$, there can thus be at most two extraspecial groups of order p^{2k+1}. Because of $\exp(p_+^{1+2k}) = \exp(p_+^{1+2}) = p$ and $\exp(p_-^{1+2k}) = \exp(M_{p^3}) = p^2$, there are exactly two isomorphism classes.

In the following, we can assume $p = 2$. Let $P := D_8 * D_8 = \langle x, y \rangle * \langle a, b \rangle$ with $x^2 = a^2 \neq 1$. Then $P_1 := \langle x, ya \rangle \cong Q_8$ and $P_2 := \langle a, bx \rangle \cong Q_8$. Because of $[ya, bx] = [y, x][a, b] = x^2 a^2 = 1$, it follows that $P \cong P_1 * P_2 \cong Q_8 * Q_8$. Thus, here too, there are at most two extraspecial groups of order 2^{2k+1}. The proof $2_-^{1+2k} \ncong 2_+^{1+2k}$ is more difficult, as both groups have exponent 4. Let

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

We show $f_4(k) = 2^{2k} - 2^k$ by induction on $k \in \mathbb{N}$. For $k = 1$, $2_+^{1+2} = D_8$ and $f_4(1) = 2$. For $k \geq 1$, $2_+^{1+2(k+1)} = 2_+^{1+2k} * D_8 \cong (2_+^{1+2k} \times D_8)/Z$, where $Z := \langle (z, z) \rangle \leq \mathrm{Z}(2_+^{1+2k}) \times \mathrm{Z}(D_8)$ (see proof of Theorem 9.19). Let $(x, y) \in 2_+^{1+2k} \times D_8$ be of order 4. Then x or y has order 4. If x and y have order 4, then $x^4 = y^4 = z$ and the coset $(x, y)Z$ has order 2. Therefore,

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

Now let $g_2(k) := |\{x \in 2_-^{1+2k} : x^2 = 1\}|$ and $g_4(k) = 2^{2k+1} - g_2(k)$. Then $g_2(1) = 2 = f_4(1)$ and $g_4(1) = 6 = f_2(1)$. Because of $2_+^{1+2(k+1)} = 2_+^{1+2k} * Q_8$, it follows that

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

for $k \geq 0$. In particular, $f_4(k) \neq g_4(k)$. □

Definition 9.24. A subgroup $H \leq G$ is called *subnormal*, if a sequence $H = H_0 \trianglelefteq H_1 \trianglelefteq \ldots \trianglelefteq H_k = G$ exists. We write $H \trianglelefteq\trianglelefteq G$. Subnormality is thus the transitive closure of the normal subgroup relation.

Example 9.25. Every subgroup of a nilpotent group is subnormal according to Theorem 4.10.

Remark 9.26. For $H \trianglelefteq\trianglelefteq G$, the sequence $H \trianglelefteq \mathrm{N}_G(H) \trianglelefteq \mathrm{N}_G(\mathrm{N}_G(H)) \trianglelefteq \ldots$ does not necessarily have to end at G. For example, $\langle (1,2)(3,4)\rangle \trianglelefteq \langle (1,3,2,4),(1,2)\rangle =: P \in \mathrm{Syl}_2(S_4)$, but $P = \mathrm{N}_{S_4}(P)$. On the other hand, $\langle (1,2)(3,4)\rangle \trianglelefteq V_4 \trianglelefteq S_4$.

Lemma 9.27. *Let $H \trianglelefteq\trianglelefteq G$ and M be a minimal normal subgroup of G. Then $M \leq \mathrm{N}_G(H)$ holds.*

Proof. Wlog. let $H < G$ and $H \trianglelefteq\trianglelefteq N \lhd G$. The minimality of M shows $N \cap M \in \{1, M\}$. In the case $N \cap M = 1$, it holds that $M \leq \mathrm{C}_G(N) \leq \mathrm{C}_G(H) \leq \mathrm{N}_G(H)$. So let $M \leq N$. Let $K \leq M$ be a minimal normal subgroup of N. By induction on $|G|$, we can assume $K \leq \mathrm{N}_N(H)$. For $g \in G$, gKg^{-1} is also a minimal normal subgroup of N. This shows

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

Theorem 9.28 (Wielandt)**.** *For $H, K \trianglelefteq\trianglelefteq G$, it holds that $\langle H, K\rangle \trianglelefteq\trianglelefteq G$.*

Proof. Let M be a minimal normal subgroup of G and $\overline{G} := G/M$. Obviously $\overline{H}, \overline{K} \trianglelefteq\trianglelefteq \overline{G}$. By induction on $|G|$, we can assume $\langle \overline{H}, \overline{K}\rangle \trianglelefteq\trianglelefteq \overline{G}$. This shows $\langle H, K\rangle M \trianglelefteq\trianglelefteq G$. According to Lemma 9.27, $\langle H, K\rangle \trianglelefteq \langle H, K\rangle M$ holds and the assertion follows. $\square$

Lemma 9.29. *Let $H \leq G$ be not subnormal in G. For all $H \leq K < G$, let $H \trianglelefteq\trianglelefteq K$ hold. Then H is contained in exactly one maximal subgroup of G.*

Proof. Induction on $|G : H|$. By assumption, there exists a maximal subgroup $M < G$ with $\mathrm{N}_G(H) \leq M$. Let $K < G$ also be maximal with $H \leq K$. By assumption, $H \trianglelefteq\trianglelefteq K$. If even $H \trianglelefteq K$ holds, then $K \leq \mathrm{N}_G(H) \leq M$ and $K = M$ as desired. So let $H \not\trianglelefteq K$. Let $H = H_0 \trianglelefteq \ldots \trianglelefteq H_s = K$ with $s \geq 2$ minimal. Then there exists $g \in H_2$ with $gHg^{-1} \neq H$. Now let $\tilde{H} := \langle H, gHg^{-1}\rangle \leq K$ and $gHg^{-1} \leq gH_1g^{-1} = H_1 \leq \mathrm{N}_G(H)$. This shows $\tilde{H} \leq \mathrm{N}_G(H) \leq M$ and $H \trianglelefteq \tilde{H} < G$.

Let $\tilde{H} \leq L < G$. Then $H \trianglelefteq\trianglelefteq L$ and by symmetry also $gHg^{-1} \trianglelefteq\trianglelefteq L$. From Theorem 9.28 it follows that $\tilde{H} \trianglelefteq\trianglelefteq L$. Since H is not subnormal in G, $\tilde{H}$ cannot be subnormal in G either. Thus $\tilde{H}$ also satisfies the assumption. By induction, M is the only maximal subgroup containing $\tilde{H}$. Because of $\tilde{H} \leq K$, $M = K$ must hold. $\square$

Theorem 9.30 (Baer-Suzuki)**.** *For $H \leq G$, it holds that $H \leq \mathrm{F}(G)$ if and only if $\langle H, gHg^{-1}\rangle$ is nilpotent for all $g \in G$.*

Proof. If $H \leq \mathrm{F}(G) \trianglelefteq G$, then $\langle H, gHg^{-1}\rangle \leq \mathrm{F}(G)$ is nilpotent. Conversely, assume that $\langle H, gHg^{-1}\rangle$ is nilpotent for all $g \in G$. Then H is nilpotent and it suffices to show $H \trianglelefteq\trianglelefteq G$ (Exercise 72). Assume the contrary. Let $H \leq K < G$. By induction on $|G|$, we have $H \trianglelefteq\trianglelefteq K$. According to Lemma 9.29, H lies in exactly one maximal subgroup $M < G$. For $g \in G$, we have $H \leq \langle H, gHg^{-1}\rangle < G$ (otherwise $\mathrm{F}(G) = G$ would hold) and therefore $\langle H, gHg^{-1}\rangle \leq M$. It follows that $H^G \leq M$ and $H \trianglelefteq\trianglelefteq H^G \trianglelefteq G$. Contradiction. $\square$

Corollary 9.31. *Let $x \in G$ and let $\langle x, gxg^{-1}\rangle$ be a p-group for all $g \in G$. Then $x \in \mathrm{O}_p(G)$.*

Proof. For $H := \langle x \rangle$, it holds that $\langle H, gHg^{-1} \rangle = \langle x, gxg^{-1} \rangle$. Baer-Suzuki therefore shows $H \leq \mathrm{F}(G)$. As a p-group, H lies in the unique Sylow p-subgroup $\mathrm{O}_p(G)$ of $\mathrm{F}(G)$ (Theorem 4.11). □

Corollary 9.32. *Let $x \in G \setminus \mathrm{O}_2(G)$ be an involution. Then there exists an element $y \in G \setminus \{1\}$ of odd order with $xyx^{-1} = y^{-1}$.*

Proof. According to Corollary 9.31, there exists $g \in G$ such that $D := \langle x, gxg^{-1} \rangle$ is not a 2-group. Since gxg^{-1} is also an involution, D is a dihedral group according to Exercise 32. In particular, the order of $y := xgxg^{-1}$ is not a power of 2. Furthermore, $xyx^{-1} = gxg^{-1}x^{-1} = y^{-1}$ holds. By replacing y with a power, we can achieve that $|\langle y \rangle| > 1$ is odd. □

Example 9.33. Corollary 9.31 has been generalized in many directions (without proof):

- (Revin) Let π be a set of odd prime numbers. Let $x \in G$ and let $\langle x, gxg^{-1} \rangle$ be a π-group for all $g \in G$. Then $x \in \mathrm{O}_\pi(G)$.
- (Guralnick, Tong-Viet, Tracey) Let $x \in G$ be a p-element and $[x, g]$ a p-element for all p'-elements $g \in G$. Then $x \in \mathrm{O}_p(G)$.
- (Guest) Let $x \in G$ be an element of prime order $p \geq 5$. If $\langle x, gxg^{-1} \rangle$ is solvable for all $g \in G$, then $\langle gxg^{-1} : g \in G \rangle$ is solvable.
- (Thompson) G is solvable if and only if $\langle x, y \rangle$ is solvable for all $x, y \in G$.

Remark 9.34. For induction proofs, we often use minimal normal subgroups N due to their simple structure (Theorem 2.27). However, one has no control over G/N. For solvable groups, $F(G)$ is a good substitute for N according to Remark 3.20. We now construct a generalization of the Fitting group for non-solvable groups with similarly good properties.

Definition 9.35.

(i) $G \neq 1$ is called *quasisimple*, if $G' = G$ (perfect) and $G/\mathrm{Z}(G)$ is simple.

(ii) A *component* of G is a subnormal quasisimple subgroup of G.

Example 9.36. Every non-abelian simple group is quasisimple.

Lemma 9.37. *Let K be a component of G. Then:*

(i) If $K \leq H \leq G$, then K is a component of H.

(ii) If $N \lhd K$, then $N \leq \mathrm{Z}(K)$.

(iii) If $K \not\subseteq N \trianglelefteq G$, then KN/N is a component of G/N.

Proof.

(i) By definition, there exists a subnormal series $K = K_0 \trianglelefteq \ldots \trianglelefteq K_n = G$. Then $K = K_0 \cap H \trianglelefteq \ldots \trianglelefteq K_n \cap H = H$. This shows (i).

(ii) We have $N\mathrm{Z}(K)/\mathrm{Z}(K) \trianglelefteq K/\mathrm{Z}(K)$. Since $K/\mathrm{Z}(K)$ is simple, it follows that $N \leq \mathrm{Z}(K)$ or $K = N\mathrm{Z}(K)$. In the second case, $K = K' = (N\mathrm{Z}(K))' = N' \leq N$.

(iii) Here $N \cap K \lhd K$ and $N \cap K \leq \mathrm{Z}(K)$ by (ii). This shows $(K/K \cap N)/(\mathrm{Z}(K)/K \cap N) \cong K/\mathrm{Z}(K)$. Because

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

it follows that $\mathrm{Z}(K/K \cap N) = \mathrm{Z}(K)/K \cap N$, since $K/\mathrm{Z}(K)$ is simple. In particular, $(K/K \cap N)/\mathrm{Z}(K/K \cap N)$ is simple. Furthermore, $(KN/N)' = K'N/N = KN/N$. Thus $KN/N \cong K/K \cap N$ is quasisimple. Finally, $KN/N = K_0N/N \trianglelefteq \ldots \trianglelefteq K_nN/N = G/N$. □

Lemma 9.38. *Let K be a component of G and $H \trianglelefteq\trianglelefteq G$. Then $K \leq H$ or $[K, H] = 1$.*

Proof. We can assume $H < G$. Let $H \leq N \lhd G$. In the case $G = K$, one obtains $H \leq N \leq \mathrm{Z}(G)$ from Lemma 9.37. Then $[K, H] = 1$. We can therefore assume $K < G$. Let $K \leq M \lhd G$. Then $H_1 := [H, K] \leq [N, M] \leq N \cap M$ and $K \leq \mathrm{N}_M(H_1) =: G_1 \leq M < G$ by Lemma 3.3. By Lemma 9.37, K is a component of G_1 and $H_1 \trianglelefteq G_1$. By induction on $|G|$, we can assume $[K, H_1] = 1$ or $K \leq H_1$. In the first case, $1 = [K, H, K] = [K, K, H]$. From Lemma 3.6 it follows that $[H, K] = [H, K'] = [H, K, K] = 1$. Now let $K \leq H_1 \leq N$. Then K is a component of N and $H \trianglelefteq\trianglelefteq N$. By induction, the claim holds for N and we are done. □

Theorem 9.39. *Let $K_1, \ldots, K_n$ be the components of G. Then*

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

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

Proof. For $i \neq j$ we have $[K_i, K_j] = 1$, because otherwise $K_i \leq K_j \leq K_i$ by Lemma 9.38. This shows $\mathrm{E}(G) = K_1 * \ldots * K_n$. Since $\mathrm{F}(G)$ is nilpotent, $\mathrm{F}(G)$ cannot contain any component of G. Lemma 9.38 thus yields $[\mathrm{F}(G), K_i] = 1$ and $[\mathrm{F}(G), \mathrm{E}(G)] = 1$. □

Definition 9.40. One calls

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

the *generalized Fitting group* of G.

Example 9.41. For $n \geq 5$ we have $\mathrm{F}^*(S_n) = \mathrm{E}(S_n) = A_n$, because A_n is a component of S_n.

Remark 9.42. The next theorem generalizes Theorem 3.19.

Theorem 9.43. *It holds that* $\mathrm{C}_G(\mathrm{F}^*(G)) \leq \mathrm{F}^*(G)$.

Proof. Let $G \neq 1$. We first show $\mathrm{F}^*(G) \neq 1$. For this, let N be a minimal normal subgroup of G. If N is abelian, then $1 \neq N \leq \mathrm{F}(G) \leq \mathrm{F}^*(G)$. Otherwise $N = T_1 \oplus \ldots \oplus T_n$ with non-abelian simple groups $T_1, \ldots, T_n$ by Theorem 2.27. Because of $T_i \trianglelefteq N \trianglelefteq G$, the T_i are components and it follows $1 \neq N \leq \mathrm{E}(G) \leq \mathrm{F}^*(G)$.

