Math 214: Theory of Finite Groups

Fall 1999

Robert Boltje
Department of Mathematics
University of California
Santa Cruz, CA 95064
U.S.A.
boltje@math.ucsc.edu

December 15, 1999

Contents

1 The Symmetric Group

1.1 Definition Let Ω be a set. The set of all bijections $\sigma\colon \Omega \to \Omega$ forms a group $\mathrm{Sym}(\Omega)$ under composition. If $\Omega = \{1, \dots, n\}$ for some $n \in \mathbb{N}$, we write $\mathrm{Sym}(n)$ instead. The group $\mathrm{Sym}(\Omega)$ is called the *symmetric group of* Ω and $\mathrm{Sym}(n)$ is called the *symmetric group of degree* n.

1.2 Remark Let $n \in \mathbb{N}$.

(a) Let $i_1, \dots, i_k$ be k pairwise distinct elements of $\{1, \dots, n\}$. Then by $(i_1, \dots, i_k) \in \mathrm{Sym}(n)$ we denote the element σ with $\sigma(i_j) = i_{j+1}$ for $1 \leqslant j \leqslant k-1$, $\sigma(i_k) = i_1$, and $\sigma(i) = i$ for $i \notin \{i_1, \dots, i_k\}$. We call $(i_1, \dots, i_k)$ a *cycle* of *length* k or shortly a *k-cycle*. Thus, a 1-cycle is the identity. A 2-cycle is also called a *transposition*. It is not difficult to see that every element $\sigma \in \mathrm{Sym}(n)$ can be written as a product of pairwise disjoint cycles. If, by adding 1-cycles, we require that each element of $\{1, \dots, n\}$ occurs in a cycle of σ, then there is only one way of writing σ as product of pairwise disjoint cycles, up to reordering the cycles (note that disjoint cycles commute with each other). Assume that, with this way of writing, the cycle lengths of the cycles occurring in σ are $k_1 \geqslant \cdots \geqslant k_r$. Then we call σ of *cycle-type* $(k_1, \dots, k_r)$. Note that $k_1 + \cdots + k_r = n$ so that $(k_1, \dots, k_r)$ is a *partition* of n.

(b) Two elements $\sigma, \tau \in \mathrm{Sym}(n)$ are conjugate in $\mathrm{Sym}(n)$ (i.e., there exists $\rho \in \mathrm{Sym}(n)$ such that $\tau = \rho\sigma\rho^{-1}$) if and only if they have the same cycle type. (Exercise 1)

(c) $\mathrm{Sym}(n)$ is generated by $\{(1,2), (2,3), \dots, (n-1, n)\}$. In fact, for each cycle $(i_1, \dots, i_k)$ we have

$$(i_1, \dots, i_k) = (i_1, i_2)(i_2, i_3) \cdots (i_{k-1}, i_k)$$

and for $i < j$ in $\{1, \dots, n\}$ we have

$$(i, j) = (i, i+1)(i+1, i+2) \cdots (j-2, j-1)(j-1, j)(j-2, j-1) \cdots (i, i+1)\,.$$

(d) If Ω is a set of n elements, then $\mathrm{Sym}(\Omega) \cong \mathrm{Sym}(n)$. In fact, if we choose any bijection $f\colon \Omega \to \{1, \dots, n\}$, then $\mathrm{Sym}(\Omega) \to \mathrm{Sym}(n)$, $\sigma \mapsto f \circ \sigma \circ f^{-1}$ is a group isomorphism.

(e) By (c), every $\sigma \in \mathrm{Sym}(n)$ can be written as a product of transpositions: $\sigma = \tau_1 \cdots \tau_r$. If one can also write $\sigma = \tau_1' \cdots \tau_s'$ with transpositions $\tau_1', \dots, \tau_s'$, then $r - s$ is even (see linear algebra). Therefore, the *sign map*

$$\mathrm{sgn}\colon \mathrm{Sym} \longrightarrow \{-1, 1\}, \quad \sigma \mapsto (-1)^r\,,$$

if σ is a product of r transpositions, is well-defined. Clearly, it is a group homomorphism. Its kernel $\mathrm{Alt}(n)$ is called the *alternating group of degree* n. If $n \geqslant 2$, then $[\mathrm{Sym}(n) : \mathrm{Alt}(n)] = 2$. Note that, by the first equation in part (c), a k-cycle is in $\mathrm{Alt}(n)$ if and only if k is odd.

(f) It is easy to show by induction on n that $\mathrm{Sym}(n)$ has order $n!$.

1.3 Lemma (a) *For $n \geqslant 3$, the group* $\mathrm{Alt}(n)$ *is generated by the 3-cycles of the form* $(i, i+1, i+2)$, $1 \leqslant i \leqslant n-2$.

(b) *For $n \geqslant 5$, any two 3-cycles in* $\mathrm{Alt}(n)$ *are conjugate.*

Proof (a) Each element in $\mathrm{Alt}(n)$ is a product of an even number of transpositions. Since

$$(a,b)(c,d) = (a,b)(b,c)(b,c)(c,d) \quad \text{and} \quad (a,b)(a,c) = (a,c,b)\,,$$

$\mathrm{Alt}(n)$ is generated by all 3-cycles. Each 3-cycle or its inverse is of the form (a,b,c) with $a < b < c$. We can reduce the difference $c-a$ by the formulas

$$(a,b,d) = (a,b,c)(b,c,d)^2 \quad \text{and} \quad (a,c,d) = (a,b,c)^2(b,c,d)$$

whenever $a < b < c < d$. This proves the result.

(b) Let $\pi_1, \pi_2 \in \mathrm{Alt}(n)$ be two 3-cycles. By Remark 1.2(b), there exists $\sigma \in \mathrm{Sym}(n)$ with $\pi_2 = \sigma\pi_1\sigma^{-1}$. Since $n \geqslant 5$, there exists a transposition τ which is disjoint to π_1. Therefore, $\tau\pi_1\tau^{-1} = \pi_1$ and $(\sigma\tau)\pi_1(\sigma\tau)^{-1} = \pi_2$. But either σ or $\sigma\tau$ is an element of $\mathrm{Alt}(n)$. □

1.4 Theorem *For $n \geqslant 5$, the group* $\mathrm{Alt}(n)$ *is simple.*

Proof Assume that $1 \neq N \trianglelefteq \mathrm{Alt}(n)$. We have to show that $\mathrm{Alt}(n) = N$ and by Lemma 1.3 it suffices to show that N contains an arbitrary 3-cycle. Let $1 \neq \sigma \in N$ and write $\sigma = \pi_1 \cdots \pi_r$ as a product of pairwise disjoint cycles. We consider the following cases.

Case 1: One of the elements π_i has length at least 4, so $\pi_i = (a,b,c,d,\dots)$. Set $\rho := (a,b,c)$. Then N also contains

$$\rho\sigma\rho^{-1}\sigma^{-1} = (a,b,c)(a,b,c,d,e_1,\dots,e_r)(a,c,b)(e_r,\dots,e_1,d,c,b,a) = (a,b,d)\,.$$

Case 2: All elements π_i have length at most 3 and one of them is a 3-cycle. After reordering the elements π_i we may assume that $\pi_1 = (a,b,c)$. We may assume that $r \geqslant 2$. Then $\pi_2 = (d,e)$ or $\pi_2 = (d,e,f)$. Set $\rho := (a,b,d)$. Then N contains

$$\rho^{-1}\sigma\rho\sigma^{-1} = (a,d,b)(a,b,c)(d,e)(a,b,d)(a,c,b)(e,d) = (a,d,b,c,e)$$

or

$$\rho^{-1}\sigma\rho\sigma^{-1} = (a,d,b)(a,b,c)(d,e,f)(a,b,d)(a,c,b)(f,e,d) = (a,d,b,c,e)\,,$$

and , by case 1, N contains also a 3-cycle.

Case 3: All elements π are transpositions and $r \geqslant 3$. So $\sigma = (a,b)(c,d)(e,f)$ with a,b,c,d,e,f pairwise distinct. Set $\rho := (a,c,e)$. Then N contains

$$\rho\sigma\rho^{-1}\sigma^{-1} = (a,c,e)(a,b)(c,d)(e,f)(a,e,c)(a,b)(c,d)(e,f) = (a,c,e)(b,f,d)\,,$$

and, by case 2, N contains also a 3-cycle.

Case 4: We have $\sigma = (a,b)(c,d)$ with pairwise distinct $(a,b)(c,d)$. Set $\rho := (a,c,e)$ with $e \notin \{a,b,c,d\}$. Then N contains

$$\rho\sigma\rho^{-1}\sigma^{-1} = (a,c,e)(a,b)(c,d)(a,e,c)(a,b)(c,d) = (a,c,e,d,b)\,,$$

and, by case 1, N contains also a 3-cycle.

Therefore, in any case, N contains a 3-cycle and the theorem is proved. □

2 Groups Acting on Sets

2.1 Definition An *action* of a group G on a set Ω is a function

$$\varphi\colon G \times \Omega \longrightarrow \Omega$$

satisfying

(i) $\varphi(g, \varphi(h, \omega)) = \varphi(gh, \omega)$,

(ii) $\varphi(1, \omega) = \omega$,

for all $\omega \in \Omega$ and $g, h \in G$. In this case we call Ω a *G-set* and φ the underlying structure map.