Now let $C := \mathrm{C}_G(\mathrm{F}^*(G)) \trianglelefteq G$. It suffices to show that C is abelian, because then one has $C \leq \mathrm{F}(G) \leq \mathrm{F}^*(G)$. According to what was just shown, it is sufficient to prove $\mathrm{F}^*(C/\mathrm{Z}(C)) = 1$. Let $\mathrm{F}(C/\mathrm{Z}(C)) = N/\mathrm{Z}(C)$. Because of $\mathrm{Z}(C) \leq \mathrm{Z}(N)$, $N \trianglelefteq C$ is then nilpotent and therefore $N \leq \mathrm{F}(C)$. Now $\mathrm{F}(C)$ is characteristic in $C \trianglelefteq G$ and therefore $\mathrm{F}(C) \trianglelefteq G$. This shows $N \leq \mathrm{F}(G) \cap C \leq \mathrm{Z}(C)$. Thus $\mathrm{F}(C/\mathrm{Z}(C)) = 1$.

Finally, let $K/\mathrm{Z}(C)$ be a component of $C/\mathrm{Z}(C)$. Then

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

and $K = K''\mathrm{Z}(C)$. In particular, $K/K'' \cong \mathrm{Z}(C)/\mathrm{Z}(C) \cap K''$ is abelian and $K' = K''$. From $K \trianglelefteq\trianglelefteq C$ it follows $K' \trianglelefteq\trianglelefteq C$. To show that $K'/\mathrm{Z}(K')$ is simple, we assume $\mathrm{Z}(K') < N \trianglelefteq K'$. Then $N\mathrm{Z}(C)/\mathrm{Z}(C) \trianglelefteq\trianglelefteq C/\mathrm{Z}(C)$ and Lemma 9.38 shows $K \leq N\mathrm{Z}(C)$ or $[K, N] \leq \mathrm{Z}(C)$. In the first case $K' \leq (N\mathrm{Z}(C))' \leq N' \leq N \leq K'$. In the second case $[K, K, N] = [K, N, K] = 1$ and Lemma 3.6 yields the contradiction $[N, K'] = [N, K, K] = 1$. Thus $K'/\mathrm{Z}(K')$ is simple and K' is a component of $C \trianglelefteq G$. Then K' is also a component of G and we obtain the contradiction $K' \leq \mathrm{F}^*(G) \cap C \leq \mathrm{Z}(C)$. Consequently $C/\mathrm{Z}(C)$ has no components and $\mathrm{F}^*(C/\mathrm{Z}(C)) = 1$. □

Example 9.44. Let $\mathrm{F}^*(G) = \mathrm{E}(G) = K$ be quasisimple. According to Theorem 9.43,

$$G/K \cong (G/\mathrm{C}_G(K))/(K/\mathrm{Z}(K)) \leq \mathrm{Out}(K) \overset{\text{Exercise 73}}{\leq} \mathrm{Out}(K/\mathrm{Z}(K)).$$

A conjecture of Schreier (which so far could only be proven using the classification of finite simple groups) states that $\mathrm{Out}(S)$ is solvable for every simple group S. Therefore, $K/\mathrm{Z}(K)$ is the only non-abelian composition factor of G. A theorem of Hölder states

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

10 The Simplicity of $\mathrm{PSL}(n, q)$

Remark 10.1.

(i) In the following, let $n \in \mathbb{N}$ and $q \neq 1$ be a prime power. Let $\mathbb{F}_q$ be the field with q elements (Algebra) and $\mathrm{GL}(n, q) := \mathrm{GL}(n, \mathbb{F}_q)$ as well as $\mathrm{SL}(n, q) := \mathrm{SL}(n, \mathbb{F}_q)$.

(ii) For $i, j \in \{1, \ldots, n\}$, let $e_{ij} = (\delta_{ir}\delta_{js})_{r,s=1}^n \in \mathbb{F}_q^{n\times n}$. Then $e_{ij}e_{kl} = \delta_{jk}e_{il}$ holds.

Lemma 10.2. *It holds that* $\mathrm{Z}(\mathrm{GL}(n, q)) = \mathbb{F}_q^\times 1_n$ *and* $\mathrm{Z}(\mathrm{SL}(n, q)) = \mathrm{Z}(\mathrm{GL}(n, q)) \cap \mathrm{SL}(n, q)$.

Proof. Clearly, $\mathbb{F}_q^\times 1_n \subseteq \mathrm{Z}(\mathrm{GL}(n, q))$. For both statements, it therefore suffices to show $\mathrm{C}_{\mathrm{GL}(n,q)}(\mathrm{SL}(n, q)) \subseteq \mathbb{F}_q^\times 1_n$. Let $A = (a_{ij}) \in \mathrm{C}_{\mathrm{GL}(n,q)}(\mathrm{SL}(n, q))$ and $i, j \in \{1, \ldots, n\}$ with $i \neq j$. Then $1_n + e_{ij} \in \mathrm{SL}(n, q)$ and $A(1_n + e_{ij}) = (1_n + e_{ij})A$. It follows

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

This shows $a_{ij} = 0$ for $i \neq j$ and $a_{ii} = a_{jj}$. □

Definition 10.3. One calls

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

the *projective* (*special*) *linear group* of degree n over $\mathbb{F}_q$.

Theorem 10.4.

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

Proof. Let $A \in \mathrm{GL}(n,q)$. Then the first row of A is not the zero vector. There are therefore q^n-1 possibilities for the first row. The second row must not be linearly dependent on the first row. This gives q^n-q possibilities for the second row. The third row does not lie in the span of the first two rows. There are thus q^n-q^2 possibilities for the third row etc. Conversely, every such choice yields a matrix with linearly independent rows, hence an invertible matrix. This shows

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

and the first claim follows from Lemma 10.2.

For the second claim, we observe that the homomorphism $\det\colon \mathrm{GL}(n,q) \to \mathbb{F}_q^\times$ is surjective. Therefore $|\mathrm{SL}(n,q)| = \frac{|\mathrm{GL}(n,q)|}{q-1} = |\mathrm{PGL}(n,q)|$. Now let $\lambda 1_n \in \mathbb{F}_q^\times 1_n \cap \mathrm{SL}(n,q) = \mathrm{Z}(\mathrm{SL}(n,q))$. Then $1 = \det(\lambda 1_n) = \lambda^n$ and $|\langle\lambda\rangle| \mid \gcd(n,q-1)$. Since $\mathbb{F}_q^\times$ is cyclic (Algebra or Theorem 9.8), there is exactly one subgroup $L \leq \mathbb{F}_q^\times$ with $|L| = \gcd(n,q-1)$ (Theorem 2.4). It then holds that $\lambda \in L$. Conversely, every element $\gamma \in L$ satisfies the condition $\gamma^n = 1$. Thus $|\mathrm{Z}(\mathrm{SL}(n,q))| = |L| = \gcd(n,q-1)$. □

Example 10.5.

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

(ii) If q is a power of 2, then $\mathrm{PSL}(2,q) \cong \mathrm{SL}(2,q)$. For $q=2$ it also holds that $\mathrm{GL}(n,2) = \mathrm{SL}(n,2) \cong \mathrm{PSL}(n,2) \cong \mathrm{PGL}(n,2)$. In particular, $\mathrm{PSL}(2,2) \cong \mathrm{SL}(2,2) \cong \mathrm{GL}(2,2) \cong S_3$.

Lemma 10.6 (Iwasawa)**.** *Let $G \leq \mathrm{Sym}(\Omega)$ be primitive and perfect. If there exists a solvable normal subgroup $A \trianglelefteq G_\omega$ ($\omega \in \Omega$) with $\langle gAg^{-1} : g \in G\rangle = G$, then G is simple.*

Proof. Let $1 \neq N \trianglelefteq G$. According to Lemma 6.20 and Theorem 1.24, $G = G_\omega N \leq \mathrm{N}_G(NA)$, i. e. $NA \trianglelefteq G$. By assumption $G = \langle gAg^{-1} : g \in G\rangle \leq NA$ and $G/N \cong A/A\cap N$ is solvable. In the case $N < G$ one obtains the contradiction $G/N = G'/N = (G/N)' < G/N$. Thus $N = G$ and G is simple. □

Lemma 10.7. *For $n \geq 2$, $\mathrm{PSL}(n,q)$ acts faithfully and primitively on the set Ω of 1-dimensional subspaces of $\mathbb{F}_q^n$.*

Proof. Obviously $\mathrm{SL}(n,q)$ acts on Ω. Let $A \in \mathrm{SL}(n,q)$ be in the kernel of this action. For the i-th unit vector $e_i = (0,\ldots,0,1,0,\ldots,0)$ there then exists a $\lambda_i \in \mathbb{F}_q$ with $Ae_i = \lambda_i e_i$. Thus A is a diagonal matrix with diagonal $(\lambda_1,\ldots,\lambda_n)$. Because of $\lambda_1 e_1 + \lambda_i e_i = A(e_1+e_i) \in \mathbb{F}_q(e_1+e_i)$ for $i > 1$, it even holds that $\lambda_1 = \ldots = \lambda_n$. Conversely, every matrix in $\mathrm{Z}(\mathrm{SL}(n,q))$ acts trivially on Ω. We have thus shown that $\mathrm{PSL}(n,q)$ acts faithfully on Ω.

For primitivity, it suffices by Theorem 6.35 to show that $\mathrm{PSL}(n,q)$ acts 2-transitively on Ω. So let $\langle v_1\rangle \neq \langle v_2\rangle$ and $\langle w_1\rangle \neq \langle w_2\rangle$ in Ω. One can extend v_1, v_2 (resp. w_1, w_2) to a basis $v_1,\ldots,v_n$ (resp. $w_1,\ldots,w_n$) of $\mathbb{F}_q^n$. Then there exists $A \in \mathrm{GL}(n,q)$ with $Av_i = w_i$ for $i = 1,\ldots,n$. Let $\lambda := \det(A)$ and $B \in \mathrm{GL}(n,q)$ with $Bv_1 = \lambda^{-1}w_1$ and $Bv_i = w_i$ for $i = 2,\ldots,n$. Then $B \in \mathrm{SL}(n,q)$ and the corresponding element $\overline{B} \in \mathrm{PSL}(n,q)$ maps $(\langle v_1\rangle, \langle v_2\rangle)$ to $(\langle w_1\rangle, \langle w_2\rangle)$. □

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

Proof. In the case $n = 1$, $\mathrm{SL}(n,q) = 1$ and the claim is clear. So let $n \geq 2$. It is clear that the matrices $1_n + \lambda e_{ij}$ have determinant 1. Conversely, let $A \in \mathrm{SL}(n,q)$ be arbitrary. By the multiplication $A(1_n + \lambda e_{ij})$, the λ-fold of the i-th column of A is added to the j-th column. Analogously, the multiplication $(1_n + \lambda e_{ij})A$ effects the addition of the λ-fold of the j-th row to the i-th row. These are the elementary operations in the Gaussian algorithm. Because of $\det(A) = 1$, there exists an $i \in \{1,\ldots,n\}$ with $a_{1i} \neq 0$. After a column operation, we may assume $i > 1$. If one replaces A by $A(1_n + (1-a_{11})a_{1i}^{-1}e_{i1})$, then $a_{11} = 1$. After further column operations, we may assume $a_{1j} = 0$ for $j > 1$. Analogously, one obtains $a_{j1} = 0$ for $j > 1$ by row operations. In the case $n = 2$, then already $A = 1_2$ because of $\det(A) = 1$. So let $n \geq 3$ and $A' := (a_{ij})_{i,j=2}^n$. Then $A' \in \mathrm{SL}(n-1,q)$ holds. By induction on n, one can thus transform A' into the identity matrix using row and column operations. These operations also work for A and do not change the first row and column. Overall, one thus has matrices $P, Q \in \langle 1_n + \lambda e_{ij} : \lambda \in \mathbb{F}_q,\ i \neq j\rangle$ with $PAQ = 1_n$. The claim follows. □

Lemma 10.9. *For $n \geq 2$ and $(n,q) \notin \{(2,2),(2,3)\}$, $\mathrm{SL}(n,q)$ is perfect.*

Proof. According to Lemma 10.8, it suffices to show that the matrices $1_n + \lambda e_{ij}$ are commutators. It holds that $(1_n + \lambda e_{ij})(1_n - \lambda e_{ij}) = 1_n + \lambda e_{ij} - \lambda e_{ij} - \lambda^2 e_{ij}^2 = 1_n$ and $(1_n + \lambda e_{ij})^{-1} = 1_n - \lambda e_{ij}$. Let first $n \geq 3$, $\lambda \in \mathbb{F}_q$ and $i,j,k \in \{1,\ldots,n\}$ be pairwise distinct. Then

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

Now let $n = 2$ and $q > 3$. Let $\alpha, \beta \in \mathbb{F}_q^\times$ and

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

Then

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

Because of $q > 3$, we can choose α such that $\alpha^2 \neq 1$ holds. With $\beta := \lambda(\alpha^2-1)^{-1}$, then $[A,B] = 1_2 + \lambda e_{12}$ and $[(B^{-1})^{\mathrm{t}}, (A^{-1})^{\mathrm{t}}] = [A,B]^{\mathrm{t}} = 1_2 + \lambda e_{21}$. This shows the claim. □

Example 10.10. Because of $|\mathrm{SL}(2,2)| = 6$ and $|\mathrm{SL}(2,3)| = 24$, $\mathrm{SL}(2,2)$ and $\mathrm{SL}(2,3)$ are not perfect.

Theorem 10.11 (Jordan-Moore-Dickson)**.** *For $n \geq 2$ and $(n,q) \notin \{(2,2),(2,3)\}$, $\mathrm{PSL}(n,q)$ is simple.*

Proof. We use Iwasawa's Lemma. Let $G := \mathrm{SL}(n,q)$, $Z := \mathrm{Z}(G)$ and $\overline{H} := HZ/Z$ for $H \leq G$. According to Lemma 10.7, $\overline{G}$ is a primitive permutation group. According to Lemma 10.9, $\overline{G}' = \overline{G'} = \overline{G}$, i. e. $\overline{G}$ is perfect. Let $e_i := (\delta_{ij})_{j=1}^n \in \mathbb{F}_q^n$ and let $H \leq G$ be the stabilizer of $U := \langle e_1 \rangle$. Let

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

Because of

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

A is an abelian subgroup of H. For $h \in H$ and $v, w \in \mathbb{F}_q^n$ with $v + U = w + U$, it holds that $h(v - w) \in hU = U$ and therefore $hv + U = hw + U$. Thus H acts on $\mathbb{F}_q^n/U$. Let $h = (h_{ij}) \in H$ be in the kernel of this action. Then $he_i \in e_i + U$ for $i = 2, \ldots, n$. This shows $h_{ij} = \delta_{ij}$ for $i \geq 2$. Because of $\det h = 1$, it also holds that $h_{11} = 1$ and thus $h \in A$. Conversely, every element from A acts trivially on $\mathbb{F}_q^n/U$. Thus A is the kernel and therefore $A \trianglelefteq H$. Certainly then $\overline{A}$ is also an abelian normal subgroup of $\overline{H}$. It remains to show that $\overline{G} = \langle \overline{gAg^{-1}} : g \in G \rangle$ holds. According to Lemma 10.8, it suffices to show $1_n + \lambda e_{ij} \in \bigcup_{g \in G} gAg^{-1}$ ($\lambda \in \mathbb{F}_q$, $i \neq j$). By definition, $1_n + \lambda e_{1j} \in A$ already holds. For $j \neq i \geq 2$, let $g_i \in G$ with

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

Then $(g_i e_{1j} g_i^{-1}) e_j = e_i$ and $(g_i e_{1j} g_i^{-1}) e_k = 0$ for $k \neq j$. This shows $g_i(1_n + \lambda e_{1j}) g_i^{-1} = 1_n + \lambda g_i e_{1j} g_i^{-1} = 1_n + \lambda e_{ij}$. The claim follows. □

Remark 10.12.

(i) According to Theorem 10.4, $|\mathrm{PSL}(2,4)| = |\mathrm{PSL}(2,5)| = 60$. From Theorem 6.40 it therefore follows that $\mathrm{PSL}(2,4) \cong \mathrm{PSL}(2,5) \cong A_5$. One can further show $\mathrm{PSL}(2,7) \cong \mathrm{PSL}(3,2) \cong \mathrm{GL}(3,2)$, $\mathrm{PSL}(2,9) \cong A_6$ and $\mathrm{PSL}(4,2) \cong \mathrm{GL}(4,2) \cong A_8$.

(ii) The smallest simple group that is not isomorphic to C_p, A_n or $\mathrm{PSL}(n,q)$ is the *special unitary* group $\mathrm{SU}(3,3)$ of order 6048. For $A = (a_{ij}) \in \mathrm{GL}(n,q^2)$ one defines $\overline{A} := (a_{ij}^q)$ (Frobenius automorphism) and

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

It holds that $\mathrm{PSU}(2,q) \cong \mathrm{PSL}(2,q)$. For $n \geq 3$ and $(n,q) \neq (3,2)$, $\mathrm{PSU}(n,q)$ is simple.[19]

[19] See notes on combinatorial group theory

(iii) Let $G := \mathrm{GL}(n,q)$ with $n \geq 2$ and $(n,q) \notin \{(2,2),(2,3)\}$. Since $\mathrm{SL}(n,q)$ is quasisimple, $\mathrm{SL}(n,q) \leq \mathrm{E}(G)$ holds. Because $\mathrm{C}_G(\mathrm{SL}(n,q)) \leq \mathrm{Z}(G)$ (proof of Lemma 10.2), there can be no further components according to Theorem 9.39, i. e. $\mathrm{E}(G) = \mathrm{SL}(n,q)$. From Theorem 9.39 it also follows that $\mathrm{Z}(G) \leq \mathrm{F}(G) \leq \mathrm{C}_G(\mathrm{E}(G)) \leq \mathrm{Z}(G)$, thus $\mathrm{F}(G) = \mathrm{Z}(G) = \mathbb{F}_q^\times 1_n$ and $\mathrm{F}^*(G) = \mathbb{F}_q^\times \mathrm{SL}(n,q)$. In this case,

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

Theorem 10.13. *Let P be a Sylow p-subgroup of $\mathrm{SL}(2,q)$. Then:*

(i) For $p \mid q$, P is elementary abelian of order q.

(ii) For $p = 2 \nmid q$, P is a (generalized) quaternion group.

(iii) For $2 < p \nmid q$, P is cyclic.

Proof. Let $G := \mathrm{SL}(2,q)$. As is well known, $|G| = (q+1)q(q-1)$. For $p \mid q$, $P = \{1_2 + \lambda e_{12} : \lambda \in \mathbb{F}_q\}$ is obviously an elementary abelian Sylow p-subgroup of G. Now let $p = 2 \nmid q$ and let $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in P$ be an involution. Then $A = A^{-1} = \left(\begin{smallmatrix} d & -b \\ -c & a \end{smallmatrix}\right)$ (note $\det(A) = 1$) and it follows that $A = -1_2$ (note $1 \neq -1$ in $\mathbb{F}_q$). Thus P possesses only one involution. According to Theorem 9.6, P is cyclic or a quaternion group. In the first case, G is 2-nilpotent according to Theorem 7.22. From Lemma 10.9 it follows that $q = 3$. The action on the four 1-dimensional subspaces yields a homomorphism $G \to S_4$ with image A_4. Since A_4 is not 2-nilpotent, this is excluded. Thus P is a quaternion group.

Finally, let $2 < p \nmid q$. Because of $\gcd(q+1, q-1) \leq 2$, $|P|$ is a divisor of $q+1$ or a divisor of $q-1$. Let $\mathbb{F}_q^\times = \langle \zeta \rangle$ (Algebra or Theorem 9.8). Then $\left(\begin{smallmatrix} \zeta & 0 \\ 0 & \zeta^{-1} \end{smallmatrix}\right)$ generates a cyclic subgroup of order $q-1$ in G. If $|P|$ is a divisor of $q-1$, then P is thus cyclic. In Example 6.23 we constructed a cyclic group $S \leq \mathrm{GL}(2,q)$ of order $q^2 - 1$ (Singer cycle). Because of

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

$|S \cap \mathrm{SL}(2,q)|$ is divisible by $q+1$. Thus P is also cyclic in the case $|P| \mid q+1$. □

Remark 10.14. Because of $\mathrm{PSL}(2,q) = \mathrm{SL}(2,q)/\langle \pm 1_2 \rangle$, one also obtains the Sylow p-subgroups of $\mathrm{PSL}(2,q)$ from Theorem 10.13. If q is odd, then a 2-Sylow subgroup of $\mathrm{PSL}(2,q)$ is a dihedral group, since $Q_{2^n}/\mathrm{Z}(Q_{2^n}) \cong D_{2^{n-1}}$, where $D_4 := C_2^2$. Gorenstein and Walter have conversely shown that A_7 and $\mathrm{PSL}(2,q)$ with q odd are the only simple groups with a dihedral group (or C_2^2) as a 2-Sylow subgroup (note $A_6 \cong \mathrm{PSL}(2,9)$). Brauer and Suzuki have shown that no simple group possesses a quaternion group as a Sylow subgroup.

11 Schur Extensions

Remark 11.1. According to Theorem 9.43, the structure of G is influenced by $\mathrm{F}^*(G)$. The structure of the nilpotent group $\mathrm{F}(G)$ follows from Theorem 4.10, while $\mathrm{E}(G)$ is a central product of quasisimple components K. According to the classification of simple groups, the possibilities for $K/\mathrm{Z}(K)$ are known. We will see how the possibilities for K can be derived from this.

Example 11.2. Let G be a group with 2-Sylow subgroup $P = \langle x, y\rangle \cong D_{2^n}$. Assume first $Z := \mathrm{Z}(G) \cap P \neq 1$. Because of $|\mathrm{Z}(P)| = 2$, it follows $Z = \mathrm{Z}(P)$. We show $\mathrm{Foc}_G(P) \leq \langle x\rangle$. For this, let $g \in G$, $h, ghg^{-1} \in P$. In the case $h^2 \neq 1$, we have $h, ghg^{-1} \in \langle x\rangle$, because $P \setminus \langle x\rangle$ consists of involutions. Then $[g, h] \in \langle x\rangle$. Now assume $h^2 = 1$. In the case $h \in \langle x\rangle$, we have $h \in Z$ and $ghg^{-1} \in Z$ follows from $Z \trianglelefteq G$. Again, $[g, h] \in \langle x\rangle$. In the last case $h, ghg^{-1} \in P \setminus \langle x\rangle$, it also holds that $[g, h] \in \langle x\rangle$. Thus $\mathrm{Foc}_G(P) \leq \langle x\rangle$. According to Higman, G' has the cyclic 2-Sylow subgroup $\mathrm{Foc}_G(P) = P \cap G'$. According to Theorem 7.22, G' is 2-nilpotent. According to Feit-Thompson, G' and G are solvable.

Now let $Z = 1$ and $\mathrm{E}(G) = K_1 * \ldots * K_n$ with components $K_1, \ldots, K_n$. Let $P_i \in \mathrm{Syl}_2(K_i)$. By Sylow, P_i is isomorphic to a subgroup of P. According to Feit-Thompson and Theorem 7.22, P_i cannot be cyclic. Thus $P_i \cap \langle x\rangle$ has index 2 in P_i. It follows easily that P_i itself is a dihedral group or $P_i \cong C_2^2$. As above, $|\mathrm{Z}(K_i)|$ is now odd. According to Theorem 9.17, $P_1 \times \ldots \times P_n \in \mathrm{Syl}_2(\mathrm{E}(G))$ is isomorphic to a subgroup of P. On the other hand, every subgroup $Q \leq P$ can be generated by two elements, because $|Q : Q \cap \langle x\rangle| = |\langle x\rangle Q : \langle x\rangle| \leq 2$. This shows $n = 1$ and $\mathrm{E}(G) = K$ is quasisimple. Because of $P_1 \cong P_1\mathrm{Z}(K)/\mathrm{Z}(K) \in \mathrm{Syl}_2(K/\mathrm{Z}(K))$, we have $K/\mathrm{Z}(K) \cong A_7$ or $K/\mathrm{Z}(K) \cong \mathrm{PSL}(2, q)$ (Remark 10.14). We will show that $\mathrm{Z}(K) = 1$ or $K/\mathrm{Z}(K) \in \{A_6, A_7\}$ and $\mathrm{Z}(K) \cong C_3$ holds (Example 11.38).

Definition 11.3. A *Schur extension* of a finite group G is a group $\widehat{G}$ such that there exists a $Z \leq \mathrm{Z}(\widehat{G}) \cap \widehat{G}'$ with $\widehat{G}/Z \cong G$.

Example 11.4.

(i) Every extraspecial group is a Schur extension of an elementary abelian group. In particular, D_8 and Q_8 are Schur extensions of C_2^2.

(ii) Every quasisimple group G is a Schur extension of the simple group $G/\mathrm{Z}(G)$. In particular, $\mathrm{SL}(2, 5)$ is a Schur extension of A_5 (Remark 10.12).

(iii) Let $\widehat{G}$ be a Schur extension of a cyclic group $G \cong \widehat{G}/Z$. According to Exercise 10(a), $\widehat{G}$ is abelian, because $\widehat{G}/\mathrm{Z}(\widehat{G}) \cong (\widehat{G}/Z)/(\mathrm{Z}(\widehat{G})/Z)$ is cyclic. This shows $Z \leq \widehat{G}' = 1$ and $\widehat{G} \cong G$.

(iv) Theorem 7.15 shows that the Sylow p-subgroups of a Schur extension $\widehat{G}$ are non-abelian if p is a divisor of $|Z|$ (where $Z \leq \widehat{G}' \cap \mathrm{Z}(\widehat{G})$).

Theorem 11.5. *If $\mathrm{Z}(G)$ has finite index in G, then G' is finite. In particular, every Schur extension of a finite group is finite.*

Proof. Let $Z := \mathrm{Z}(G)$ and $n := |G : Z| < \infty$. Let R be a transversal for G/Z. For $\Gamma := \{[r, s] : r, s \in R\}$ it holds that $|\Gamma| \leq |R|^2 = |G/Z|^2 = n^2$. For $r, s \in R$ and $z \in Z$ it holds that $[rz, s] = [r, s] = [r, sz]$. Every element $g \in G'$ thus has the form $g = c_1 \ldots c_m$ with $c_1, \ldots, c_m \in \Gamma$. It suffices to show that one can choose $m < n^3$ (then it follows that $|G'| < n^{2n^3} < \infty$). Assume $m \geq n^3$. Then there exists a $\gamma \in \Gamma$ with $|\{i \in \{1, \ldots, m\} : c_i = \gamma\}| \geq n$. Because of $c_i c_{i+1} = c_{i+1}(c_{i+1}^{-1} c_i c_{i+1}) = c_{i+1}\delta$ with $\delta \in \Gamma$, we can assume $c_1 = \ldots = c_n = \gamma$. According to Example 7.9, the transfer $V\colon G \to Z$, $g \mapsto g^n$ is a homomorphism (for the definition of the transfer $V_{H/K}$ one only needs $|G : H| < \infty$). Since Z is abelian, $G' \subseteq \mathrm{Ker}(V)$ holds. Thus $c_1 \ldots c_n = \gamma^n = 1$ and one can reduce m.

For the second assertion, let $\widehat{G}$ be a Schur extension of the finite group G with $\widehat{G}/Z \cong G$. Then $|\widehat{G} : \mathrm{Z}(\widehat{G})| \leq |\widehat{G} : Z| = |G| < \infty$ and therefore $|\widehat{G}| = |G||Z| \leq |G||\widehat{G}'| < \infty$. □

Definition 11.6. Let G be a finite group and A an (possibly infinite) abelian group. The set $C^1(G,A)$ of all maps of the form $G \to A$ becomes an abelian group via $(\alpha\beta)(g) := \alpha(g)\beta(g)$ for $\alpha, \beta \in C^1(G,A)$ and $g \in G$ (it holds that $C^1(G,A) \cong A^{|G|}$). Let $C^2(G,A) := C^1(G \times G, A)$ and

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

Evidently, $Z^2(G,A)$ is then a subgroup of $C^2(G,A)$. The elements in $Z^2(G,A)$ are called *factor systems* (or (2-)*cocycles*) of G with values in A.

Lemma 11.7. *The map $\partial\colon C^1(G,A) \to Z^2(G,A)$ with $\partial\alpha(x,y) := \alpha(x)\alpha(y)\alpha(xy)^{-1}$ for $\alpha \in C^1(G,A)$ and $x,y \in G$ is a homomorphism.*

Proof. Evidently, $\partial\alpha \in C^2(G,A)$ for $\alpha \in C^1(G,A)$. For $x,y,z \in G$ it holds that

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

This shows $\partial\alpha \in Z^2(G,A)$. For $\alpha, \beta \in C^1(G,A)$ and $x,y \in G$ it finally holds that

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

Thus ∂ is a homomorphism. □

Definition 11.8. Let $B^2(G,A) := \partial(C^1(G,A)) \trianglelefteq Z^2(G,A)$ and $H^2(G,A) := Z^2(G,A)/B^2(G,A)$. $H^2(G,A)$ is called the *second cohomology group* of G with values in A.

Lemma 11.9. *For $\overline{\alpha} \in H^2(G,A)$ there exists an $\alpha \in Z^2(G,A)$ with $\alpha B^2(G,A) = \overline{\alpha}$ and $\alpha(1,x) = \alpha(x,1) = 1$ for $x \in G$.*

Proof. Let first $\beta \in Z^2(G,A)$ with $\beta B^2(G,A) = \overline{\alpha}$ be arbitrary. By definition of $Z^2(G,A)$, $\beta(x,1)\beta(x,1) = \beta(1,1)\beta(x,1)$ and $\beta(x,1) = \beta(1,1)$ for $x \in G$. Analogously, $\beta(1,x) = \beta(1,1)$. Let $\gamma(x) := \beta(1,1)^{-1}$ for $x \in G$ and $\alpha := \beta\partial\gamma \in Z^2(G,A)$. Then $\alpha B^2(G,A) = \overline{\alpha}$ and $\alpha(x,1) = \beta(x,1)\gamma(x)\gamma(1)\gamma(x)^{-1} = 1$ for $x \in G$. Certainly, $\alpha(1,x) = 1$ also holds. □

Definition 11.10. $M(G) := H^2(G,\mathbb{C}^\times)$ is called the *Schur multiplier* of G.