Let Ω_1 and Ω_2 be two G-sets with structure maps φ_1 and φ_2. We call a map $f\colon \Omega_1 \to \Omega_2$ a *G-map* (or *G-equivariant* or a *morphism of G-sets*), if

$$f(\varphi_1(g, \omega_1)) = \varphi_2(g, f(\omega_1))$$

for all $\omega_1 \in \Omega_1$ and $g \in G$. The G-sets Ω_1 and Ω_2 are called isomorphic, if there exists a bijective G-map between them (note that the inverse of such a map is again a morphism of G-sets)

2.2 Remark Let $\varphi\colon G \times \Omega \to \Omega$ be an action of a group G on a set Ω.

(a) If there is no risk of confusion we prefer the notation ${}^g\omega := \varphi(g, \omega)$ (or sometimes $g\omega := \varphi(g, \omega)$) for $g \in G$ and $\omega \in \Omega$. With this notation the axioms (i) and (ii) in the above definition translate to

(i) ${}^{(gh)}\omega = {}^g({}^h\omega)$,

(ii) ${}^1\omega = \omega$,

for $g, h \in G$ and $\omega \in \Omega$. Moreover, in this notation, the condition for a map $f\colon \Omega_1 \to \Omega_2$ being a G-map reads

$$f({}^g\omega_1) = {}^g f(\omega_1)\,.$$

for all $\omega_1 \in \Omega_1$ and $g \in G$.

(b) For fixed $g \in G$ the map $\Omega \to \Omega$, $\omega \mapsto {}^g\omega$, is a bijection, the inverse being $\omega \mapsto {}^{g^{-1}}\omega$. This follows immediately from the axioms (i) and (ii).

(c) For each $\omega \in \Omega$ the set $\mathrm{stab}_G(\omega) := \{g \in G \mid {}^g\omega = \omega\}$ is a subgroup of G, called the *stabilizer* of ω in G. We have the rule $\mathrm{stab}_G({}^g\omega) = g\mathrm{stab}_G(\omega)g^{-1}$ for each $g \in G$.

(d) For each $\omega \in \Omega$ the set $\mathrm{orb}_G(\omega) := \{{}^g\omega \mid g \in G\}$ is called the *G-orbit* of ω. The G-orbits form a partition of Ω (i.e., Ω is the disjoint union of the different G-orbits). In particular, the relation

$$\omega_1 \sim \omega_2 \quad :\Longleftrightarrow \quad \text{there exists } g \in G \text{ with } \omega_1 = {}^g\omega_2$$

is an equivalence relation.

2.3 Lemma *Let G be a group and let Ω be a set. Then the maps*

$$\{\varphi\colon G\times\Omega\to\Omega \mid \varphi \text{ action}\}\underset{\beta}{\overset{\alpha}{\leftrightarrows}}\{\rho\colon G\to \mathrm{Sym}(\Omega) \mid \rho \text{ group homomorphism}\}$$

$$\varphi\mapsto\Big(g\mapsto(\omega\mapsto\varphi(g,\omega))\Big)$$

$$\Big((g,\omega)\mapsto(\rho(g))(\omega)\Big)\hookleftarrow\rho$$

are well-defined inverse bijections.

Proof Let $\varphi\colon G\times\Omega\to\Omega$ be an action and set $\rho:=\alpha(\varphi)$. Then $\rho(g)$ is a bijection from Ω to Ω by Remark 2.2(b). Moreover, for $g,h\in G$ and $\omega\in\Omega$ we have

$$(\rho(g)\circ\rho(g))(\omega)=(\rho(g))(\varphi(h,\omega))=\varphi(g,\varphi(h,\omega))=\varphi(gh,\omega)=(\rho(gh))(\omega)\,.$$

This implies that ρ is a group homomorphism.

Conversely, let $\rho\colon G\to\mathrm{Sym}(\Omega)$ be a group homomorphism and set $\varphi:=\beta(\rho)$. Then we have for all $g,h\in G$ and $\omega\in\Omega$:

$$\varphi(gh,\omega)=(\rho(gh))(\omega)=(\rho(g)\circ\rho(h))(\omega)=(\rho(g))(\varphi(h,\omega)=\varphi(g,\varphi(h,\omega))$$

and also $\varphi(1,\omega)=(\rho(1))(\omega)=\mathrm{id}_\Omega(\omega)=\omega$. Therefore, φ is an action.

Finally, for each action φ and each homomorphism ρ, we have

$$\beta(\alpha(\varphi))(g,\omega)=((\alpha(\varphi))(g))(\omega)=\varphi(g,\omega)$$

and

$$(\alpha(\beta(\rho))(g))(\omega)=(\beta(\rho))(g,\omega)=(\rho(g))(\omega)$$

for arbitrary $g\in G$ and $\omega\in\Omega$, showing that $\alpha\circ\beta=\mathrm{id}$ and $\beta\circ\alpha=\mathrm{id}$. □

2.4 Definition Let Ω be a G-set under the action $\varphi\colon G\times\Omega\to\Omega$ and let $\rho\colon G\to\mathrm{Sym}(\Omega)$ be the corresponding group homomorphism.

(a) The action is called *faithful*, if ρ is injective. The kernel of ρ is called the *kernel* of the action.

(b) The action is called *transitive*, if Ω consists only of one orbit.

(c) The action is called *free*, if $\mathrm{stab}_G(\omega)=1$ for each $\omega\in\Omega$.

2.5 Examples Let G be a group.

(a) Let $H\leqslant G$. Then $G\times G/H\to G$, $(g,g'H)\mapsto gg'H$, defines a transitive action of G on G/H. For $g\in G$ one has $\mathrm{stab}_G(gH)=g\mathrm{stab}_G(H)g^{-1}=gHg^{-1}$. The kernel of this action is $\bigcap_{g\in G}gHg^{-1}$, the biggest normal subgroup of G contained in H. For $H=1$, one obtains the *translation action* $G\times G\to G$, $(g,g')\mapsto gg'$. It is faithful, transitive, and free.

(b) There is a *conjugation action* $G \times G \to G$, $(g, x) \mapsto gxg^{-1}$, of G on G. One has $\mathrm{stab}_G(x) = C_G(x)$, the *centralizer* of x in G. There is also a conjugation action of G on the set $\mathfrak{U}$ of subgroups of G: $G \times \mathfrak{U} \to \mathfrak{U}$, $(g, H) \mapsto gHg^{-1}$. One has $\mathrm{stab}_G(H) = N_G(H)$, the *normalizer* of H in G.

More generally, for any subset X of G, we call

$$C_G(X) := \{g \in G \mid gx = xg \text{ for all } x \in X\}$$

the *centralizer* of X in G and

$$N_G(X) := \{g \in G \mid gXg^{-1} = X\}$$

the *normalizer* of X in G. Note that $C_G(X) \trianglelefteq N_G(X)$. Obviously, $C_G(G) = Z(G)$, the *center* of G.

(c) The subgroup of $\mathrm{O}_2(\mathbb{R})$ which maps a regular n-gon with origin in its center on itself is the dihedral group D_{2n} of order $2n$. It is generated by a rotation d by $2\pi/n$ and any reflection s. Its elements are $d^i s^j$ with $0 \leqslant i \leqslant n-1$ and $0 \leqslant j \leqslant 1$. Using the relations $d^n = 1$, $s^2 = 1$, and $sd = d^{-1}s$ one can carry out every computation in D_{2n}.

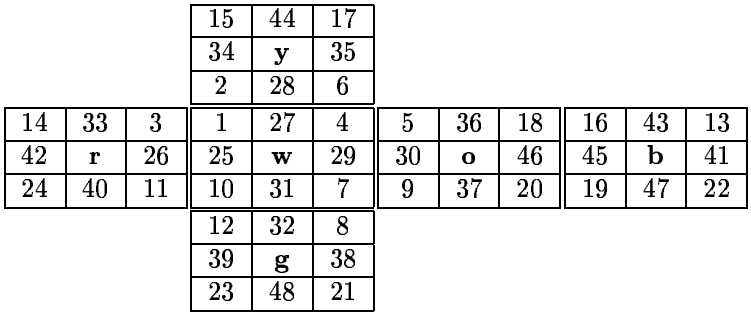
Let $T \subset \mathbb{R}^3$ be a regular tetrahedron with the origin in its center (i.e., the origin is its center of mass). We want to determine the group $G := \{g \in \mathrm{O}_3(\mathbb{R}) \mid g(T) = T\}$. Clearly, each $g \in G$ permutes the vertices v_1, v_2, v_3, v_4 of T, which defines an action $G \times \{1,2,3,4\} \to \{1,2,3,4\}$ and by Lemma 2.3 a group homomorphism $\rho : G \to \mathrm{Sym}(4)$. The map ρ is injective, since a linear transformation is uniquely determined by the images of the four vertices. Moreover, ρ is surjective, since each transposition is in its image. In fact, the transposition (i, j) is realized as the reflection at the hyperplane which contains the other two vertices and is perpendicular to the line connecting v_i and v_j.

One might also be interested in the physically possible transformations of the tetrahedron (reflections at hyperplanes can not be carried out with real objects). This group is $T \cap \mathrm{SO}(3)$, since only the rotations are possible. It is now easy to see that $T \cap \mathrm{SO}(3)$ is isomorphic to $\mathrm{Alt}(4)$.

In the same sense, the symmetry group of a cube is a group of order 48 which is isomorphic to $\mathrm{Sym}(4) \times \mathbb{Z}/2\mathbb{Z}$, and its subgroup of rotations is isomorphic to $\mathrm{Sym}(4)$ (cf. Exercise 7).

Moreover, the symmetry group of a dodecahedron or icosahedron is a group of order 120. Its subgroup of rotations is isomorphic to $\mathrm{Alt}(5)$. However, the group of 120 elements is not isomorphic to $\mathrm{Sym}(5)$ but to $\mathbb{Z}/2\mathbb{Z} \times \mathrm{Alt}(5)$, since as for the cube it contains the reflection at the origin as central element. One idea to show these results is to use the action of the symmetry group on the 5 different cubes sitting inside a dodecahedron.

(d) *Rubik's cube.* The following is an unfolded version of Rubik's cube with the colors red, yellow, white, green, orange, and white.



We assume that the cube has the centers of its sides fixed in $\mathbb{R}^3$. Then there are 48 *places* on its surface. We mark them by $1, \ldots, 48$ as in the above picture. We distinguish between these places and the 48 physical, colored *sides* of the little cubes, which can be moved. We also number them and assume that at the beginning (when the cube is in its original state) the side with number k is on the place with number k. Now any combination of rotations (let us call them *moves*) moves the numbered sides to other places. If such a combination puts the side which was in place k to place $\sigma(k)$, then the so defined map $\sigma\colon \{1, \ldots, 48\} \to \{1, \ldots, 48\}$ is an element of Sym(48) and composition of moves corresponds to composition of permutations. Therefore, the moves form a subgroup Ru of Sym(48) generated by the elements

$$
\begin{aligned}
r &= (1,15,22,12)(2,13,23,10)(3,14,24,11)(25,34,41,39)(26,33,42,40)\,,\\
y &= (1,5,16,14)(2,6,17,15)(3,4,18,13)(27,36,43,33)(28,35,44,34)\,,\\
w &= (1,10,7,4)(2,11,8,5)(3,12,9,6)(25,31,29,27)(26,32,30,28)\,,\\
g &= (7,11,22,20)(8,12,23,21)(9,10,24,19)(31,40,47,37)(32,39,48,38)\,,\\
o &= (4,8,19,17)(5,9,20,18)(6,7,21,16)(29,38,45,35)(30,37,46,36)\,,\\
b &= (13,16,19,22)(14,17,20,23)(15,18,21,24)(41,43,45,47)(42,44,46,48)\,.
\end{aligned}
$$

In fact, each constellation of the cube corresponds in a bijective way to a permutation $\sigma \in Ru$, namely the one which is given by $i \mapsto \sigma(i)$, if the side with number i is on place $\sigma(i)$. Using GAP (Exercise 6) one finds that the order of Ru is $43252003274489856000 = 2^{27} \cdot 3^{14} \cdot 5^3 \cdot 7^2 \cdot 11$.

2.6 Remark Let G be a group.

(a) If Ω_i, $i \in I$, are G-sets, then also the disjoint union $\dot{\bigcup}_{i\in I}\Omega_i$ and $\times_{i\in I}\Omega_i$ are G-sets in an obvious way.

(b) If Ω is a G-set, then each G-orbit and union of G-orbits is again a G-set.

(c) If $f\colon \Omega \to \Omega'$ is a morphism of G-sets and $\omega \in \Omega$, then $\mathrm{stab}_G(\omega) \leqslant \mathrm{stab}_G(f(\omega))$. In fact, for $g \in \mathrm{stab}_G(\omega)$, one has ${}^g f(\omega) = f({}^g\omega) = f(\omega)$. Moreover, $f(\mathrm{orb}_G(\omega)) = \mathrm{orb}_G(f(\omega))$, since $f({}^g\omega) = {}^g f(\omega) \in \mathrm{orb}_G(f(\omega))$ and ${}^g f(\omega) = f({}^g\omega) \in f(\mathrm{orb}_G(\omega))$ for all $g \in G$.

2.7 Theorem *Let G be a group.*

(a) Let Ω be a transitive G-set, $\omega \in \Omega$, and $H := \mathrm{stab}_G(\omega)$. Then the map

$$f\colon G/H \longrightarrow \Omega\,, \quad gH \mapsto {}^g\omega\,,$$

is an isomorphism of G-sets.

(b) For $H_1, H_2 \leqslant G$ one has: $G/H_1 \cong G/H_2 \iff H_1$ and H_2 are conjugate in G.

Proof (a) The map f is well-defined, since $f(ghH) = {}^{(gh)}\omega = {}^g({}^h\omega) = {}^g\omega = f(gH)$ for all $g \in G$ and $h \in H$. It is G-equivariant, since $f(g_1g_2H) = {}^{(g_1g_2)}\omega = {}^{g_1}({}^{g_2}\omega) = {}^{g_1}f(g_2H)$ for all $g_1, g_2 \in G$. The map f is surjective by Remark 2.6(c). Finally, it is injective, since, for $g_1, g_2 \in G$, $f(g_1H) = f(g_2H)$ implies ${}^{g_1}\omega = {}^{g_2}\omega$, ${}^{g_2^{-1}g_1}\omega = \omega$, and $g_2^{-1}g_1 \in H$ so that $g_1H = g_2H$.

(b) $\Rightarrow$: Let $f\colon G/H_1 \to G/H_2$ be an isomorphism and let $g \in G$ such that $f(H_1) = gH_2$. Then, by Remark 2.6(c), $H_1 = \mathrm{stab}_G(H_1) \leqslant \mathrm{stab}_G(gH_2) = gH_2g^{-1}$. The same argument applied to the fact $f^{-1}(gH_2) = H_1$ gives $gH_2g^{-1} \leqslant H_1$.

$\Leftarrow$: Assume that $H_1 = gH_2g^{-1}$ for some $g \in G$. The G-set $\Omega := G/H_2$ is transitive and $\mathrm{stab}_G(gH_2) = gH_2g^{-1} = H_1$. Therefore, by part (a), G/H_2 is isomorphic to G/H_1. □

2.8 Remark Let G be a group and let $\mathcal{S}$ be a set of representatives of the conjugacy classes of subgroups of G.

(a) Each transitive G-set is isomorphic to G/H for a unique $H \in \mathcal{S}$. Each finite G-set is isomorphic to a disjoint union of copies of G/H, $H \in \mathcal{S}$, and the number of times each G/H occurs is uniquely determined.

(b) *Orbit equation:* If Ω is a finite G-set and $\mathcal{R} \subset \Omega$ is a set of representatives for the G-orbits of Ω. Then

$$|\Omega| = \sum_{\omega \in \mathcal{R}} [G : \mathrm{stab}_G(\omega)]\,,$$

since Ω is the disjoint union of its G-orbits and the G-orbit of $\omega \in \mathcal{R}$ is isomorphic to $G/\mathrm{stab}_G(\omega)$ which has order $[G : \mathrm{stab}_G(\omega)]$.

Theorems 2.9 and 2.10 are consequences of the orbit equation.

2.9 Theorem *Let G be a p-group and $1 \neq N \trianglelefteq G$. Then $Z(G) \cap N \neq 1$. In particular, $Z(G) \neq 1$.*

Proof Consider the conjugation action of G on N (here we need that N is normal in G). An element $x \in N$ forms an orbit of length 1 if and only if $x \in N \cap Z(G)$. The orbit equation gives

$$|N| = |N \cap Z(G)| + \sum_{\substack{x \in C \\ C_G(x) \neq G}} [G : C_G(x)]\,,$$

where $\mathcal{C}$ denotes a set of representatives of the G-conjugacy classes of elements of N. This implies that p divides $|N \cap Z(G)|$. □

2.10 Theorem (Sylow, 1832–1918) *Let p be a prime, G a finite group of order $n = p^a m$ with $p \nmid m$, and let $s_k(G)$ denote the number of subgroups of G of order k, for $k \in \mathbb{N}$.*

(a) For each $b \in \{0, \ldots, a\}$ one has $s_{p^b}(G) \equiv 1 \mod p$.

(b) Each p-subgroup of G is contained in a Sylow p-subgroup of G.

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

Proof (a) The claim is clear for $b = 0$. So let $b \geqslant 1$. Set $\mathcal{M} := \{X \subseteq G \mid |X| = p^b\}$. G acts on $\mathcal{M}$ by translations: $(g, X) \mapsto gX$. For a set of representatives $\mathcal{R} \subseteq \mathcal{M}$ of the G-orbits we have the orbit equation

$$\binom{n}{p^b} = |\mathcal{M}| = \sum_{X \in \mathcal{R}} [G : \mathrm{stab}_G(X)] \,. \tag{$*$}$$

Claim 1: For each $X \in \mathcal{M}$, we have $|\mathrm{stab}_G(X)| \mid p^b$. In fact, for fixed $X \in \mathcal{M}$, $H := \mathrm{stab}_G(X)$ acts on X by $(h, x) \mapsto hx$, where $h \in H$, $x \in X$. This action is free and the orbit equation for this action gives $|X| = |H| \cdot k$, if k is the number of H-orbits of X.

Claim 2: If $X \in \mathcal{M}$ with $|\mathrm{stab}_G(X)| = p^b$, then the G-orbit of X contains a subgroup of G. In fact, set $H := \mathrm{stab}_G(X)$ and choose any $x \in X$. Then we have $Hx \subseteq X$ and since $|H| = p^b = |X|$ we must have $Hx = X$. This implies that $x^{-1}Hx = x^{-1}X$ is a subgroup of G which is contained in the G-orbit of X.

Claim 3: If the G-orbit of $X \in \mathcal{M}$ contains a subgroup U of G, then the G-orbit of X is G/U and U is the only subgroup in this G-orbit. In fact, this is obvious.

Claim 4: One has

$$\binom{n}{p^b} \equiv p^{a-b} \cdot m \cdot s_{p^b}(G) \mod p^{a-b+1} \,. \tag{$**$}$$

In fact, by claims 1 and 2, for each $X \in \mathcal{R}$ the following holds: If the G-orbit of X does not contain a subgroup of G, then $|\mathrm{stab}_G(X)|$ divides p^{b-1}, and therefore $[G : \mathrm{stab}_G(X)] \equiv 0 \mod p^{a-b+1}$. By Claims 1, 2, and 3, the remaining G-orbits correspond bijectively to the set of subgroups of G of order p^b. Moreover, if X is in such an orbit, we have $[G : \mathrm{stab}_G(X)] = p^{a-b}m$. Now the claim follows from Equation $(*)$.