Theorem 11.11. *The Schur multiplier $M(G)$ is a finite abelian group with $\exp(M(G)) \mid |G|$.*

Proof. Certainly $M(G)$ is abelian. Let $n := |G|$ and let $\beta \in Z^2(G,\mathbb{C}^\times)$ be arbitrary. Since $\mathbb{C}$ is algebraically closed, there exist $\gamma(x) \in \mathbb{C}^\times$ with $\gamma(x)^n = \prod_{y\in G}\beta(y,x)^{-1}$ for $x \in G$. It then holds that

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

for $y,z \in G$. Let $\alpha := \beta\partial\gamma \in Z^2(G,\mathbb{C}^\times)$. Then $\overline{\alpha} := \alpha B^2(G,\mathbb{C}^\times) = \beta B^2(G,\mathbb{C}^\times) \in M(G)$ and

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

for all $y,z \in G$. In particular, there are only finitely many possibilities for α and it follows that $|M(G)| < \infty$. Furthermore, $\overline{\alpha}^n = \overline{\alpha^n} = 1$. □

Remark 11.12. It even holds that $\exp(G)\exp(M(G)) \mid |G|$ (Exercise 80) and $\exp(M(G))^2 \mid |G|$ (without proof). The conjecture formulated by Schur $\exp(M(G)) \mid \exp(G)$ was, however, disproved in 1974.

Lemma 11.13. *For $\alpha \in Z^2(G,A)$, the map $\Psi_\alpha \colon \mathrm{Hom}(A,\mathbb{C}^\times) \to M(G)$, $\lambda \mapsto (\lambda \circ \alpha)B^2(G,\mathbb{C}^\times)$ is a homomorphism.*

Proof. For $\lambda \in \mathrm{Hom}(A,\mathbb{C}^\times)$ and $x,y,z \in G$, we have

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

and $\lambda\circ\alpha \in Z^2(G,\mathbb{C}^\times)$. For $\lambda,\mu \in \mathrm{Hom}(A,\mathbb{C}^\times)$, we have $(\lambda\mu)\circ\alpha = (\lambda\circ\alpha)(\mu\circ\alpha)$. Thus Ψ_α is indeed a homomorphism. □

Lemma 11.14. *For a finite abelian group A, $\mathrm{Hom}(A,\mathbb{C}^\times) \cong A$.*

Proof. Let $A = \langle a_1\rangle \oplus \ldots \oplus \langle a_n\rangle$ and $d_i := |\langle a_i\rangle|$ for $i = 1,\ldots,n$. Let $\zeta_i \in \mathbb{C}$ be a primitive d_i-th root of unity. For every $\lambda \in \mathrm{Hom}(A,\mathbb{C}^\times)$, it then holds that $\lambda(a_i) \in \langle\zeta_i\rangle$ (Example 1.6(v)). Conversely, every choice $\lambda(a_i) = \zeta_i^{k_i}$ defines a homomorphism. This shows $|\mathrm{Hom}(A,\mathbb{C}^\times)| = d_1\ldots d_n = |A|$. We define $F\colon A \to \mathrm{Hom}(A,\mathbb{C}^\times)$ by $F(a_1^{k_1}\ldots a_n^{k_n})(a_i) := \zeta_i^{k_i}$ for $i = 1,\ldots,n$. It is easily shown that F is a well-defined isomorphism. □

Theorem 11.15 (Schur)**.** *Let $\widehat{G}$ be a Schur extension of G with $\widehat{G}/Z \cong G$. Then Z is isomorphic to a subgroup of $M(G)$. In particular, $|\widehat{G}| \le |G||M(G)|$ and G possesses only finitely many Schur extensions up to isomorphism.*

Proof. For $x \in G$ we choose a preimage $\widehat{x} \in \widehat{G}$ under the canonical epimorphism $\widehat{G} \to \widehat{G}/Z \cong G$. Let $\widehat{1} = 1$. Let $\alpha(x,y) := \widehat{x}\widehat{y}\widehat{xy}^{-1} \in Z$ for $x,y \in G$. For $x,y,z \in G$ it then holds that

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

This shows $\alpha \in Z^2(G,Z)$. According to Theorem 11.5 and Lemma 11.14 it suffices to show that the map Ψ_α from Lemma 11.13 is injective. So let $\lambda \in \mathrm{Hom}(Z,\mathbb{C}^\times)$ with $\lambda\circ\alpha = \partial\gamma$ for some $\gamma \in C^1(G,\mathbb{C}^\times)$. Then $1 = \lambda(1) = \lambda(\alpha(1,1)) = \partial\gamma(1,1) = \gamma(1)$. Let $\widehat{\lambda}\colon \widehat{G} \to \mathbb{C}^\times$ with $\widehat{\lambda}(\widehat{x}a) := \gamma(x)\lambda(a)$ for $x \in G$ and $a \in Z$. Because of $\gamma(1) = 1$, $\widehat{\lambda}$ is an extension of λ. For $x,y \in G$ and $a,b \in Z$ it holds that

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

Thus $\widehat{\lambda}$ is a homomorphism with $\widehat{G}/\mathrm{Ker}(\widehat{\lambda}) \le \mathbb{C}^\times$. It follows that $Z \le \widehat{G}' \le \mathrm{Ker}(\widehat{\lambda})$. This shows $\lambda = 1$ and we are finished. □

Definition 11.16. A Schur extension $\widehat{G}$ of G is called *maximal*, if $|\widehat{G}| = |G||M(G)|$.

Theorem 11.17 (Schur)**.** *Every finite group G possesses a maximal Schur extension.*

Proof. According to Theorem 11.11, $M(G) = \langle\overline{\alpha}_1\rangle \oplus \ldots \oplus \langle\overline{\alpha_n}\rangle$. Let $d_i := |\langle\overline{\alpha_i}\rangle|$ and $A_i \leq \mathbb{C}^\times$ with $|A_i| = d_i$ for $i = 1, \ldots, n$. Let $\alpha_i \in Z^2(G, \mathbb{C}^\times)$ with $\alpha_i B^2(G, \mathbb{C}^\times) = \overline{\alpha_i}$. Then $\alpha_i^{d_i} = \partial\gamma_i$ for some $\gamma_i \in C^1(G, \mathbb{C}^\times)$. Let $\delta_i(x) \in \mathbb{C}^\times$ with $\delta_i(x)^{d_i} = \gamma_i(x)^{-1}$ for $x \in G$. After replacing α_i by $\alpha_i\partial\delta_i$, we have $\alpha_i^{d_i} = 1$ for $i = 1, \ldots, n$. In particular, $\alpha_i \in Z^2(G, A_i)$ for $i = 1, \ldots, n$. According to Lemma 11.9, we may also assume $\alpha_i(x, 1) = \alpha_i(1, x) = 1$ for $x \in G$. Let $A := A_1 \times \ldots \times A_n \cong M(G)$ and $\alpha \in C^2(G, A)$ with $\alpha(x, y) = (\alpha_1(x, y), \ldots, \alpha_n(x, y))$ for $x, y \in G$. Then clearly $\alpha \in Z^2(G, A)$ with $\alpha(1, x) = \alpha(x, 1) = 1$ for $x \in G$.

We define a new operation on $\widehat{G} := G \times A$ via

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

For $x, y, z \in G$ and $a, b, c \in A$, we then have

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

The operation is thus associative. Because of $(1_G, 1_A) \cdot (x, a) = (x, \alpha(1, x)a) = (x, a)$, $(1_G, 1_A)$ is an identity element. Finally, $(x^{-1}, \alpha(x^{-1}, x)^{-1}a^{-1}) \cdot (x, a) = (1_G, 1_A)$. Thus $\widehat{G}$ is a finite group.

We identify $g \in G$ with $(g, 1_A) \in \widehat{G}$ and $a \in A$ with $(1_G, a) \in \widehat{G}$. Then clearly A is the kernel of the epimorphism $\widehat{G} \to G$, $(x, a) \mapsto x$. This shows $A \trianglelefteq \widehat{G}$ and $\widehat{G}/A \cong G$. For $(x, a) \in \widehat{G}$ and $b \in A$, we have $(x, a) \cdot b = (x, ab) = (x, ba) = b \cdot (x, a)$. It follows that $A \leq \mathrm{Z}(\widehat{G})$. It remains to show $A \leq \widehat{G}'$.

Let $\pi_i \colon A \to A_i \leq \mathbb{C}^\times$ be the i-th projection. With the map Ψ_α from Lemma 11.13, we then have $\Psi_\alpha(\pi_i) = (\pi_i \circ \alpha)B^2(G, \mathbb{C}^\times) = \overline{\alpha_i}$ for $i = 1, \ldots, n$. Because $M(G) = \langle\overline{\alpha_1}, \ldots, \overline{\alpha_n}\rangle$, Ψ_α is surjective. According to Lemma 11.14, $\mathrm{Hom}(A, \mathbb{C}^\times) \cong A \cong M(G)$. Therefore Ψ_α is also injective. According to Theorem 2.11 (applied to $\widehat{G}/\widehat{G}'$), there exist normal subgroups $N_1, \ldots, N_s \trianglelefteq \widehat{G}$ with $\widehat{G}' = N_1 \cap \ldots \cap N_s$, such that $\widehat{G}/N_i$ is cyclic for $i = 1, \ldots, s$. Assume $A \not\leq \widehat{G}'$. Then there exists an i with $A \not\leq N_i$. By embedding $\widehat{G}/N_i$ into $\mathbb{C}^\times$, one obtains a homomorphism $\varphi \colon \widehat{G} \to \mathbb{C}^\times$ with $\varphi(A) \neq 1$. The restriction φ_A is thus a non-trivial element in $\mathrm{Hom}(A, \mathbb{C}^\times)$. For $x, y \in G$, we have

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

This yields $\Psi_\alpha(\varphi_A) = 1$ in contradiction to the injectivity of Ψ_α. Thus $A \leq \widehat{G}'$ and $\widehat{G}$ is a Schur extension of G. □

Theorem 11.18. *For $H \leq G$ there exists a homomorphism $F \colon M(G) \to M(H)$ with $\overline{\alpha}^{|G:H|} = 1$ for $\overline{\alpha} \in \mathrm{Ker}(F)$.*

Proof. Let $\alpha \in Z^2(G, \mathbb{C}^\times)$. Then the restriction α_H certainly lies in $Z^2(H, \mathbb{C}^\times)$. In the case $\alpha \in B^2(G, \mathbb{C}^\times)$, we also have $\alpha_H \in B^2(H, \mathbb{C}^\times)$. This induces a well-defined homomorphism $F \colon M(G) \to M(H)$. Let $\alpha B^2(G, \mathbb{C}^\times) \in \mathrm{Ker}(F)$, i. e. $\alpha_H = \partial\gamma$ for some $\gamma \in C^1(H, \mathbb{C}^\times)$. Let $\widetilde{\gamma} \in C^1(G, \mathbb{C}^\times)$ be an arbitrary extension of γ. By replacing α with $\alpha\partial\widetilde{\gamma}^{-1}$, we can assume $\alpha_H = 1$. Let R be a transversal for G/H. For $x \in G$ let $r_x \in R$ and $h_x \in H$ with $x = r_x h_x$. Let $\gamma(x) := \alpha(r_x, h_x)$ for $x \in G$ and $\beta := \alpha\partial\gamma$. For $x \in G$ and $h \in H$ it then holds that

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

Now let $x, y \in G$. Then $\beta(x,y) = \beta(x, r_y h_y) = \beta(x, r_y)\beta(xr_y, h_y)\beta(r_y, h_y)^{-1} = \beta(x, r_y)$. Finally, let $\delta(x) := \prod_{r\in R} \beta(x,r)$ for $x \in G$. For $x, y \in G$ it is then

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

This shows $\beta^{|G:H|} = \partial\delta \in B^2(G, \mathbb{C}^\times)$. Thus $\alpha^{|G:H|} \in B^2(G, \mathbb{C}^\times)$ also holds. □

Corollary 11.19. *If $H_1, \ldots, H_n \leq G$ with coprime indices $|G : H_i|$, then $M(G)$ is isomorphic to a subgroup of $M(H_1) \times \ldots \times M(H_n)$. In particular, $M(G) = 1$ if all Sylow subgroups of G are cyclic.*

Proof. Let $\Gamma_i \colon M(G) \to M(H_i)$ be the homomorphism from Theorem 11.18. Then

$$\Gamma \colon M(G) \to M(H_1) \times \ldots \times M(H_n), \qquad \overline{\alpha} \mapsto (\Gamma_1(\overline{\alpha}), \ldots, \Gamma_n(\overline{\alpha}))$$

is a homomorphism with $\operatorname{Ker}(\Gamma) = \bigcap_{i=1}^n \operatorname{Ker}(\Gamma_i)$. Let $\overline{\alpha} \in \operatorname{Ker}(\Gamma)$. By Theorem 11.18, $\alpha^{|G:H_i|} = 1$ holds for $i = 1, \ldots, n$. Since the indices $|G : H_i|$ are coprime, it follows that $\overline{\alpha} = 1$. Thus Γ is a monomorphism. For the second assertion, one chooses for $H_1, \ldots, H_n$ the Sylow subgroups of G (one for each prime divisor of $|G|$ is sufficient). According to Example 11.4(iii), then $M(H_1) = \ldots = M(H_n) = 1$ and the assertion follows. □

Remark 11.20. The next lemma quantifies Theorem 11.5 for p-groups.

Lemma 11.21. *Let H be an arbitrary group and $|H : \mathrm{Z}(H)| = p^n$ a prime power. Then $|H'| \leq p^{\binom{n}{2}}$ holds.*

Proof. Induction on n. For $n = 1$, $H' = 1$ by Exercise 10. Now let $n \geq 2$. Since $H/\mathrm{Z}(H)$ is nilpotent, H is also nilpotent. Therefore there exists $x \in \mathrm{Z}_2(H) \setminus \mathrm{Z}(H)$. For $a, b \in H$, $[x,b] \in \mathrm{Z}(H)$ and $[x, ab] = [x,a] \cdot {}^a[x,b] = [x,a][x,b]$ hold. Thus $H \to H$, $a \mapsto [x,a]$ is a homomorphism with image

$$N := [x, H] = \big\{[x,a] : a \in H\big\} \leq H' \cap \mathrm{Z}(H).$$

Because of $\mathrm{Z}(H)/N < \mathrm{Z}(H)\langle x\rangle/N \leq \mathrm{Z}(H/N)$, we have $|H/N : \mathrm{Z}(H/N)| \leq p^{n-1}$. Induction yields $|H'/N| = |(H/N)'| \leq p^{\binom{n-1}{2}}$. From

$$[x,a] = [x,b] \iff {}^a x = {}^b x \iff a\mathrm{C}_H(x) = b\mathrm{C}_H(x)$$

it follows that $|N| = |H : \mathrm{C}_H(x)| \leq |H : \mathrm{Z}(H)\langle x\rangle| \leq p^{n-1}$. In total, we now have

$$|H'| = |H'/N||N| \leq p^{\binom{n-1}{2}+n-1} = p^{\binom{n}{2}}.$$ □

Theorem 11.22 (Green). *If $|G| = p_1^{a_1} \ldots p_s^{a_s}$ is the prime factorization of $|G|$, then*

$$|M(G)| \leq p_1^{\binom{a_1}{2}} \ldots p_s^{\binom{a_s}{2}}.$$

Proof. According to Corollary 11.19, one can assume that G is a p-group. Let $\widehat{G}$ be a maximal Schur extension of G with $|\widehat{G}/\mathrm{Z}(\widehat{G})| \leq |\widehat{G}/Z| = |G| = p^a$. By Lemma 11.21, $|M(G)| = |Z| \leq |\widehat{G}'| \leq p^{\binom{a}{2}}$ holds. □

Theorem 11.23. *Let F be a free group, $N \trianglelefteq F$ and $G \cong F/N$ (Theorem 8.7). Then:*

(i) $N/[F,N]$ is a finitely generated abelian group with torsion part $(F' \cap N)/[F,N]$.