Claim 5: One has $s_{p^b}(G) \equiv 1 \mod p$. In fact, note that the Congruence $(**)$ holds for every group G with of order n. So it holds for the cyclic group of order n. But we know that a cyclic group of order n has precisely one subgroup of order p^b. This implies

$$p^{a-b}m \equiv \binom{n}{p^b} \equiv p^{a-b} \cdot m \cdot s_{p^b}(G) \mod p^{a-b+1} \,,$$

and therefore, $p^{a-b+1} \mid p^{a-b} \cdot m \cdot (s_{p^b}(G) - 1)$, which is equivalent to $p \mid m \cdot (s_{p^b}(G) - 1)$. Since p does not divide m, we obtain $p \mid (s_{p^b}(G) - 1)$, and part (a) is proved.

(b) and (c). Let $P \leqslant G$ such that $|P| = p^a$ and let $U \leqslant G$ such that $|U| = p^b$ for arbitrary $b \in \{0, \ldots, a\}$. We will show that there exists $g \in G$ with $U \leqslant gPg^{-1}$. This then implies (b) and (c). Consider the transitive conjugation action of G on the set $\Omega := \{gPg^{-1} \mid g \in G\}$. From $P \in \Omega$, $\mathrm{stab}_G(P) = N_G(P)$, and $p^a = |P| \mid |N_G(P)|$, we obtain that $\Omega = [G : N_G(P)]$ is not divisible by p. With G also U acts on Ω (but not necessarily transitive). The orbit equation for this action yields

$$|\Omega| = \sum_{Q \in \mathcal{R}} [U : \mathrm{stab}_U(Q)] \,,$$

where $\mathcal{R} \subseteq \Omega$ is a set of representatives for the U-orbits of Ω. Since p does not divide $|\Omega|$, we have $U = \mathrm{stab}_U(Q)$ for at least one $Q \in \Omega$. This implies $U \leqslant N_G(Q)$. It follows that UQ is a subgroup of $N_G(Q)$ with $Q \trianglelefteq UQ$. By the first Isomorphism Theorem we have $UQ/Q \cong U/U \cap Q$, and further, $|UQ| = |Q| \cdot |U/(U \cap Q)| = p^a \cdot |U/(U \cap Q)|$. Since $|U| = p^b$, the group UQ is a p-group, and since $p^{a+1} \nmid |G|$, we obtain $|U/(U \cap Q)| = 1$, and so $U \leqslant Q$. But since $Q \in \Omega$, $Q = gPg^{-1}$ for some $g \in G$, and the proof is complete. $\square$

3 Semidirect Products and Wreath Products

3.1 Definition Let G and S be groups. We say that S acts on G by group automorphisms, if S acts on G by an action $\varphi\colon S \times G \to G$ such that $\varphi(s, g_1 \cdot g_2) = \varphi(s, g_1) \cdot \varphi(s, g_2)$ (or ${}^s(g_1 \cdot g_2) = {}^s g_1 \cdot {}^s g_2$) for all $s \in S$ and $g_1, g_2 \in G$. Equivalently, the image of the corresponding homomorphism $\rho\colon S \to \mathrm{Sym}(G)$ is contained in $\mathrm{Aut}(G)$, the group of group automorphisms of G.

3.2 Theorem *Let $\varphi\colon S \times G \to G$ be an action of a group S on a group G via group automorphisms. Then the set $G \times S$ becomes a group under the multiplication*

$$(g, s) \times (h, t) := (g \cdot {}^s h, s \cdot t)$$

with identity element $(1_G, 1_S)$ and with inverse

$$(g, s)^{-1} = \left(g \cdot {}^{s^{-1}}(g^{-1}), s^{-1}\right),$$

for all $g, h \in G$ and $s, t \in S$. This group is called the semidirect product *of G and S with respect to φ and is denoted by $G \rtimes S$ (or $G \rtimes_\varphi S$ or $G \rtimes_\rho S$, if the action needs to be specified). The maps*

$$i_G\colon G \longrightarrow G \rtimes S, \quad g \mapsto (G, 1_S),$$
$$i_S\colon S \longrightarrow G \rtimes S, \quad s \mapsto (1_G, s),$$

are injective group homomorphisms and the map

$$p_S\colon G \rtimes S \longrightarrow S, \quad (g, s) \mapsto s,$$

is a surjective group homomorphism. Moreover,

$$i_G(G) \trianglelefteq G \rtimes S, \quad i_G(G) \cdot i_S(S) = G \rtimes S,$$
$$i_G(G) \cap i_S(S) = 1, \quad \ker(p_S) = i_G(G),$$

and

$$S \longrightarrow (G \rtimes S)/i_G(G), \quad s \mapsto (1_G, s) \cdot i_G(G),$$

is an isomorphism.

Proof Easy verifications. □

3.3 Theorem *Let Γ be a group, $G \trianglelefteq \Gamma$, and $S \leqslant \Gamma$ such that $G \cdot S = \Gamma$ and $G \cap S = 1$ (i.e., G is a normal complement of S in Γ and S is a complement of G in Γ). Then, with the conjugation action of S on G, one obtains an isomorphism*

$$f\colon G \rtimes S \longrightarrow \Gamma, (g, s) \mapsto gs.$$

Proof Let $g, h \in G$ and $s, t \in S$. Then

$$f((g,s)(h,t)) = f(g \cdot shs^{-1}, st) = gshs^{-1}st = gsht = f(g,s)f(h,t)\,,$$

showing that f is a homomorphism. Since $GS = \Gamma$, the homomorphism f is surjective. Moreover, if $f(g,s) = 1$ for $g \in G$ and $s \in S$, then $gs = 1 \in \Gamma$, and $g = s^{-}1 \in G \cap S = 1$. This implies $g = 1$ and also $s = 1$. □

3.4 Examples (a) For $n \in \mathbb{N}$, the dihedral group D_{2n} is a semidirect product $C_n \rtimes S$ with C_n the cyclic group of rotations and S any subgroup of order 2 generated by a reflection.

(b) For $n \geqslant 2$, the symmetric group $\mathrm{Sym}(n)$ is a semidirect product $\mathrm{Alt}(n) \rtimes S$ with S generated by any transposition.

(c) If a group S acts trivially on a group G, the resulting semidirect product is the direct product.

3.5 Remark Let Γ be a group and let $G \trianglelefteq \Gamma$. In general, G has no complement in Γ. But if there exists a complement of G in Γ, then any two such complements are isomorphic. However, if S is a subgroup of Γ, then in general not any two normal complements of S in Γ are isomorphic. (See Exercise 10)

3.6 Definition Let $n \in \mathbb{N}$, $H \leqslant \mathrm{Sym}(n)$, and let G be a group. The *wreath product* $G \wr H$ of G with H is the semidirect product $(G \times \cdots \times G) \rtimes H$, where H acts on the product $G \times \cdots \times G$ of n copies of G by

$$\sigma(g_1, \ldots, g_n) := (g_{\sigma^{-1}(1)}, \ldots, g_{\sigma^{-1}(n)})\,,$$

for $g_1, \ldots, g_n \in G$ and $\sigma \in H$. Note that $G \wr H$ depends on the number n and if there is any risk of confusion one has to specify in which symmetric group one wants H to be considered as a subgroup.

3.7 Examples (a) Let $n \in \mathbb{N}$ and let G be a subgroup of the multiplicative group of a field K. The set $\mathrm{Mon}_n(G)$, consisting of $n \times n$-matrices in $M_n(K)$ which have entries in $G \cup \{0\}$ and which have exactly one non-zero entry in each row and column, is a subgroup of $\mathrm{GL}_n(K)$. Moreover, it is not difficult to see that the map

$$G \wr \mathrm{Sym}(n) \longrightarrow \mathrm{Mon}_n(G)$$

which maps $((g_1, \ldots, g_n), \sigma)$ to the matrix whose j-th column has only one nonzero entry, namely $g_{\sigma(j)}$ in the $\sigma(j)$-th row, is an isomorphism.

More generally, if G is any group, one calls $\mathrm{Mon}(G) := G \wr \mathrm{Sym}(n)$ the *monomial group of G of degree n*. We write $\mathrm{Mon}(K)$ for the monomial group of $K^\times$ of degree n.

(b) We give other names to the places and sides on Rubik's cube, namely according to the following figure:

			5c	10y	6b						
			5y	**y**	6x						
			1b	2y	2c						
5b	5x	1c	1a	2x	2a	2b	6y	6c	6a	10x	5a
9y	**r**	1y	1x	**w**	3x	3y	**o**	11y	11x	**b**	9x
8c	8y	4b	4a	4x	3a	3c	7x	7b	7a	12x	8a
			4c	4y	3b						
			8x	**g**	7y						
			8b	12y	7c						

First note that each move of the cube takes little corner cubes to corner cubes and edge cubes to edge cubes. Mathematically, this means, the corresponding permutation lies in the subgroup $\mathrm{Sym}(\{1,\dots,24\}) \times \mathrm{Sym}(\{25,\dots,48\})$. But there are more restrictions. Considering the effect of moves to corner cubes one sees that on a coarse scale the eight corners $1,\dots,8$ are permuted and, on a more precise scale, simultaneously for each corner cube i, its sides (ia, ib, ic) go to some permutation of (ja, jb, jc) if j is the corner it is moved to. Therefore, for each $i = 1,\dots,8$ we obtain a permutation of $\{a, b, c\}$. Moreover, the permutation of the eight corners together with the eight permutations of $\{a, b, c\}$ determine the effect of a move on the corner cubes. This allows us to view the possible effects of a moves on the corner cubes as a subset of the set $(\mathrm{Sym}(\{a, b, c\}) \times \cdots \times \mathrm{Sym}(\{a, b, c\})) \times \mathrm{Sym}(8)$ which 8 copies of $\mathrm{Sym}(\{a, b, c\})$. More precisely, if $\sigma \in \mathrm{Sym}(8)$ describes the permutation of the 8 corner cubes, then we write the permutation of $\{a, b, c\}$ resulting from taking the i-corner to the $\sigma(i)$-th corner into the $\sigma(i)$-th component of $\mathrm{Sym}(\{a, b, c\}) \times \cdots \times \mathrm{Sym}(\{a, b, c\})$. Now one can check that the composition of moves corresponds to multiplication in the wreath product $\mathrm{Sym}(\{a, b, c\}) \wr \mathrm{Sym}(8)$. Similar considerations apply to the edge cubes, where the group $\mathrm{Sym}(\{x, y\}) \wr \mathrm{Sym}(12)$ arises. Altogether we can now view the group Ru as subgroup of the direct product

$$(\mathrm{Sym}(\{a, b, c\}) \wr \mathrm{Sym}(8)) \times (\mathrm{Sym}(\{x, y\}) \wr \mathrm{Sym}(12)) .$$

But we can say even more. When we look from the outside on corner cube, we chose the labels a, b, and c always in a way that they occur in clockwise orientation. Since each move does not change that orientation, we can replace $\mathrm{Sym}(\{a, b, c\})$ with $\mathrm{Alt}(\{a, b, c\})$. Writing C_3 instead of $\mathrm{Alt}(\{a, b, c\})$ and C_2 instead of $\mathrm{Sym}(\{x, y\})$, the moves of Rubik's cube form a subgroup Ru of the group

$$G := (C_3 \wr \mathrm{Sym}(8)) \times (C_2 \wr \mathrm{Sym}(12)) . \qquad (*)$$

The group G has order $3^8 \cdot 8! \cdot 2^{12} \cdot 12! = 2^{7+12+10} \cdot 3^{8+2+5} \cdot 5^{1+2} \cdot 7^{1+1} \cdot 11 = 2^{29} \cdot 3^{15} \cdot 5^3 \cdot 7^2 \cdot 11$. Comparing this with the order of Ru (calculated by GAP in Example 2.5(d)) we find $[G : Ru] = 12$. Denoting the permutation (a, b, c)

by σ and $(1,2)$ by τ we obtain new expressions for the 6 generators:

$$\begin{aligned}
r &= \big(((\sigma,1,1,\sigma^2,\sigma^2,1,1,\sigma),(1,5,8,4)),((1,1,1,1,\tau,1,1,1,\tau,1,1,1),(1,5,9,8))\big)\,,\\
y &= \big(((\sigma^2,\sigma,1,1,\sigma,\sigma^2,1,1),(1,2,6,5)),((1,1,1,1,1,\tau,1,1,1,\tau,1,1),(2,6,10,5))\big)\,,\\
w &= \big(((1,1,1,1,1,1,1,1),(1,4,3,2)),((1,1,1,1,1,1,1,1,1,1,1,1),(1,4,3,2))\big)\,,\\
g &= \big(((1,1,\sigma^2,\sigma,1,1,\sigma,\sigma^2),(3,4,8,7)),((1,1,1,1,1,1,1,\tau,1,1,1,\tau),(4,8,12,7))\big)\,,\\
o &= \big(((1,\sigma^2,\sigma,1,1,\sigma,\sigma^2,1),(2,3,7,6)),((1,1,1,1,1,1,\tau,1,1,1,\tau,1),(3,7,11,6))\big)\,,\\
b &= \big(((1,1,1,1,1,1,1,1),(5,6,7,8)),((1,1,1,1,1,1,1,1,1,1,1,1),(9,10,11,12))\big)\,.
\end{aligned}$$

Note that each of the generators and therefore each element

$$\big(((\lambda_1,\dots,\lambda_8),\pi),((\mu_1,\dots,\mu_{12}),\rho)\big) \in Ru$$

satisfies the conditions

$$\lambda_1\cdots\lambda_8 = 1\,,\quad \mu_1\cdots\mu_{12} = 1\,,\quad \operatorname{sgn}(\pi)\operatorname{sgn}(\rho) = 1\,. \tag{$**$}$$

It is easy to see that conversely, all elements of G satisfying the Conditions $(**)$ form a subgroup of G of index 12. In fact, it is easy to see that the map $G \to C_3 \times C_2 \times C_2$ which sends an element as above to $(\lambda_1\cdots\lambda_8, \mu_1\cdots\mu_{12}, \operatorname{sgn}(\pi)\operatorname{sgn}(\rho))$ is a surjective group homomorphism. This shows that we have now identified Ru as the subgroup consisting of those elements of G satisfying the Conditions $(**)$.

3.8 Remark (a) Let G, H, S, T be groups and let $\varphi\colon S \times G \to G$ and $\psi\colon T \times H \to H$ be actions via group automorphisms. Assume further that $\alpha\colon G \to H$ and $\beta\colon S \to T$ are group homomorphisms such that

$$\alpha(\varphi(s,g)) = \psi(\beta(s),\alpha(g)) \tag{$*$}$$

for all $s \in S$ and $g \in G$. Then the map

$$\gamma\colon G \rtimes_\varphi S \to H \rtimes_\psi T\,,\quad (g,s) \mapsto (\alpha(g),\beta(s))\,,$$

is a group homomorphism. In fact, for $s_1, s_2 \in S$ and $g_1, g_2 \in G$, we have

$$\begin{aligned}
\gamma((g_1,s_1)(g_2,s_2)) &= \gamma(g_1\cdot\varphi(s_1,g_2), s_1s_2) = \big(\alpha(g_1\cdot\varphi(s_1,g_2)),\beta(s_1s_2)\big)\\
&= \big(\alpha(g_1)\alpha(\varphi(s_1,g_2)),\beta(s_1)\beta(s_2)\big)\\
&= \big(\alpha(g_1)\psi(\beta(s_1),\alpha(g_2)),\beta(s_1)\beta(s_2)\big)\\
&= (\alpha(g_1),\beta(s_1))(\alpha(g_2),\beta(s_2)) = \gamma(g_1,s_1)\gamma(g_2,s_2)\,.
\end{aligned}$$

Moreover, if α and β are isomorphisms, then so is γ.

(b) Let $p < q$ be primes such that $p \mid q-1$, let $G =< g >, H =< h >$ be groups of order q, and let $S =< s >$ and $T =< t >$ be groups of order

p. Then, there is an isomorphism $(\mathbb{Z}/q\mathbb{Z})^\times \cong \mathrm{Aut}(G)$ taking a unit $a+q\mathbb{Z}$ to the automorphism σ_a which is given by raising every element of G to its a-th power. The same holds for $\mathrm{Aut}(H)$. Moreover, $\mathrm{Aut}(G)$, $\mathrm{Aut}(H)$, and $(\mathbb{Z}/q\mathbb{Z})^\times$ are cyclic of order $q-1$ and have a unique subgroup of order p. Let $a+q\mathbb{Z}, b+q\mathbb{Z} \in (\mathbb{Z}/q\mathbb{Z})^\times$ be two generators of the subgroup of $(\mathbb{Z}/q\mathbb{Z})^\times$ of order p and consider the actions $\varphi\colon S \times G \to G$ and $\psi\colon T \times H \to H$ given by

$$\varphi(s^m, g^n) := g^{na^m}, \quad \psi(t^m, h^n) := h^{nb^m},$$

for $m, n \in \mathbb{Z}$, or equivalently by mapping s to the automorphism σ_a on G and t to the automorphism σ_b on H. Note that any non-trivial action is of that form. There exist $k, l \in \mathbb{Z}$ such that $a^k + q\mathbb{Z} = b + q\mathbb{Z}$ and $b^l + q\mathbb{Z} = a + q\mathbb{Z}$. Now the isomorphisms given by $\alpha\colon G \to H$, $g \mapsto h$, and $\beta\colon S \to T$, $s \mapsto t^l$, satisfy Equation $(*)$. In fact,

$$\alpha(\varphi(s^m, g^n)) = \alpha(g^{na^m}) = h^{na^m}$$

and

$$\psi(\beta(s^m), \alpha(g^n)) = \psi(t^{ml}, h^n) = h^{nb^{ml}} = h^{na^m},$$

since $b^l \equiv a \mod q$.

These considerations show that any two non-trivial actions of groups of order p on groups of order q (with p and q as above) lead to isomorphic semidirect products.

3.9 Theorem *Let p and q be primes and assume $p < q$.*

(a) If p does not divide $q-1$, there is only one isomorphism class of groups of order pq, namely the one of the cyclic group.

(b) If p divides $q-1$, there are two isomorphism classes of groups of order pq. One is represented by the cyclic group, the other one by a semidirect product $\mathbb{Z}/q\mathbb{Z} \rtimes \mathbb{Z}/p\mathbb{Z}$ with $\mathbb{Z}/p\mathbb{Z}$ acting non-trivially on $\mathbb{Z}/q\mathbb{Z}$.

Proof Assume that G is a group of order pq. From Sylow's Theorem it follows that G has a normal Sylow q-subgroup. In fact, the number of conjugates of a Sylow q-subgroup Q is $[G : N_G(Q)]$ and also congruent to 1 modulo q. Since $[G : N_G(Q)]$ divides $[G : Q] = p$, this number has to be 1. Therefore, $Q \lhd G$. Let P be Sylow p-subgroup of G. Then P is a complement of Q and G is isomorphic to the semidirect product $Q \rtimes P$ with respect to the conjugation action of P on Q. Note that $|\mathrm{Aut}(Q)| = q-1$. If $p \nmid q-1$, then every action of P on Q is trivial, and therefore $G \cong Q \times P$ is a cyclic group. If $p \mid q-1$, then there are two cases. In case P acts trivially on Q, again G is cyclic. In case P acts non-trivially on Q, the group G is not abelian (and therefore not cyclic) and isomorphic to a semidirect product as in Remark 3.8(b). Finally note that, by Remark 3.8(b), any two non-trivial actions of P on Q lead to isomorphic semidirect products. This completes the proof. □

4 Subnormal Series and the Jordan-Hölder Theorem

4.1 Definition Let G be a group. A subgroup H of G is called a *characteristic* subgroup of G, if $f(H) = H$ for all $f \in \mathrm{Aut}(G)$. It is equivalent to require only $f(H) \leqslant H$ for all $f \in \mathrm{Aut}(G)$. (Note that every characteristic subgroup of G is normal in G.)