(ii) For $N/[F,N] = (F' \cap N)/[F,N] \oplus K/[F,N]$, F/K is a maximal Schur extension of G.

(iii) For every Schur extension $\widehat{G}$ of G, there exists an $L \trianglelefteq F$ with $N = (F' \cap N)L$ and $\widehat{G} \cong F/L$. In particular, $\widehat{G}$ is a factor group of a maximal Schur extension.

(iv) $\boxed{M(G) \cong (F' \cap N)/[F,N]}$ (Hopf formula).

Proof.

(i) Since G is finite, we can assume that F is finitely generated. According to Theorem 1.10, N is also finitely generated. With $N \trianglelefteq F$, we have $[F,N] \trianglelefteq F$ and $[F,N] \leq F' \cap N$. Because $N/[F,N] \leq \mathrm{Z}(F/[F,N])$, $\mathrm{Z}(F/[F,N])$ has finite index in $F/[F,N]$. According to Theorem 11.5, $F'/[F,N]$ is finite. Therefore, $(F' \cap N)/[F,N]$ is also finite. Because $N' \leq [F,N]$, $N/[F,N]$ is abelian. Furthermore,

$$(N/[F,N])/\big((F' \cap N)/[F,N]\big) \cong N/(F' \cap N) \cong F'N/F' \leq F/F'.$$

According to Example 8.11, F/F' is a free abelian group with finite rank. With F/F', $F'N/F'$ must also be torsion-free. Therefore, $(F' \cap N)/[F,N]$ is the torsion part of $N/[F,N]$.

(ii) Because $K/[F,N] \leq N/[F,N] \leq \mathrm{Z}(F/[F,N])$, we have $K \trianglelefteq F$. Let $\widehat{G} := F/K$ and $Z := N/K$. Then $\widehat{G}/Z \cong F/N \cong G$ and $Z \leq \mathrm{Z}(\widehat{G})$ because of $[F,N] \leq K$. From $N/[F,N] \leq F'K/[F,N]$ it follows that

$$Z = N/K \leq F'K/K = (F/K)' = \widehat{G}'.$$

Thus $\widehat{G}$ is a Schur extension with $Z \cong (F' \cap N)/[F,N]$. From Theorem 11.15 it follows that $|M(G)| \geq |(F' \cap N)/[F,N]|$. For the reverse inequality, we first show (iii).

(iii) Let $\alpha\colon F \to G$ and $\beta\colon \widehat{G} \to G$ be the canonical epimorphisms with $N = \mathrm{Ker}(\alpha)$ and $Z := \mathrm{Ker}(\beta)$. Since F is free, there exists a homomorphism $\rho\colon F \to \widehat{G}$ with $\beta\rho = \alpha$. It then holds that $\widehat{G} = \rho(F)Z$ and $Z \leq \widehat{G}' \leq \rho(F)' \leq \rho(F)$, so $\rho(F) = \widehat{G}$. Obviously $L := \mathrm{Ker}(\rho) \leq \mathrm{Ker}(\alpha) = N$. Because $\beta\rho(N) = \alpha(N) = 1$, we have $\rho(N) \leq \mathrm{Ker}(\beta) = Z$. This shows $\rho([F,N]) \leq [\widehat{G}, Z] = 1$ and $[F,N] \leq L$. From $\rho(N) = Z \leq \widehat{G}' = \rho(F')$ it also follows that $N \leq F'L$ and $(F' \cap N)L = F'L \cap N = N$ by Dedekind. Now it holds that

$$|Z| = \frac{|\widehat{G}|}{|G|} = |N : L| = |(F' \cap N)L : L| = |F' \cap N : F' \cap L| \leq |(F' \cap N)/[F,N]|.$$

Therefore, the Schur extension constructed in (ii) is indeed maximal.

According to (i) and the fundamental theorem of finitely generated abelian groups, it holds that

$$L/[F,N] = (L \cap F')/[F,N] \oplus M/[F,N],$$

where $(L \cap F')/[F,N]$ is the torsion part. Because $|N : L| = |F' \cap N : F' \cap L|$, $M/[F,N]$ is the torsion-free part of $N/[F,N]$. According to (ii), F/M is a maximal Schur extension and $\widehat{G} \cong F/L \cong (F/M)/(L/M)$.

(iv) Follows from the proof of (ii). □

Theorem 11.24 (Jones). *For every p-group P of order p^n, it holds that $|M(P)||P'| \leq p^{\binom{n}{2}}$.*

Proof. Let $P = F/N$ be a presentation, $H = F/[F,N]$ and $\mathrm{Z}(H) := Z/[F,N]$. Because of $N/[F,N] \leq \mathrm{Z}(H)$, it holds that $H/\mathrm{Z}(H) \cong F/Z \cong P/(Z/N)$. In particular, $H/\mathrm{Z}(H)$ is a p-group with order $\leq p^n$. From Lemma 11.21 it follows that $|F'/[F,N]| = |H'| \leq p^{\binom{n}{2}}$. With the Hopf formula one obtains $|M(P)||P'| = |(F' \cap N)/[F,N]||F'/(F' \cap N)| = |F'/[F,N]| \leq p^{\binom{n}{2}}$. □

Theorem 11.25. *Let $\widehat{G}_1$, $\widehat{G}_2$ be maximal Schur extensions of G with $\widehat{G}_1/Z_1 \cong G \cong \widehat{G}_2/Z_2$. Then*

(i) (Schur) $\widehat{G}_1' \cong \widehat{G}_2'$ *and* $\widehat{G}_1/\widehat{G}_1' \cong G/G' \cong \widehat{G}_2/\widehat{G}_2'$.

(ii) (Gaschütz) $\widehat{G}_1/\mathrm{Z}(\widehat{G}_1) \cong \widehat{G}_2/\mathrm{Z}(\widehat{G}_2)$.

(iii) (Read) $\mathrm{Z}(\widehat{G}_1)/Z_1 \cong \mathrm{Z}(\widehat{G}_2)/Z_2$.

Proof. Let $G = F/N$, $K_i \trianglelefteq F$ and $\widehat{G}_i \cong F/K_i$ as in Theorem 11.23. We show that the specified groups do not depend on i.

(i) It holds that

$$\begin{aligned} \widehat{G}_i' &\cong F'K_i/K_i \cong F'/(F' \cap K_i) = F'/(F' \cap N \cap K_i) = F'/[F,N], \\ \widehat{G}_i/\widehat{G}_i' &\cong (\widehat{G}_i/Z_i)/(\widehat{G}_i'/Z_i) \cong G/G'. \end{aligned}$$

(ii) For $L/[F,N] := \mathrm{Z}(F/[F,N])$ it holds that $[F,L] \leq [F,N] \leq K_i$ and $L/K_i \leq \mathrm{Z}(F/K_i)$. Conversely, let $xK_i \in \mathrm{Z}(F/K_i)$. Then $[x,F] \leq K_i \cap F' = K_i \cap F' \cap N = [F,N]$ and it follows that $x[F,N] \in \mathrm{Z}(F/[F,N]) = L/[F,N]$. This shows

$$\widehat{G}_i/\mathrm{Z}(\widehat{G}_i) \cong (F/K_i)/\mathrm{Z}(F/K_i) = (F/K_i)/(L/K_i) \cong F/L.$$

(iii) With the notation from (ii) it holds that

$$\mathrm{Z}(\widehat{G}_i)/Z_i \cong (L/K_i)/(N/K_i) \cong L/N.$$ □

Remark 11.26. According to Theorem 11.25(i), a maximal Schur extension of a perfect group G is also perfect and uniquely determined up to isomorphism (this is generalized in Theorem 11.28). It is called the *universal Schur extension* of G.[20] According to Theorem 11.23, every Schur extension of G is isomorphic to a factor group of the universal Schur extension.

Theorem 11.27. *The universal Schur extension of a perfect group has trivial Schur multiplier.*

Proof. Let $\widehat{G}$ be a maximal Schur extension of G with $\widehat{G}/Z \cong G$. Let $\widehat{\widehat{G}}$ be a maximal Schur extension of $\widehat{G}$ with $\widehat{\widehat{G}}/W \cong \widehat{G}$. Since G is perfect, $\widehat{G}$ and $\widehat{\widehat{G}}$ are also perfect. Let $\mathrm{Z}(\widehat{\widehat{G}}/W) = X/W$. It holds that

$$[\widehat{\widehat{G}}, X, \widehat{\widehat{G}}] = [\widehat{\widehat{G}}, \widehat{\widehat{G}}, X] \leq [\widehat{\widehat{G}}, W] = 1.$$

From Lemma 3.6 it follows that $[X, \widehat{\widehat{G}}] = [X, \widehat{\widehat{G}}, \widehat{\widehat{G}}] = 1$ and $X \leq \mathrm{Z}(\widehat{\widehat{G}}) \leq X$. Let L/W be the preimage of Z under $\widehat{\widehat{G}}/W \cong \widehat{G}$. Then $L/W \leq \mathrm{Z}(\widehat{\widehat{G}}/W) = \mathrm{Z}(\widehat{\widehat{G}})/W$ and $\widehat{\widehat{G}}/L \cong (\widehat{\widehat{G}}/W)/(L/W) \cong \widehat{G}/Z \cong G$. Thus $\widehat{\widehat{G}}$ is a Schur extension of G. This shows $\widehat{\widehat{G}} \cong \widehat{G}$ and $M(\widehat{G}) = 1$. □

[20] Schur speaks of *representation groups*.

Theorem 11.28. *If $|G/G'|$ and $|M(G)|$ are coprime, then G has, up to isomorphism, only one maximal Schur extension.*

Proof. As in Theorem 11.25, let $G = F/N$ and $\widehat{G}_i = F/K_i$ for $i = 1, 2$. We choose $x_1, \ldots, x_n \in F$ with

$$\langle x_1, \ldots, x_n \rangle F'N/F'N = F/F'N \cong G/G' \cong C_{d_1} \times \ldots \times C_{d_n}$$

and $x_j^{d_j} \in F'N$ for $j = 1, \ldots, n$. According to Theorem 11.23, $F'N = F'(F' \cap N)K_i = F'K_i$. Let $a_j \in K_1$ with $x_j^{d_j} a_j \in F'$. As a divisor of $|G/G'|$, d_j is coprime to

$$|K_1/(K_1 \cap K_2)| = |K_1K_2/K_2| \leq |N/K_2| = |(N/[F,N])/(K_2/[F,N])| = |M(G)|.$$

Therefore, there exists a $b_j \in K_1$ with $b_j^{d_j} \equiv a_j \pmod{K_1 \cap K_2}$. It follows that

$$(x_j b_j)^{d_j} \equiv x_j^{d_j} b_j^{d_j} \equiv 1 \pmod{F'(K_1 \cap K_2)}.$$

By replacing x_j with $x_j b_j$, we can assume $x_j^{d_j} \in F'(K_1 \cap K_2)$ for $j = 1, \ldots, n$. Because $F' \cap K_1 = [F,N] = F' \cap K_2$, the map $F'N/K_1 \to F'N/K_2$, $yK_1 \mapsto yK_2$ with $y \in F'$ is a well-defined isomorphism. In this process, $x_j^{d_j} K_1$ is mapped to $x_j^{d_j} K_2$.

Every element in $\widehat{G}_i$ has the form $x_1^{e_1} \ldots x_n^{e_n} y K_i$ with $y \in F'$ and uniquely determined $0 \leq e_j < d_j$. Therefore, the map

$$\Gamma \colon \widehat{G}_1 \to \widehat{G}_2, \qquad x_1^{e_1} \ldots x_n^{e_n} y K_1 \mapsto x_1^{e_1} \ldots x_n^{e_n} y K_2$$

is well-defined and bijective. For $0 \leq f_j < d_j$ and $z \in F'$, it holds that

$$x_1^{e_1} \ldots x_n^{e_n} y \cdot x_1^{f_1} \ldots x_n^{f_n} z \equiv x_1^{e_1+f_1} \ldots x_n^{e_n+f_n} \pmod{F'}.$$

Let $e_j + f_j = g_j + k_j d_j$ with $0 \leq g_j < d_j$ for $j = 1, \ldots, n$. Then there exists $c \in F'$ with

$$x_1^{e_1} \ldots x_n^{e_n} y \cdot x_1^{f_1} \ldots x_n^{f_n} z = x_1^{g_1} \ldots x_n^{g_n} x_1^{k_1 d_1} \ldots x_n^{k_n d_n} c.$$

This shows

$$\Gamma(x_1^{g_1} \ldots x_n^{g_n} x_1^{k_1 d_1} \ldots x_n^{k_n d_n} c K_1) = x_1^{g_1} \ldots x_n^{g_n} x_1^{k_1 d_1} \ldots x_n^{k_n d_n} c K_2 = \Gamma(x_1^{e_1} \ldots x_n^{e_n} y K_1) \Gamma(x_1^{f_1} \ldots x_n^{f_n} z K_1),$$

i.e., Γ is an isomorphism. □

Theorem 11.29 (Hochschild-Serre sequence)**.** *Let $N \trianglelefteq G$ and $H = G/N$. Then there exists an exact sequence of the form*

$$M(G) \to M(H) \to N/[G,N] \to G/G' \to H/H' \to 1.$$

Proof. According to the second isomorphism theorem, we may replace H/H' by $G/G'N$. Certainly then

$$\alpha \colon G/G' \to G/G'N, \quad xG' \to xG'N$$

is an epimorphism. Because of $[G,N] \leq G'$,

$$\beta \colon N/[G,N] \to G/G', \quad x[G,N] \to xG'$$

is a well-defined homomorphism with image $NG'/G' = \mathrm{Ker}(\alpha)$. Now let F be a free group and $\rho \colon F \to G$ an epimorphism with kernel $K \trianglelefteq F$. For $L := \rho^{-1}(N) \trianglelefteq F$, it holds that $L/K \cong N$ and