4.2 Example For every group G its center $Z(G)$ and its commutator subgroup G' is characteristic in G.

4.3 Remark Let G be a group and let S be group acting on G via group automorphisms. In that situation we call G an *S-group*.

(a) Any subgroup $H \leqslant G$ which is stable under S (i.e., ${}^sH = H$ for all $s \in S$, or equivalently ${}^sH \subseteq H$ for all $s \in S$) will be called an *S-subgroup*. We will be mostly interested in the cases $S = \{1\}$, $S = G$ acting via conjugation, and $S = \mathrm{Aut}(G)$ acting in the obvious way by $(f, g) \mapsto f(g)$ for $f \in \mathrm{Aut}(G)$ and $g \in G$. In these three cases, the S-subgroups of G are respectively all the subgroups of G, the normal subgroups of G, and the characteristic subgroups of G.

(b) Let also H be an S-group. We call an S-equivariant map $f\colon G \to H$ an *S-homomorphism* if f is also a group homomorphism. G and H are called isomorphic S-groups, if there exists an S-isomorphism (i.e., a bijective S-homomorphism) between them. The kernel and image of an S-homomorphism is an S-stable subgroup.

(c) If U_i, $i \in I$, are S-subgroups of G, then also $\bigcap_{i\in I} U_i$ and $\langle \bigcup_{i\in I} U_i \rangle$.

(d) Let $U \trianglelefteq H$ be S-subgroups of G, then it is easy to see that the action of S on H induces an action of S on H/U, namely $(s, hU) \mapsto ({}^sh)U$, so that H/U is again an S-group. Moreover, the natural epimorphism $H \twoheadrightarrow H/U$ is an S-homomorphism.

4.4 Theorem (Homomorphism Theorem) *Let S be a group and let $f\colon G \to H$ be an S-homomorphism between two S-groups. Moreover, let $N \trianglelefteq G$ be an S-subgroup containing* $\ker(f)$. *Then there exists a unique S-homomorphism $\overline{f}\colon G/N \to H$ such that $\overline{f}(gN) = f(g)$ for all $g \in G$.*

Proof As for the usual homomorphism theorem. The only thing one has to show additionally is that $\overline{f}$ is an S-homomorphism. But for $g \in G$ and $s \in S$ we have $\overline{f}({}^s(gN)) = \overline{f}(({}^sg)N) = f({}^sg) = {}^sf(g) = {}^s\overline{f}(gN)$. □

4.5 Theorem (First Isomorphism Theorem) *Let G be an S-group and let U, V be S-subgroups such that $U \leqslant N_G(V)$. Then $UV = VU \leqslant G$, $U \cap V \trianglelefteq U$, $V \trianglelefteq UV$, and the inclusion $U \to UV$ induces an S-isomorphism*

$$U/U \cap V \longrightarrow UV/V\,, \quad u(U \cap V) \mapsto uV\,.$$

Proof As for the usual First Isomorphism Theorem and by observing that all the involved homomorphisms are S-homomorphisms. □

4.6 Theorem (Second Isomorphism Theorem) *Let G be an S-group, and let $N \trianglelefteq G$ and $H \trianglelefteq G$ be S-subgroups with $N \leqslant H$. Then $H/N \trianglelefteq G/N$ and the canonical map $G/N \to G/H$, $gN \mapsto gH$ induces an S-isomorphism*

$$(G/N)/(H/N) \longrightarrow G/H\,, \quad (gN)(H/N) \mapsto gH\,.$$

Proof As for the usual Second Isomorphism Theorem and by observing that all involved homomorphisms are S-homomorphisms. □

4.7 Lemma (Dedekind Identity) *Let G be a group and let $U, V, W \leqslant G$ such that $U \leqslant W$. Then*

$$(UV) \cap W = U(V \cap W) \quad \textit{and} \quad W \cap (VU) = (W \cap V)U\,.$$

Proof We only prove the first equation. The proof for the second one is similar. Let $w \in (UV) \cap W$. Then there exist $u \in U$ and $v \in V$ with $w = uv$. It follows from $U \leqslant W$ that $v = u^{-1}w \in V \cap W$, and therefore, $w = uv \in U(V \cap W)$. Conversely let $u \in U$ and $v \in V \cap W$. Then $uv \in UV$ and $uv \in UW = W$. □

4.8 Theorem (Third Isomorhism Theorem or Butterfly Lemma) *Let S be a group, let G be an S-group and let $U, V \leqslant G$ be S-subgroups. Moreover, let $U_0 \trianglelefteq U$ and $V_0 \trianglelefteq V$ be S-subgroups. Then*

(a) *$U_0(U \cap V_0) \trianglelefteq U_0(U \cap V)$, $V_0(U_0 \cap V) \trianglelefteq V_0(U \cap V)$, $(U_0 \cap V)(U \cap V_0) \trianglelefteq (U \cap V)$, and all these subgroups are S-subgroups of G.*

(b) *$U_0(U \cap V)/U_0(U \cap V_0) \cong V_0(U \cap V)/V_0(U_0 \cap V) \cong (U \cap V)/(U_0 \cap V)(U \cap V_0)$ as S-groups.*

Proof Since $U_0 \trianglelefteq U$ we have $U_0(U \cap V_0) \leqslant U$ and $U_0(U \cap V) \leqslant U$. Moreover it is easy to verify that $U \cap V_0 \trianglelefteq U \cap V$. Therefore, and by the First Isomorphism Theorem we have for each $u_0 \in U_0$ and $x \in U \cap V$:

$$\begin{aligned} u_0 x U_0 (U \cap V_0) x^{-1} u_0^{-1} &= u_0 U_0 x x^{-1} (U \cap V_0) u_0^{-1} = U_0 (U \cap V_0) u_0^{-1} \\ &= (U \cap V_0) U_0 u_0^{-1} = (U \cap V_0) U_0 = U_0 (U \cap V_0)\,. \end{aligned}$$

This implies $U_0(U \cap V_0) \trianglelefteq U_0(U \cap V)$.

Next, consider the S-homomorphism

$$f\colon U \cap V \hookrightarrow U_0(U \cap V) \twoheadrightarrow U_0(U \cap V)/U_0(U \cap V_0)\,,$$

the composition of the inclusion and the natural epimorphism. We have

$$\ker(f) = U_0(U \cap V_0) \cap (U \cap V) = (U_0 \cap U \cap V)(U \cap V_0) = (U_0 \cap V)(U \cap V_0)\,,$$

and so $(U_0 \cap V)(U \cap V_0) \trianglelefteq (U \cap V)$. Moreover, f is surjective, since for $u_0 \in U_0$ and $x \in U \cap V$ we have

$$u_0 x U_0 (U \cap V_0) = x x^{-1} u_0 x U_0 (U \cap V_0) = x U_0 (U \cap V_0) = f(x)\,,$$

and by the Homomorphism Theorem be obtain one of the desired S-isomorphisms. The rest is proved in the same way by exchanging the roles of U and V. □

4.9 Definition Let G and S be groups and assume that S acts on G via group automorphisms.

An *S-subnormal series* of G is a chain of S-subgroups

$$1 = G_0 \trianglelefteq G_1 \trianglelefteq \cdots G_{n-1} \trianglelefteq G_n = G \qquad (*)$$

of G with $G_{i-1} \trianglelefteq G_i$ for each $i = 1, \ldots, n$. The number n is called the *length* of the series and the S-groups G_i/G_{i-1} are called the *factors* of the series in $(*)$. Two S-subnormal series of G are called *S-equivalent*, if they have the same length and if their factors are S-isomorphic possibly after reordering them. The series is called *proper* if $G_{i-1} \neq G_i$ for all $i = 1, \ldots, n$. An S-subnormal series of G is called a *refinement* of $(*)$ if it also contains all the subgroups $G_0, G_1, \ldots, G_{n-1}, G_n$. A proper S-subnormal series of G is called an *S-composition series* of G if it cannot be refined to a proper S-subnormal series of G (by inserting an additional subgroup).

If $S = 1$ we omit the S in all the above notations.

If $S = G$ acting by conjugation, an S-subnormal series is called a *normal series* of G.

If $S = \mathrm{Aut}(G)$ acting in the natural way on G, and S-subnormal series is called a *characteristic series* of G.

4.10 Remark Note that a S-subnormal $(*)$ is a composition series if and only if G_i/G_{i-1} is an S-simple group (i.e., does not have another normal S-subgroup than 1 and G_i/G_{i-1}. In fact, every normal subgroup of G_i/G_{i-1} is of the form H/G_{i-1} for some subgroup $G_{i-1} \leqslant H \leqslant G_i$, H is normal in G_i if and only if H/G_{i-1} is normal in G_i/G_{i-1}, and H is an S-subgroup of G_i (or equivalently of G) if and only if H/G_{i-1} is an S-subgroup of G_i/G_{i-1}.

Note that any finite S-group has an S-composition series. We will see later that any two are equivalent.