$F/L \cong (G/K)/(L/K) \cong H$. According to the Hopf formula, we may replace $M(G)$ by $(F' \cap K)/[F,K]$ and $M(H)$ by $(F' \cap L)[F,L]$. Because of $\rho([F,L]) = [G,N]$, the map

$$\gamma\colon (F' \cap L)/[F,L] \to N/[G,N], \quad x[F,L] \mapsto \rho(x)[G,N]$$

is a well-defined homomorphism with image $\rho(F' \cap L)/[G,N] = (G' \cap N)/[G,N] = \mathrm{Ker}(\beta)$ and $\mathrm{Ker}(\gamma) = (F' \cap K)[F,L]/[F,L]$. Finally,

$$\delta\colon (F' \cap K)/[F,K] \to (F' \cap L)/[F,L], \quad x[F,K] \mapsto x[F,L]$$

is also a well-defined homomorphism with image $(F' \cap K)[F,L]/[F,L] = \mathrm{Ker}(\gamma)$. □

Corollary 11.30 (Jones). *Let $N \trianglelefteq G$. Then $|M(G/N)|$ is a divisor of $|(G' \cap N)/[G,N]||M(G)|$.*

Proof. With the notation from the proof of Theorem 11.29, it holds that

$$|M(G)/\mathrm{Ker}(\delta)| = |\delta(M(G))| = |\mathrm{Ker}(\gamma)| = \frac{|M(H)|}{|\mathrm{Ker}(\beta)|} = \frac{|M(H)|}{|(G' \cap N)/[G,N]|}.$$ □

Definition 11.31. For finite groups G, H let

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

Theorem 11.32 (Künneth formula). *For finite groups G and H it holds that*

$$\boxed{M(G \times H) \cong M(G) \times M(H) \times P(G,H).}$$

Proof. Let $\alpha \in Z^2(G \times H, \mathbb{C}^\times)$. We consider G and H as subgroups of $G \times H$. As usual, one has restrictions $\alpha_G \in Z^2(G, \mathbb{C}^\times)$ and $\alpha_H \in Z^2(H, \mathbb{C}^\times)$. Let $\varphi(x,y) := \alpha(x,y)\alpha(y,x)^{-1}$ for $x \in G$ and $y \in H$. For $x, y \in G$ and $z \in H$, we have $xz = zx$, $yz = zy$ and

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

Analogously, one shows $\varphi(x,yz) = \varphi(x,y)\varphi(x,z)$ for $x \in G$ and $y, z \in H$. Thus $\varphi \in P(G,H)$. This yields a homomorphism

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

For $\gamma \in C^1(G \times H, \mathbb{C}^\times)$, it is certain that $(\partial\gamma)_G = \partial\gamma_G \in B^2(G, \mathbb{C}^\times)$ and $(\partial\gamma)_H \in B^2(H, \mathbb{C}^\times)$. Due to $\partial\gamma(x,y) = \partial\gamma(y,x)$ for $x \in G$ and $y \in H$, we have $\varphi = 1$ for $\alpha = \partial\gamma$. Thus F induces a homomorphism $\overline{F}\colon M(G \times H) \to M(G) \times M(H) \times P(G,H)$.

Surjectivity of $\overline{F}$: Let $\alpha_1 \in Z^2(G, \mathbb{C}^\times)$, $\alpha_2 \in Z^2(H, \mathbb{C}^\times)$ and $\varphi \in P(G,H)$. According to Lemma 11.9, we may assume $\alpha_1(1,1) = \alpha_2(1,1) = 1$. For $x_1, y_1 \in G$ and $x_2, y_2 \in H$, let $\alpha(x_1x_2, y_1y_2) := \alpha_1(x_1,y_1)\alpha_2(x_2,y_2)\varphi(x_1,y_2)$. Then

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

and $\alpha \in Z^2(G \times H, \mathbb{C}^\times)$. Because of $\varphi(x,1) = \varphi(x,1)\varphi(x,1) = 1$ for $x \in G$, we have $\alpha_G = \alpha_1$ and analogously $\alpha_H = \alpha_2$. For $x \in G$ and $y \in H$, finally

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

This shows $F(\alpha) = (\alpha_1, \alpha_2, \varphi)$.

Injectivity of $\overline{F}$: Let $F(\alpha) = (\partial\gamma_1, \partial\gamma_2, 1)$ with $\gamma_1 \in C^1(G, \mathbb{C}^\times)$ and $\gamma_2 \in C^1(H, \mathbb{C}^\times)$. Then $\alpha(x,y) = \alpha(y,x)$ for $x \in G$ and $y \in H$. Let $\delta(xy) := \gamma_1(x)\gamma_2(y)\alpha(x,y)^{-1}$ for $x \in G$ and $y \in H$. Then

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

for $x_1, y_1 \in G$ and $x_2, y_2 \in H$. Thus $\alpha \in B^2(G \times H, \mathbb{C}^\times)$ and $\overline{F}$ is an isomorphism. □

Remark 11.33.

(i) For $\varphi \in P(G,H)$ and $y \in H$, the map $G \to \mathbb{C}^\times$, $x \mapsto \varphi(x,y)$ is a homomorphism. In particular, $\varphi(x,y) = 1$ for $x \in G'$ and analogously $\varphi(x,y) = 1$ for $x \in G$ and $y \in H'$. It follows that $P(G,H) \cong P(G/G', H/H')$.

(ii) For groups G, H and K, there are isomorphisms $P(G \times H, K) \cong P(G,K) \times P(H,K)$ and $P(G, H \times K) \cong P(G,H) \times P(G,K)$ via restriction (easy to show). With the next lemma, one can thus completely determine $P(G,H)$.

Lemma 11.34. *For $n, m \in \mathbb{N}$, $P(C_n, C_m) \cong C_{\gcd(n,m)}$.*

Proof. Let $\langle x \rangle \cong C_n$, $\langle y \rangle \cong C_m$ and $\varphi \in P(\langle x \rangle, \langle y \rangle)$. Then

$$\varphi(x,y)^n = \varphi(x^n, y) = \varphi(1,y) = 1 = \varphi(x,1) = \varphi(x, y^m) = \varphi(x,y)^m,$$

thus also $\varphi(x,y)^{\gcd(n,m)} = 1$. Let $\zeta \in \mathbb{C}$ be a primitive $\gcd(n,m)$-th root of unity. Then $\varphi(x,y) = \zeta^k$ with $1 \le k \le \gcd(n,m)$. Furthermore, φ is already uniquely determined by $\varphi(x,y)$. Conversely, for each $\zeta^k \in \langle \zeta \rangle$, one can construct a $\varphi \in P(\langle x \rangle, \langle y \rangle)$ with $\varphi(x,y) = \zeta^k$. This yields the isomorphism $P(C_n, C_m) \cong \langle \zeta \rangle \cong C_{\gcd(n,m)}$. □

Corollary 11.35. *If G and H are finite groups with $\gcd(|G/G'|, |H/H'|) = 1$, then $M(G \times H) \cong M(G) \times M(H)$.*

Proof. The assertion follows from Theorem 11.32, Remark 11.33 and Lemma 11.34. □

Example 11.36. If G and H are perfect groups with universal Schur extensions $\widehat{G}$ and $\widehat{H}$ respectively, then $\widehat{G} \times \widehat{H}$ is the universal Schur extension of $G \times H$ (Exercise 77).

Theorem 11.37. *For $n_1, \ldots, n_k \in \mathbb{N}$, we have*

$$M(C_{n_1} \times \ldots \times C_{n_k}) \cong \bigtimes_{1 \le i < j \le k} C_{\gcd(n_i, n_j)}.$$

Proof. By Corollary 11.19, Theorem 11.32, Remark 11.33 and Lemma 11.34, we have

$$\begin{aligned} M(C_{n_1} \times \ldots \times C_{n_k}) &\cong M(C_{n_2} \times \ldots \times C_{n_k}) \times P(C_{n_1}, C_{n_2} \times \ldots \times C_{n_k}) \cong \ldots \\ &\cong \bigtimes_{1 \le i < j \le k} P(C_{n_i}, C_{n_j}) \cong \bigtimes_{1 \le i < j \le k} C_{\gcd(n_i, n_j)}. \end{aligned}$$

□

Example 11.38.

(i) If $A \cong C_{d_1} \times \ldots \times C_{d_n}$ with $d_1 \mid \ldots \mid d_n$ as in Theorem 2.11, then the formula simplifies to

$$M(A) \cong C_{d_1}^{n-1} \times C_{d_2}^{n-2} \times \ldots \times C_{d_{n-1}}.$$

(ii) If G is elementary abelian of rank k, then $M(G)$ is elementary abelian of rank $\binom{k}{2}$. Thus the estimate in Theorem 11.22 is optimal. In particular, $M(C_2^2) \cong C_2$. The groups D_8 and Q_8 are therefore the only proper Schur extensions of C_2^2. This shows that there can be non-isomorphic maximal Schur extensions.

(iii) Let G be a p-group of order p^n with $|G : \Phi(G)| = p^k$. According to Theorem 11.24 and Corollary 11.30 (with $N = \Phi(G)$) we have

$$p^{\binom{k}{2}} = |M(G/\Phi(G))| \le |G'||M(G)| \le p^{\binom{n}{2}}.$$

Because of $|G'| \le |\Phi(G)| = p^{n-k}$ it follows that $|M(G)| \ge p^{\binom{k}{2}-n+k} = p^{\binom{k+1}{2}-n}$. Green has proven $M(G) \ne 1$ for $k \ge 4$. If G is extraspecial, one obtains $p^{\binom{n-1}{2}-1} \le |M(G)| \le p^{\binom{n}{2}-1}$. Blackburn and Evens have proven that here $|M(G)| = p^{\binom{n-1}{2}-1}$ holds for $n \ge 5$.

(iv) Let $\widehat{G}$ be a Schur extension of $G \in \{D_{2^n}, Q_{2^n}, SD_{2^n}\}$ with $\widehat{G}/Z \cong G$. According to Theorem 11.11, $\widehat{G}$ is a 2-group and $4 = |G : G'| = |\widehat{G}/Z : \widehat{G}'/Z| = |\widehat{G} : \widehat{G}'|$. According to Taussky, it therefore holds that $\widehat{G} \in \{D_{2^m}, Q_{2^m}, SD_{2^m}\}$. It follows that $|Z| \le |\mathrm{Z}(\widehat{G})| = 2$ and in the case $|Z| = 2$ we have $Z = \mathrm{Z}(\widehat{G})$ and $G \cong \widehat{G}/Z \cong D_{2^{m-1}}$. We have thus shown:

$$M(G) \cong \begin{cases} C_2 & \text{if } G \cong D_{2^n}, \\ 1 & \text{if } G \in \{Q_{2^n}, SD_{2^n}\}. \end{cases}$$

(v) The Sylow groups of A_7 are $\langle (1,2,3,4)(5,6), (1,2)(3,4) \rangle \cong D_8$, $\langle (1,2,3), (4,5,6) \rangle \cong C_3^2$, $\langle (1,\ldots,5) \rangle \cong C_5$ and $\langle (1,\ldots,7) \rangle \cong C_7$. According to Corollary 11.19 there exists a monomorphism $M(A_7) \to M(D_8) \times M(C_3^2) \cong C_6$. In fact, it holds[21]

$$M(A_n) = \begin{cases} C_6 & \text{if } n \in \{6, 7\}, \\ C_2 & \text{if } n \in \{5, 8, 9, \ldots\}. \end{cases}$$

(vi) Let $G = \mathrm{PSL}(2, p)$ for a prime $p > 3$. According to Remark 10.14, every Sylow group of G is cyclic or a dihedral group. From Example 11.4 and (iv) it follows that $M(G) \le C_2$. Therefore $\mathrm{SL}(2, p)$ is the universal Schur extension of $\mathrm{PSL}(2, p)$. Apart from the exceptions $\mathrm{SL}(2, 4) \cong \mathrm{PSL}(2, 4) \cong A_5$ and $\mathrm{PSL}(2, 9) \cong A_6$, this also holds for $\mathrm{PSL}(2, q)$ for a prime power $q \ge 5$ (without proof).

[21] See notes on combinatorial group theory

Exercises

Exercise 1. Let G be a group. Show:

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

(b) Every subgroup of index 2 is normal.

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

Exercise 2. Let U, V, W be subgroups of a (possibly infinite) group G. Show:

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

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

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

(d) $|UV||U \cap V| = |U||V|$.

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

(f) If $|G : U|$ and $|G : V|$ are finite and coprime, then $|G : U \cap V| = |G : U||G : V|$ and $G = UV$ hold.

Exercise 3. Let G be finite and $X, Y \subseteq G$ with $|X| + |Y| > |G|$. Show $G = XY$.

Exercise 4. Show that for every group G the following statements are equivalent:

(1) G is abelian.

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

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

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

Exercise 5. Let $H \leq G$ be groups with $n := |G : H| < \infty$. Show:

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

(b) The kernel of this action is $H_G = \bigcap_{g \in G} gHg^{-1}$. In particular, $|G : H_G| \leq n!$.

(c) If $|G| < \infty$ and n is the smallest prime divisor of $|G|$, then $H \trianglelefteq G$ (this generalizes Exercise 1(b)).

(d) If $n > 1$, then $\bigcup_{g \in G} gHg^{-1} \neq G$.
Hint: By replacing G with G/H_G, one can assume $|G| < \infty$.

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

Exercise 6. Let $H_1, \ldots, H_n$ be the conjugates of $H \leq G$. Show $H^G = H_1 \ldots H_n$.

Exercise 7. Show:

(a) A group is finite if and only if it possesses only finitely many subgroups.

(b) A finitely generated group possesses for each $n \in \mathrm{N}$ only finitely many subgroups of index n.

(c) Let G be finitely generated and $H \leq G$ with $|G : H| < \infty$. Then there exists a characteristic subgroup K of G with $K \leq H$ and $|G : K| < \infty$.

Exercise 8. For $3 \leq n \in \mathbb{N}$ let

$$D_{2n} := \langle \sigma, \tau \rangle \leq \mathrm{Sym}(\mathbb{C})$$

with $\sigma(z) := e^{\frac{2\pi \mathrm{i}}{n}} z$ and $\tau(z) := \overline{z}$ (complex conjugation) for $z \in \mathbb{C}$. Show that:

(a) $\langle \sigma \rangle \trianglelefteq D_{2n}$ and $|D_{2n}| = 2n$.

(b) If $\Delta \subseteq \mathbb{C}$ is the regular n-gon in the complex plane with center 0 and vertex 1 (i.e., the convex hull of the n-th roots of unity), then

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

i.e., D_{2n} is the *symmetry group* of the regular n-gon.

One calls D_{2n} the *dihedral group* of order $2n$.

Exercise 9.

(a) Show that $(\mathbb{Q}, +)$ is *locally cyclic*, i. e. every finitely generated subgroup of $\mathbb{Q}$ is cyclic. Is $\mathbb{Q}$ itself cyclic?

(b) Let p be a prime and $A := \{ap^b + \mathbb{Z} : a, b \in \mathbb{Z}\} \leq \mathbb{Q}/\mathbb{Z}$. Show that every proper subgroup of A is finite and cyclic.

(c) Let $\mathbb{Z}[X]$ be the ring of polynomials with integer coefficients. Let $\mathbb{Q}_+ := \{q \in \mathbb{Q} : q > 0\}$. Show that $(\mathbb{Z}[X], +) \cong (\mathbb{Q}_+, \cdot)$.
Hint: Prime factorization.

(d) Decide whether $(\mathbb{R}, +)$ and $(\mathbb{C}, +)$ are isomorphic.
Hint: Axiom of choice.

Exercise 10. Let G be a group. Show that:

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

(b) $\mathrm{C}_{\mathrm{Aut}(G)}(\mathrm{Inn}(G))$ consists of all automorphisms that act trivially on $G/\mathrm{Z}(G)$. In particular, $\mathrm{Z}(\mathrm{Aut}(G)) = 1$ if $\mathrm{Z}(G) = 1$.

Exercise 11.

(a) How many abelian groups of order 72 exist up to isomorphism?

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

Exercise 12. Let G be a non-abelian group of order 8. Show:

(a) G possesses an element x of order 4.
Hint: Exercise 4.

(b) For $y \in G \setminus \langle x \rangle$, it holds that $y^4 = 1$ and $yx = x^{-1}y$.

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

(d) In the case $y^2 = 1$, $G \cong D_8$.

(e) In the case $y^2 \neq 1$,

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

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

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

Exercise 13 (3. Isomorphism Theorem[22])**.** For $B \trianglelefteq A \leq G$ and $D \trianglelefteq C \leq G$, it holds that

$$(A \cap C)B/(A \cap D)B \cong (C \cap A)D/(C \cap B)D.$$

Exercise 14 (Schreier's Refinement Theorem)**.** Any two subnormal series $1 = A_0 \trianglelefteq \ldots \trianglelefteq A_k = G$ and $1 = B_0 \trianglelefteq \ldots \trianglelefteq B_l = G$ can be refined such that the factors of the new series are isomorphic up to their order. Deduce from this the Jordan-Hölder Theorem.
Hint: Exercise 13

Exercise 15. Let $A \to \mathrm{Aut}(G)$ be a group action. A subnormal series $1 = N_0 \trianglelefteq \ldots \trianglelefteq N_k = G$ is called A-*invariant* if ${}^aN_i = N_i$ for $i = 1, \ldots, k$ and all $a \in A$. An A-invariant subnormal series is called an A-*composition series* if the N_i are pairwise distinct and the series cannot be further refined as an A-invariant series. Show that the A-*composition factors* N_i/N_{i-1} are uniquely determined up to isomorphism and order. Deduce that the chief factors of G do not depend on the choice of a chief series.
Hint: Proof of Jordan-Hölder or Exercise 14.

Exercise 16.

(a) Determine the composition factors and chief factors of S_4.

(b) Determine the composition factors and chief factors of $\mathrm{GL}(2, 3)$.
Hint: Consider the natural action of $\mathrm{GL}(2, 3)$ on the set of 1-dimensional subspaces of $\mathbb{F}_3^2$.

Exercise 17. A subgroup $H \leq G$ is called *fully invariant* in G if $\alpha(H) \subseteq H$ for every endomorphism α of G. Show:

(a) Every fully invariant subgroup is characteristic in G.

(b) Every subgroup of a cyclic group is fully invariant.

[22] or Zassenhaus Lemma

(c) Which subgroups of S_4 are characteristic and which are fully invariant?

(d) $\mathrm{Z}(G)$ is always characteristic in G.

(e) $\mathrm{Z}(G)$ is not necessarily fully invariant in G.

Exercise 18. Let G be a group and $x, y \in G$. Show:

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

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

Exercise 19.

(a) Show $D_{4n} \cong D_{2n} \times C_2$ for all odd numbers $n \geq 3$.

(b) Determine all natural numbers $n \geq 3$ such that the dihedral group D_{2n} is nilpotent. Calculate the nilpotency class if applicable.

Exercise 20. Let $G = N \oplus M$ be finite. Show $\mathrm{F}(G) = \mathrm{F}(N) \oplus \mathrm{F}(M)$.
Attention: Not every subgroup of $N \oplus M$ has the form $N_1 \oplus M_1$ with $N_1 \leq N$ and $M_1 \leq M$.

Exercise 21. Show for every group G:

(a) $\exp(\mathrm{Z}_k(G)/\mathrm{Z}_{k-1}(G)) \leq \exp(\mathrm{Z}(G))$ for $k \geq 1$.
Hint: Induction on k and Exercise 18(a).

(b) $[G^{[i]}, \mathrm{Z}_j(G)] \leq \mathrm{Z}_{j-i}(G)$ for $1 \leq i \leq j$.
Hint: Induction on $i + j$ and the 3-subgroup lemma.

Exercise 22. How many nilpotent groups of order 72 are there up to isomorphism?

Exercise 23. Show that every group of order 220 has a normal subgroup of order 55.
Hint: First construct a smaller normal subgroup.

Exercise 24. Let P and Q be two distinct Sylow p-subgroups of G such that $|P \cap Q|$ is as large as possible. Show

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

Exercise 25.

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

(b) Let $G = N \oplus M$. Show $\Phi(G) = \Phi(N) \oplus \Phi(M)$.

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

Exercise 26. A group G is called *complete*, if $\mathrm{Z}(G) = 1 = \mathrm{Out}(G)$. Show:

(a) S_3 is complete.

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

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

(d) If S is a non-abelian simple group, then $\mathrm{Aut}(S)$ is complete.
Hint: Exercise 10.

Exercise 27. Construct groups $X, Y, Z \leq G$ with $[X, Y, Z] \neq [Y, X, Z]$.

Exercise 28. Let A be an abelian normal subgroup of G, such that G/A is cyclic, say $G/A = \langle xA \rangle$ with $x \in G$. Show that the map $A \to G'$, $a \mapsto [a, x]$ is an epimorphism. Conclude $|A| = |G'||A \cap \mathrm{Z}(G)|$.

Exercise 29.

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

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

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

Exercise 30. For a finite group G let $\mathrm{F}_0(G) := 1$, $\mathrm{K}_0(G) := G$ and inductively

$$\mathrm{F}_n(G)/\mathrm{F}_{n-1}(G) := \mathrm{F}(G/\mathrm{F}_{n-1}(G)), \qquad \mathrm{K}_n(G) := \bigcap_{i \geq 1} \mathrm{K}_{n-1}(G)^{[i]}$$

for $n \geq 1$. Show:

(a) Let $1 = N_0 \trianglelefteq \ldots \trianglelefteq N_k = G$ be a normal series with nilpotent factors N_i/N_{i-1} for $i = 1, \ldots, k$. Then $K_{k-i}(G) \leq N_i \leq \mathrm{F}_i(G)$ holds for $i = 0, \ldots, k$.

(b) G is solvable if and only if there exists an $l(G) = l \geq 0$ with $\mathrm{F}_{l-1}(G) < \mathrm{F}_l(G) = G$ and $\mathrm{K}_{l-1}(G) > \mathrm{K}_l(G) = 1$. If applicable, $l(G)$ is called the *Fitting length* of G.

Remark: In general, $G^{[\infty]} := \mathrm{K}_1(G)$ is the *nilpotent residual*, $\mathrm{F}_\infty(G) := \bigcup_{n \in \mathbb{N}} \mathrm{F}_n(G)$ the *solvable radical* and $G^{(\infty)} := \bigcap_{n \in \mathbb{N}} G^{(n)} = \bigcap_{n \in \mathbb{N}} \mathrm{K}_n(G)$ the *solvable residual* of G.

Exercise 31. Let G be a group and A, B conjugate subgroups of $\mathrm{Aut}(G)$. Show $G \rtimes A \cong G \rtimes B$.

Exercise 32. Let G be a finite group and $x, y \in G$ distinct involutions. Show $\langle x, y \rangle \cong D_{2n}$ (where $D_4 = C_2^2$).

Exercise 33. (Levi) Let G be a finite group in which any two conjugate elements commute. Show that G is nilpotent.
Hint: Show that elements of coprime orders commute.

Exercise 34. Let H be a π-Hall subgroup of G and $N \trianglelefteq G$. Show:

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

(b) For $U \leq G$, $H \cap U$ is not necessarily a π-Hall subgroup of U.

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

Exercise 35. A finite group G is called a *Frobenius group*, if there exists a subgroup $1 < H < G$ with $H \cap gHg^{-1} = 1$ for all $g \in G \setminus H$ (thus H is particularly far from being a normal subgroup). Show that H is a Hall subgroup of G.
Hint: Theorem 4.10 is useful.

Exercise 36.

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

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

(c) Construct a finite group G with two non-conjugate Hall subgroups of the same order.
Hint: Consider $G = \mathrm{GL}(3,2)$.
Remark: The group $\mathrm{PSL}(2,11)$ even possesses non-isomorphic Hall subgroups of the same order.

Exercise 37. Let G be a solvable group, p a prime number and $|\mathrm{Syl}_p(G)| = p_1^{a_1} \dots p_n^{a_n}$ (prime factorization). Show $p_i^{a_i} \equiv 1 \pmod{p}$ for $i = 1, \dots, n$.
Remark: This refines the congruence from Sylow's Theorem.

Exercise 38. (Goursat) Let G_1 and G_2 groups. Construct a bijection between the set of subgroups of $G_1 \times G_2$ and the set of 5-tuples $(H_1, H_2, K_1, K_2, \varphi)$, where $K_i \trianglelefteq H_i \leq G_i$ $(i = 1, 2)$ and $\varphi\colon H_1/K_1 \to H_2/K_2$ is an isomorphism.

Exercise 39. Show for $n \geq 3$:

(a) $S_n = \langle (1,2), (1,3), \dots, (1,n) \rangle = \langle (1,2), (2,3), \dots, (n-1,n) \rangle = \langle (1,2,\dots,n), (1,2) \rangle$.

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

Hint: You may use that S_n is generated by all transpositions.

Exercise 40. Determine the transitive permutation groups of degree ≤ 4. Which of these are primitive or regular?
Hint: Theorem 6.21 is helpful.

Exercise 41. Let G be a transitive permutation group of degree > 1, in which every non-trivial element has at most one fixed point and at least one element has exactly one fixed point. Show that G is a Frobenius group (see Exercise 35).

Exercise 42. Realize A_5 as a primitive permutation group of degree 5, 6 and 10.
Hint: According to Theorem 6.9, it suffices to find suitable subgroups.

Exercise 43. Show that a permutation group cannot act 5-transitively.

Exercise 44. Let G be a finite group, $N \trianglelefteq G$ and $G/N \cong H$. Show that G is isomorphic to a subgroup of $N \wr H$.
Hint: Apply Theorem 6.26 to the regular action.

Exercise 45. Show that the Sylow p-subgroups of S_{p^n} are isomorphic to $C_p \wr \ldots \wr C_p$ (n factors).

Exercise 46. Calculate the nilpotency class of $C_p \wr C_p \in \mathrm{Syl}_p(S_{p^2})$ for every prime p.

Exercise 47. Show for $n \in \mathbb{N}$ that the 2-Sylow subgroups of S_n are Carter groups.

Exercise 48. Show that a group G is a primitive permutation group if and only if there exists a minimal normal subgroup $A \trianglelefteq G$ with $\mathrm{C}_G(A) = A$.

Exercise 49. Show that $\mathrm{SL}(2, \mathbb{F}_{2^n})$ acts 3-transitively on the set of 1-dimensional subspaces of $\mathbb{F}_{2^n}^2$.

Exercise 50. Show:

(a) For every proper subgroup H of a non-abelian simple group G, $|G : H| \geq 5$ holds.
Hint: Exercise 5.

(b) There is no simple group of order 120.
Hint: Realize a counterexample as a subgroup of A_6.

(c) $\mathrm{GL}(3, 2)$ is a simple group of order 168.

(d) The infinite group $A_\infty := \bigcup_{n \geq 1} A_n$ is simple.

Exercise 51. Calculate the transfer $V_{G/G'}$ explicitly.
Remark: The from class field theory states that the transfer $V_{G'/G''}$ is always trivial.

Exercise 52. Let H be a Hall subgroup of a finite group G with $\mathrm{N}_G(H) = \mathrm{C}_G(H)$. Show that H has a normal complement.

Exercise 53. Let $H \leq G$ with prime index $p := |G : H|$ and $\gcd(|H|, p - 1) = 1$. Show $H \trianglelefteq G$.
Remark: This generalizes Exercise 5.

Exercise 54. Let G be a finite group with a cyclic Sylow p-subgroup. Let $N \trianglelefteq G$ such that $|G : N|$ is divisible by p. Show that N is p-nilpotent.
Hint: For $Q \in \mathrm{Syl}_p(N)$, $\mathrm{N}_N(Q) = Q \rtimes K$ holds by Schur-Zassenhaus. Show $[Q, K] = 1$.

Exercise 55. Prove the following statements for every supersolvable group G:

(a) If p is the smallest prime divisor of $|G|$, then G is p-nilpotent.

(b) If q is the largest prime divisor of $|G|$, then G possesses a normal q-Sylow subgroup.

Exercise 56. Show:

(a) Every non-abelian simple group of order < 168 is isomorphic to A_5.
Hint: Using suitable theorems from the lecture, one has to discuss at most three orders.

(b) Every group of order 612 is solvable.

Exercise 57. Let G be a p-nilpotent group and $Q \leq P \in \mathrm{Syl}_p(G)$. Show that $\mathrm{N}_G(Q)/\mathrm{C}_G(Q)$ is a p-group.
Remark: This is the converse of Frobenius' transfer theorem.

Exercise 58. Show that G is p-nilpotent if $G/\Phi(G)$ is p-nilpotent.
Remark: This localizes the Frattini theorem.

Exercise 59 $(2 + 2 + 2 + 2$ points**).** Let $N, M \trianglelefteq G$. Show:

(a) If $N, M \trianglelefteq G$ are p-nilpotent, then so is MN. The product of all p-nilpotent normal subgroups $\mathrm{F}_{(p)}(G)$ is therefore p-nilpotent.

(b) $\mathrm{O}_{p'}(G) \leq \mathrm{F}_{(p)}(G)$ and $\mathrm{F}_{(p)}(G)/\mathrm{O}_{p'}(G) = \mathrm{O}_p(G/\mathrm{O}_{p'}(G))$.

(c) If G/N and G/M are p-nilpotent, then so is $G/(N \cap M)$.

(d) The smallest normal subgroup of G with p-nilpotent factor group is $\mathrm{O}^{p'}(\mathrm{O}^p(G))$.[23]

Exercise 60. We show that a word w over an alphabet A can be transformed into exactly one reduced word $\overline{w}$. Assume indirectly that $v \neq w$ are reduced words and a sequence of words $v = v_1, \ldots, v_k = w$ exists, such that v_i and v_{i+1} differ only by a subword of the form aa^{-1} or $a^{-1}a$ $(a \in A)$ (for $i = 1, \ldots, k-1$). Let $|v_i|$ be the number of letters of v_i. We choose the sequence such that $\sum_{i=1}^{k} |v_i|$ is minimal. Show:

(a) There exists an i with $|v_{i-1}| < |v_i| > |v_{i+1}|$.