4.11 Theorem (Refinement Theorem of Schreier) *Let S be a group and let G be an S-group. Then any two S-subnormal series of G have S-equivalent refinements.*

Proof Let $1 = G_0 \leqslant \cdots \leqslant G_n = G$ and $1 = H_0 \leqslant \cdots H_m = G$ be two S-subnormal series of G. Between G_{i-1} and G_i $(i = 1, \ldots, n)$ we insert the S-subgroups

$$G_{i-1} = G_{i-1}(G_i \cap H_0) \leqslant G_{i-1}(G_i \cap H_1) \leqslant \cdots \leqslant G_{i-1}(G_i \cap H_m) = G_i$$

and between H_{j-1} and H_j $(j = 1, \ldots, m)$ we insert the S-subgroups

$$H_{j-1} = H_{j-1}(H_j \cap G_0) \leqslant H_{j-1}(H_j \cap G_1) \leqslant \cdots \leqslant H_{j-1}(H_j \cap G_n) = H_j\,.$$

From the Third Isomorphism Theorem it follows that the resulting two chains of subgroups are S-subnormal series of G and that they are equivalent, since

$$G_{i-1}(G_i \cap H_j)/G_{i-1}(G_i \cap H_{j-1}) \cong H_{j-1}(H_j \cap G_i)/H_{j-1}(H_j \cap G_{i-1})$$

as S-groups for all $i = 1, \ldots, n$ and $j = 1, \ldots, m$. □

4.12 Theorem (Jordan-Hölder) *Any two S-composition series of an S-group G are S-equivalent.*

Proof This follows from applying Schreier's Refinement Theorem to two S-composition series of G and omitting repetitions in the obtained series. □

4.13 Definition Let G be an S-group. The length of an S-composition series of G is called the *S-composition length* of G and its factors are called the *S-composition factors* of G. By the theorem of Jordan-Hölder, these notions are well-defined.

If $S = 1$ we speak of a *composition series*, the *composition length*, and the *composition factors* of G

If $S = G$ with the conjugation on G we call an S-composition series also a *chief series*, its length the *chief length* and its factors the *chief factors* of G.

If $S = \mathrm{Aut}(G)$ and S acts in the natural way we call the length of an S-composition series of G the *characteristic length*, and its factors the *characteristic factors* of G.

4.14 Examples (a) For any simple group G, the only existing proper subnormal series is $1 < G$ and this is also a composition series. Its composition length is 1 and its single composition factor is G.

(b) The subnormal series $1 < \mathrm{Alt}(3) < \mathrm{Sym}(3)$ is a composition series of $\mathrm{Sym}(3)$. Its length is 2 and its composition factors are isomorphic to the cyclic group of order 2 and of order 3. The cyclic group $C_6 = \langle x \rangle$ of order 6 has the same composition factors. Moreover, C_6 has two composition series, namely $1 < \langle x^2 \rangle < C_6$ and $1 < \langle x^3 \rangle < C_6$. The composition series of $\mathrm{Sym}(3)$ and C_6 above are also chief series and characteristic series.

(c) Let $G := \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ for a prime p. Then any of the $p+1$ subgroups H of order p leads to a composition series $1 < H < G$. These are all the composition series and they are also all the chief series of G. But they are not characteristic series. In fact, G is characteristicly simple (i.e., of characteristic length 1), since for each such H there exists a complement U and an automorphism of G mapping H to U and U to H. Therefore, the characteristic factors of G are just G.

5 Solvable Groups

5.1 Definition A group G is called *solvable*, if G has a subnormal series

$$1 = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_n = G \qquad (*)$$

with abelian factors G_i/G_{i-1}, $i = 1, \ldots, n$.

5.2 Remark (a) Each abelian group and each group of prime power order is solvable. In fact, for an abelian group G, $1 \leqslant G$ is a subnormal series with abelian factors, and for a p-group G, p a prime, we can use the fact that G has a subgroup of index p and that such a subgroup is normal in G.

(b) If G is a finite group, then it follows from the Second Isomorphism Theorem that G is solvable if and only if G has even a subnormal series $(*)$ with cyclic factors. Then we can find elements $g_i \in G_i$, $i = 1, \ldots, n$, such that $\langle g_i G_{i-1} \rangle = G_i/G_{i-1}$ for all $i = 1, \ldots, n$. If we set $a_i := |G_i/G_{i-1}|$, then every element $g \in G$ can be written as

$$g = g_n^{k_n} g_{n-1}^{k_{n-1}} \cdots g_1^{k_1} \text{ with } 0 \leqslant k_i < a_i \text{ for } i = 1, \ldots, n\,.$$

Moreover, the exponents $k_1, \ldots, k_n$ are unique, since $|G| = |G_n/G_{n-1}| \cdots |G_1/G_0| = a_n \cdots a_1$. Furthermore there exist unique numbers $0 \leqslant r_{i,j}^{(k)}, s_{i,j} < a_j$, for $1 \leqslant j, k < i \leqslant n$, such that

$$g_i^{-1} g_k g_i = g_{i-1}^{r_{i,i-1}^{(k)}} \cdot g_{i-2}^{r_{i,i-2}^{(k)}} \cdots g_1^{r_{i,1}^{(k)}} \text{ and } g_i^{a_i} = g_{i-1}^{s_{i,i-1}} \cdots g_1^{s_{i,1}}\,, \qquad (1)$$

for all $1 \leqslant j, k < i \leqslant n$. Using the relations in (1), one can transform any product of the elements g_i, $i = 1, \ldots, n$, into the form $g_n^{k_n} \cdots g_1^{k_1}$, by using

$$g_k g_i = g_i g_{i-1}^{r_{i,i-1}^{(k)}} \cdot g_{i-2}^{r_{i,i-2}^{(k)}} \cdots g_1^{r_{i,1}^{(k)}}$$

whenever $k < i$ in order to move all powers of g_n to the left, then then all powers of g_{n-1}, etc.

Conversely, if G is generated by elements $g_1, \ldots, g_n$ and there exist relations of the form (1), then G is solvable, since the subgroups $G_i := \langle g_1, \ldots, g_i \rangle$, $i = 1, \ldots, n$, form a subnormal series with cyclic factors.

5.3 Definition Let G be a group. For $x, y \in G$, we call

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

the *commutator* of x and y. More general for subsets $X, Y \subseteq G$ we define

$$[X, Y] := \langle \{[x, y] \mid x \in X, y \in Y\} \rangle\,.$$

The *commutator subgroup* or *derived subgroup* of G is defined as $[G, G]$ and denoted by G'. Inductively, we define for each $n \in \mathbb{N}$ the *n-th commutator subgroup* or *n-th derived subgroup* $G^{(n)}$ of G by $G^{(0)} := G$ and $G^{(n)} := [G^{(n-1)}, G^{(n-1)}] = (G^{(n-1)})'$, for $n \geqslant 1$; in particular $G^{(1)} = G'$.

5.4 Remark Let G be a group.

(a) For $x, y \in G$ we have $xy = [x, y]yx$, i.e., $[x, y] = 1$ if and only if $xy = yx$.

(b) In general, the subset $[X, Y]$ of G is not a subgroup not even if X and Y are subgroups of G. Note that $[X, Y] = [Y, X]$, since for each $x \in X$ and $y \in Y$ one has $[y, x] = [x, y]^{-1}$.

(c) For $f \in \mathrm{Aut}(G)$ and $x, y \in G$ we have $f([x, y]) = f(x)f(y)f(x^{-1})f(y^{-1}) = [f(x), f(y)]$. In particular $f(G') \leqslant G'$, and therefore, G' is characteristic. By induction on n, $G^{(n)}$ is characteristic in G for all $n \in \mathbb{N}_0$. In particular, $G^{(n)}$ is normal in G for all $n \in \mathbb{N}_0$.

(d) Recall that G/G' is abelian (in fact, $[xG', yG'] = [x, y]G' = G'$ for all $x, y \in G$), and that the normal subgroups $N \trianglelefteq G$ with abelian factor group G/N are exactly the subgroup of G containing G'. The abelian group $G^{\mathrm{ab}} := G/G'$ is called the *commutator factor group* of G.

5.5 Theorem *Let G be a group. Then the following are equivalent:*

(i) *G is solvable.*

(ii) *There exists $n \in \mathbb{N}_0$ such that $G^{(n)} = 1$.*

(iii) *G has a normal series with abelian factors.*

Proof (i) $\Rightarrow$ (ii): Let $1 = G_n \trianglelefteq G_{n-1} \trianglelefteq \cdots \trianglelefteq G_0 = G$ be a subnormal series of G with abelian factors. We show by induction on k that $G^{(k)} \leqslant G_k$. Obviously, this holds for $k = 0$. Assume we have proved the claim for $k \in \mathbb{N}_0$. Then the inclusion $G^{(k)} \leqslant G_k$ induces a map $G^{(k)} \to G_k/G_{k+1}$, $x \mapsto xG_{k+1}$. By the Homomorphism Theorem we obtain a monomorphism $G^{(k)}/(G^{(k)} \cap G_{k+1}) \to G_k/G_{k+1}$. With G_k/G_{k+1} also $G^{(k)}/(G^{(k)} \cap G_{k+1})$ is abelian. This implies $G^{(k+1)} \leqslant G^{(k)} \cap G_{k+1} \leqslant G_{k+1}$.

(ii) $\Rightarrow$ (iii): Assuming (ii), the chain $1 = G^{(n)} \leqslant G^{(n-1)} \leqslant \cdots \leqslant G^{(1)} \leqslant G^{(0)} = G$ is a normal chain of G and it has abelian factors.

(iii) $\Rightarrow$ (i): This is obvious. □

5.6 Remark (a) The example $G := \mathrm{Alt}(4)$ shows that a finite solvable group has in general no normal series with cyclic factors, since 1, $V_4 := \langle (1,2)(3,4), (1,3)(2,4) \rangle$, and G are the only normal subgroups of G. If a group G has a normal series with cyclic factors, then we call G *supersolvable*. Obviously every supersolvable group is solvable.

(b) If G is a group and $H \leqslant G$, then obviously $H' \leqslant G'$. By induction on n we obtain $H^{(n)} \leqslant G^{(n)}$ for all $n \in \mathbb{N}_0$. Therefore, Theorem 5.5 implies that each subgroup of a solvable group is again solvable.