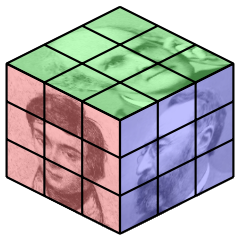
(b) If $v_{i-1} = \ldots a \ldots$, $v_i = \ldots aa^{-1}a \ldots$, $v_{i+1} = \ldots a \ldots$, then one can delete v_i and v_{i+1}.

(c) If $v_{i-1} = \ldots aa^{-1} \ldots$, $v_i = \ldots aa^{-1} \ldots bb^{-1} \ldots$, $v_{i+1} = \ldots bb^{-1} \ldots$, then one can replace v_i by v_i' with $|v_i'| = |v_i| - 4$.

(d) All other cases are analogous and lead likewise to a contradiction.

[23] In some books one writes $\mathrm{O}^{pp'}(G) := \mathrm{O}^{p'}(\mathrm{O}^p(G))$ and $\mathrm{O}_{p'p}(G)$ instead of $\mathrm{F}_{(p)}(G)$.

Christmas puzzle. Let $G \leq S_{48}$ be the group of the Rubik's cube as in the Christmas lecture. We consider the "extended" Rubik's cube with pictures on all sides:



(a) Describe the group of all states of the extended Rubik's cube using G. How many states are there?

(b) How can the extended Rubik's cube be solved if one can already solve the ordinary Rubik's cube?

(c) Who are the three men?

Exercise 61.

(a) Give a presentation of S_4 with generators and relations.

(b) Determine the structure of $\langle x, y \mid x^2 = y^2 = 1 \rangle$.
Hint: It is a semidirect product of well-known groups.

Exercise 62. Let G be a group with normal subgroup N, such that G/N is a free group. Show that N has a complement in G.
Hint: Remark 5.3.

Exercise 63. Let G be a non-abelian group of order 12. Let $P \in \mathrm{Syl}_3(G)$ and $Q \in \mathrm{Syl}_2(G)$. Show:

(a) In the case $P \not\trianglelefteq G$, then $G \cong A_4$.
Hint: Use the action on $\mathrm{Syl}_3(G)$.

Now let $P \trianglelefteq G$ and thus $G = P \rtimes Q$.

(b) In the case $Q \cong C_2^2$, then $G \cong D_{12}$.

(c) In the case $Q \cong C_4$, then

$$G := \langle x, y \mid x^3 = y^4 = 1,\ yxy^{-1} = x^{-1} \rangle.$$

Remark: This group is called *dicyclic*.

(d) How many groups of order 12 are there up to isomorphism?

Exercise 64. Let $P := \langle x, y \mid x^4 = y^2 = [x, y]^2 = [x, x, y] = [y, x, y] = 1 \rangle$. Show that the following 14 groups of order 16 are pairwise non-isomorphic:

$$C_{16}, C_8 \times C_2, C_4^2, C_4 \times C_2^2, C_2^4, D_{16}, SD_{16}, Q_{16}, M_{16}, D_8 \times C_2, Q_8 \times C_2, C_4 \rtimes C_4, D_8 * C_4, P.$$

Hint: Compare G', $\exp(G)$, $\Phi(G)$ and $\mathrm{Z}(G)$ in this order.
Remark: These are all groups of order 16 up to isomorphism.

Exercise 65.

(a) Let $G = N_1 \oplus \ldots \oplus N_k$ with characteristic subgroups $N_1, \ldots, N_k \leq G$. Show

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

(b) Determine all $n \in \mathbb{N}$ such that $\mathrm{Aut}(C_n)$ is cyclic.
Hint: Use (a).

(c) Show $\mathrm{Aut}(G) \ncong C_3$ for every finite group G.

Exercise 66. Let p be a prime, $n \geq 3$ and $P := M_{p^n}$. Show:

(a) $\mathrm{Z}(P) = \Phi(P)$.

(b) Every proper subgroup of P is abelian.

(c) $UV = VU$ for all $U, V \leq P$.

(d) For $p = 2$, $\mathrm{Aut}(P)$ is a 2-group.
Hint: Remark 4.21.

Exercise 67. A finite group is called a *Dedekind group*, if all subgroups are normal.

(a) According to Theorem 4.10, every Dedekind group is nilpotent. Show that a nilpotent group is a Dedekind group if and only if each of its Sylow subgroups is a Dedekind group.

(b) Show that a p-group for $p > 2$ is a Dedekind group if and only if it is abelian.
Hint: Theorem 9.6.

(c) Show that $Q_8 \times C_2^n$ is a Dedekind group for all $n \geq 0$.
Remark: Dedekind proved that $Q_8 \times C_2^n$ is the only non-abelian Dedekind group of order 2^{n+3}.

Exercise 68. Let P be a non-abelian p-group and $A \leq P$ with $|A| = p^2$ and $\mathrm{C}_P(A) = A$. Show that P has maximal class.
Hint: Induction on $|P|$.

Exercise 69. (Wong) Let $n \geq 4$ and $M_{2^n} \cong P \in \mathrm{Syl}_2(G)$. Show that G is 2-nilpotent.
Hint: Exercise 66 and Remark 7.19.

Exercise 70. Let E be extraspecial of order p^{d+1}. Then $\overline{E} := E/E'$ is a d-dimensional vector space over $\mathbb{F}_p \cong E'$. Show that

$$\beta \colon \overline{E} \times \overline{E} \to E', \quad (xE', yE') \mapsto [x, y]$$

is a well-defined non-degenerate alternating bilinear form (alternating means $\beta(x, x) = 0$ for all $x \in \overline{E}$). Conclude that d is even without using Theorem 9.20.

Exercise 71. Show that for every finite p-group $P \neq 1$, the following statements are equivalent:

(a) P is extraspecial.

(b) $|\mathrm{Z}(P)| = |\Phi(P)| = p$.

(c) $|\mathrm{Z}(P)| = |P'| = p$.

(d) $\mathrm{Z}(P) = P' = \Phi(P)$ is cyclic.

Hint: Exercise 18.
Remark: In the case $\Phi(P) = 1$ or $P' = \Phi(P) = \mathrm{Z}(P)$, P is called *special*.

Exercise 72. Let G be a finite group. Show:

(a) $H \leq \mathrm{F}(G)$ holds if and only if H is a subnormal nilpotent subgroup of G.

(b) For $H, K \trianglelefteq\trianglelefteq G$, it holds that $H \cap K \trianglelefteq\trianglelefteq G$.

(c) For $H \trianglelefteq\trianglelefteq G$ and $P \in \mathrm{Syl}_p(G)$, it holds that $H \cap P \in \mathrm{Syl}_p(H)$.
Remark: Kleidman has proven the converse using the CFSG, i. e. $H \trianglelefteq\trianglelefteq G$ if $H \cap P \in \mathrm{Syl}_p(H)$ for all prime numbers p and all $P \in \mathrm{Syl}_p(G)$.

Exercise 73. Let G be a finite perfect group. Show that $\mathrm{Aut}(G)$ is isomorphic to a subgroup of $\mathrm{Aut}(G/\mathrm{Z}(G))$.

Exercise 74. Construct a finite, non-solvable group G with $\mathrm{E}(G) = 1$.

Exercise 75. Show that $\mathrm{GL}(2,4) \cong A_5 \times C_3$.

Exercise 76. Show:

(a) All involutions in $G := \mathrm{GL}(3,4)$ are conjugate.
Hint: Since the minimal polynomial splits, one can use the Jordan normal form.

(b) All involutions in $S := \mathrm{SL}(3,4)$ are conjugate.
Hint: Choose $x \in S$ concretely and show that $\mathrm{C}_G(x) \nsubseteq S$.

(c) All involutions in $\overline{S} := S/\mathrm{Z}(S) = \mathrm{PSL}(3,4)$ are conjugate.

(d) $\mathrm{PSL}(3,4)$ and A_8 are non-isomorphic simple groups of the same order.

Exercise 77. Let $\widehat{G}$ be a Schur extension of a finite group G with $\widehat{G}/Z \cong G$.

(a) Show that for $W \leq Z$, $\widehat{G}/W$ is also a Schur extension of G.

(b) Let $\widehat{H}$ be a Schur extension of a finite group H. Show that $\widehat{G} \times \widehat{H}$ is a Schur extension of $G \times H$.

Exercise 78. Determine the Schur multiplier and a corresponding Schur extension of D_{2n} with $n \geq 3$.

Exercise 79. Let A and B be finite abelian groups and $f\colon A \to B$ a homomorphism. Let $A^* := \mathrm{Hom}(A, \mathbb{C}^\times)$. Show:

(a) The map $f^*\colon B^* \to A^*$, $\lambda \mapsto \lambda \circ f$ is a homomorphism.

(b) The map $\Gamma_A\colon A \to (A^*)^*$ with $\Gamma_A(a)(\lambda) := \lambda(a)$ for $a \in A$ is an isomorphism.
Hint: According to Lemma 11.14, it suffices to show that Γ_A is a monomorphism.

(c) $(f^*)^* \circ \Gamma_A = \Gamma_B \circ f$.

(d) $|\mathrm{Hom}(A, B)| = |\mathrm{Hom}(B, A)|$.

(e) f is surjective (resp. injective) if and only if f^* is injective (resp. surjective).

(f) The number of subgroups of A isomorphic to B is the number of factor groups of A isomorphic to B.

Exercise 80 (Alperin-Kuo)**.** Show that $\exp(M(G))\exp(G) \mid |G|$ for every finite group G.
Hint: Apply Theorem 11.18 to a cyclic p-subgroup $H \leq G$.

Exercise 81. Let $Z \leq \mathrm{Z}(G)$ with $\gcd(|Z|, |G/Z|) = 1$. Show:

(a) $H^2(G/Z, Z) = 1$.

(b) Z possesses a complement in G.
Remark: This can be used to prove the Schur-Zassenhaus theorem.

Exercise 82. Let A be an abelian group and $\alpha\colon G \to \mathrm{Aut}(A)$, $x \to \alpha_x$ a homomorphism. We define

$$Z^2_\alpha(G, A) := \big\{\gamma\colon G \times G \to A : \forall x, y, z \in G : \gamma(x, y)\gamma(xy, z) = \alpha_x(\gamma(y, z))\gamma(x, yz)\big\}.$$

Show:

(a) For $\gamma \in Z^2_\alpha(G, A)$, $\widehat{G}_\gamma := A \times G$ becomes a group with the operation

$$(a, x) * (b, y) := (a\alpha_x(b)\gamma(x, y), xy).$$

(b) $A_\gamma := A \times 1$ is a normal subgroup of $\widehat{G}_\gamma$ isomorphic to A and $G_\gamma/A_\gamma \cong G$.

(c) Conversely, let $\widehat{G}$ with $A \trianglelefteq \widehat{G}$ and $\widehat{G}/A \cong G$. Let $\alpha\colon G \to \mathrm{Aut}(A)$ be the conjugation action of $\widehat{G}$ on A. Show that there exists a $\gamma \in Z^2_\alpha(G, A)$ with $\widehat{G} \cong \widehat{G}_\gamma$.

Remark: For Schur extensions, α is the trivial map.

A Appendix

A.1 Hall's characterization of solvable groups

Remark A.1. Burnside's p^aq^b-theorem states that every group of order p^aq^b for primes p and q is solvable. One usually proves this theorem in representation theory or character theory,[24] even though there are (elaborate) purely group-theoretic proofs. We use this theorem to prove a converse of Theorem 5.35.

Lemma A.2. *Let H_1, H_2, H_3 be solvable subgroups of a group G with $G = H_1H_2 = H_1H_3$ and $\gcd(|G : H_2|, |G : H_3|) = 1$. Then G is solvable.*

Proof. In the case $H_1 = 1$, $G = H_2$ is solvable. So let $H_1 \neq 1$ and let A be a minimal normal subgroup of H_1. Since H_1 is solvable, A is an elementary abelian p-group. Because of $\gcd(|G : H_2|, |G : H_3|) = 1$, we can assume wlog. that p is not a divisor of $|G : H_2|$. Then H_2 contains a Sylow p-subgroup of G. By Sylow, there exists $g \in G$ with $A \leq gH_2g^{-1}$. Because of $G = H_1H_2$, we may assume $g \in H_1$. Then $A = g^{-1}Ag \leq H_2$ and $N := A^G = A^{H_1H_2} = A^{H_2} \leq H_2$. Like H_2, N is also solvable. Obviously, H_iN/N for $i = 1, 2, 3$ satisfy the same assumptions as H_i. By induction on $|G|$, G/N is therefore solvable and thus also G. □

Theorem A.3 (Hall)**.** *For every finite group G, the following statements are equivalent:*

(1) G is solvable.

(2) For every prime p, G possesses a p'-Hall subgroup.

(3) G possesses a Sylow system.

Proof.

(1) ⇒ (2): Theorem 5.35

(2) ⇒ (3): Lemma 5.39

(3) ⇒ (1): Let $(P_1, \ldots, P_n)$ be a Sylow system of G. In the case $n \leq 2$, G is solvable by Burnside's p^aq^b-theorem. So let $n \geq 3$ and $H_i := \prod_{j \neq i} P_j$ for $i = 1, 2, 3$. According to Lemma 5.39, H_i is a p_i'-Hall subgroup of G. Obviously, $\{P_j : j \neq i\}$ is a Sylow system of H_i. By induction on n, we can assume that H_i is solvable. Furthermore, $G = H_1H_2 = H_1H_3$ as well as $\gcd(|G : H_2|, |G : H_3|) = 1$ holds. From Lemma A.2, the claim follows. □

[24] See lecture notes

Table 1: Number of groups of order ≤ 2000

	1	2	3	4	5	6	7	8	9	10

A.2 Tables

Table 1: Number of groups of order ≤ 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

Table 1: Number of groups of order ≤ 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[25]	4	66	2	5	19	4
1030+	1	54	1	4	2	11	1	4	1	231

[25]This number was corrected after 20 years in [D. Burrell, *On the number of groups of order 1024*, Comm. Alg. 50 (2022), 2408–2410].

Table 1: Number of groups of order ≤ 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

Table 1: Number of groups of order ≤ 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

Table 2: Non-abelian simple groups of order $\leq 10^6$

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

Table 3: Primitive permutation groups of degree $d \leq 15$

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	$\mathrm{AGL}(1,8),\ \mathrm{A\Gamma L}(1,8),\ \mathrm{AGL}(3,2),\ \mathrm{PSL}(2,7),\ \mathrm{PGL}(2,7),\ A_8,\ S_8$
9	$C_3^2 \rtimes C_4,\ S_3 \wr C_2,\ M_9 = C_3^2 \rtimes Q_8,\ \mathrm{AGL}(1,9),\ \mathrm{A\Gamma L}(1,9),$ $\mathrm{ASL}(2,3),\ \mathrm{AGL}(2,3),\ \mathrm{SL}(2,8),\ \mathrm{A\Sigma L}(2,8),\ A_9,\ S_9$
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	$A_6,\ S_6,\ A_7,\ A_8,\ A_{15},\ S_{15}$

Index