(c) If G is a group and $N \trianglelefteq G$, then $(G/N)' = G'N/N$, since $xNyN(xN)^{-1}(yN)^{-1} = [x, y]N$ for all $x, y \in G$. By induction on n we obtain $(G/N)^{(n)} = G^{(n)}N/N$ for all $n \in \mathbb{N}_0$. Therefore, Theorem 5.5 implies that each factor group of a solvable group is solvable.

(d) Recall that for a group G and $N \trianglelefteq G$ one has: G is solvable if and only if N and G/N are solvable. In fact, (b) and (c) show that with G also N and G/N are solvable. Conversely, if $1 = N_0 \leqslant N_1 \leqslant \cdots \leqslant N_k = N$ and

$1 = U_0/N \leqslant U_1/N \leqslant \cdots \leqslant U_l/N = G/N$ are subnormal series with abelian factors, then $1 = N_0 \leqslant \cdots \leqslant N_k = U_0 \leqslant \cdots \leqslant U_l = G$ is a subnormal series of G with abelian factors.

5.7 Theorem *A finite group G is solvable if and only if its composition factors are cyclic of prime order.*

Proof If G is solvable there exists a subnormal series of G with cyclic factors (see Remark 5.2(b)). Refining this series to a composition series shows that the composition factors of G are cyclic and of prime order (since they are simple). Conversely, if G has a composition series with cyclic factors, then G is by definition solvable. □

6 Nilpotent Groups

6.1 Definition A normal series

$$1 = G_0 \leqslant \cdots \leqslant G_n = G \qquad (*)$$

of a group G is called a *central series* of G if $G_i/G_{i-1} \leqslant Z(G/G_{i-1})$ for all $i = 1, \ldots, n$. If G has a central series, we call G *nilpotent.*

6.2 Remark Let G be a group.

(a) A normal series $(*)$ of G is a central series if and only if $[G_i, G] \leqslant G_{i-1}$ for all $i = 1, \ldots, n$. In fact, we have: $G_i/G_{i-1} \leqslant Z(G/G_{i-1}) \iff gG_{i-1} \in Z(G/G_{i-1})$ for all $g \in G_i \iff 1 = [gG_{i-1}, xG_{i-1}] = [g,x]G_{i-1}$ for all $g \in G_i$ and $x \in G \iff [g,x] \in G_{i-1}$ for all $g \in G_i$ and $x \in G \iff [G_i, G] \leqslant G_{i-1}$.

(b) By Theorem 2.9, each p-group is nilpotent. Moreover, each abelian group G is nilpotent, since $1 \leqslant G$ is a central series. On the other hand, each nilpotent group is supersolvable, since every central series can be refined to a normal series with cyclic factors.

6.3 Definition For a group G one defines its *upper* (or *ascending*) *central series*

$$1 = Z^0(G) \leqslant Z^1(G) \leqslant \cdots \leqslant G$$

by

$$Z^0(G) = 1 \text{ and } Z^i(G)/Z^{i-1}(G) = Z(G/Z^{i-1}(G)) \text{ for } i \geqslant 1\,,$$

and its *lower* (or *descending*) *central series*

$$1 \leqslant \cdots \leqslant Z_1(G) \leqslant Z_0(G) = G$$

by

$$Z_0(G) = G \text{ and } Z_i(G) = [Z_{i-1}(G), G] \text{ for } i \geqslant 1\,.$$

6.4 Remark Let G be a group.

(a) One has $Z_1(G) = G'$ and $Z^1(G) = Z(G)$.

(b) It is not difficult to see by induction on i that $Z_i(G)$ and $Z^i(G)$, $i \in \mathbb{N}_0$, are characteristic subgroups of G.

(c) If $Z^n(G) = G$ (resp. $Z_n(G) = 1$) for some $n \in \mathbb{N}_0$ then the upper (resp. lower) central series truncated after $Z^n(G)$ (resp. $Z_n(G)$) is a central series. If $Z^{i+1}(G) = Z^i(G)$ (resp. $Z_{i+1}(G) = Z_i(G)$) for some $i \in \mathbb{N}_0$, then $Z^{i+n}(G) = Z^i(G)$ (resp. $Z_{i+n}(G) = Z_i(G)$) for all $n \in \mathbb{N}_0$.

The following theorem explains the names *upper* and *lower* central series.

6.5 Theorem *Let $1 = N_0 \leqslant N_1 \leqslant \cdots \leqslant N_r = G$ be a central series of a group G. Then one has*

$$Z_{r-i} \leqslant N_i \leqslant Z^i(G)$$

for all $i = 0, \ldots, r$. In particular, $Z_r(G) = 1$ and $Z^r(G) = G$. Furthermore, $Z_c(G) = 1$ if and only $Z^c(G) = G$ for any $c \in \mathbb{N}_0$. The smallest $c \in \mathbb{N}_0$ with this property is called the nilpotency class *of G.*

Proof First we show $N_i \leqslant Z^i(G)$ by induction on i. For $i = 0$ the statement is trivial. Assume that $N_i \leqslant Z^i(G)$ holds for some $i \in \mathbb{N}_0$. Then, for all $x \in N_{i+1}$ and $g \in G$, we have

$$[gZ^i(G), xZ^i(G)] = [g, x]Z^i(G) \subseteq N_i Z^i(G) = Z^i(G)\,,$$

which implies that $xZ^i(G) \in Z(G/Z^i(G))$ and $x \in Z^{i+1}(G)$.

Next we show $Z_{r-i}(G) \leqslant N_i$ by induction on $r - i$. For $i = r$ the assertion is trivial. Assume that $Z_{r-i}(G) \leqslant N_i$ for some $0 < i \leqslant r$. Then, for all $x \in Z_{r-i}(G)$ and $g \in G$ we have

$$[g, x]N_{i-1} = [gN_{i-1}, xN_{i-1}] = N_{i-1}\,,$$

since $x \in N_i$ and N_i/N_{i-1} is central in G/N_{i-1}. This implies $Z_{r-i+1}(G) \leqslant N_{i-1}$.

The remaining assertions are now immediate. □

6.6 Lemma *Let G be a finite group, p a prime, $P \leqslant G$ a Sylow p-subgroup of G, and $N_G(P) \leqslant U \leqslant G$. Then $N_G(U) = U$.*

Proof Let $g \in N_G(U)$. Then $gPg^{-1} \leqslant gUg^{-1} = U$ so that gPg^{-1} and P are Sylow p-subgroups of U. Therefore, there exists $u \in U$ with $ugPg^{-1}u^{-1} = P$. This implies $ug \in N_G(P) \leqslant U$ and $g \in u^{-1}U = U$. □

6.7 Theorem *For every finite group G the following are equivalent:*

(i) *G is nilpotent.*
(ii) *$Z_n(G) = 1$ for some $n \in \mathbb{N}_0$.*
(iii) *For all $U < G$ one has $U < N_G(U)$.*
(iv) *Every maximal subgroup of G is normal in G.*
(v) *Every Sylow subgroup of G is normal in G.*
(vi) *G is isomorphic to the direct product of its Sylow subgroups.*
(vii) *$Z(G/N) > 1$ for each proper normal subgroup $N \triangleleft G$.*
(viii) *$Z^n(G) = G$ for some $n \in \mathbb{N}_0$.*
(ix) *If $x, y \in G$ have coprime order, then $xy = yx$.*

Proof (i) $\Rightarrow$ (ii): Let $1 = N_0 \leqslant \cdots \leqslant N_r = G$ be a central series of G. Then by Theorem 6.5 we have $Z_r(G) \leqslant N_0 = 1$ and $Z_r(G) = 1$.

(ii) $\Rightarrow$ (iii): Let $i \in \mathbb{N}$ be such that $Z_i(G) \leqslant U$ but $Z_{i-1}(G) \not\leqslant U$. Then, for all $z \in Z_{i-1}(G)$ and $u \in U$, we have:

$$zuz^{-1}u^{-1} = [z,u] \in [Z_{i-1}(G), G] = Z_i(G) \leqslant U\,,$$

and therefore, $zuz^{-1} \in U$. This implies $U < U \cdot Z_{i-1}(G) \leqslant N_G(U)$.

(iii) $\Rightarrow$ (iv): Let $U < G$ be a maximal subgroup. Then, by (iii), $U < N_G(U) \leqslant G$ and $N_G(U) = G$.

(iv) $\Rightarrow$ (v): Let p be a prime divisor of $|G|$ and let P be a Sylow p-subgroup of G. Assume that P is not normal in G. Then $N_G(P) < G$ and there exists a maximal subgroup U of G with $N_G(P) \leqslant U$. By Lemma 6.6 we have $N_G(U) = U$ which contradicts (iv). Therefore, P is normal in G.

(v) $\Rightarrow$ (vi): We may assume that $G \neq 1$, since obviously all the nine conditions hold for the trivial group. Let $p_1, \ldots, p_r$ be the prime divisors of $|G|$ and let P_i be the unique Sylow p_i-subgroup of G for $i = 1, \ldots, r$. Consider the map

$$f\colon P_1 \times \cdots \times P_r \longrightarrow G\,, \quad (x_1, \ldots, x_r) \mapsto x_1 \cdots x_r\,.$$

We will show that f is an isomorphism. If $r = 1$, this is clear. So we assume that $r \geqslant 2$. Let $i \neq j$ be elements of $\{1, \ldots, r\}$ and let $x \in P_i$ and $y \in P_j$. Then $[x,y] = xyx^{-1}y^{-1} \in P_i \cap P_j = 1$, which implies that f is a homomorphism. For each $i = 1, \ldots, r$, the group P_i is contained in the image of f. Therefore, $|\mathrm{im}(f)|$ is divisible by $|P_i|$ for each $i = 1, \ldots, r$. This implies that g is surjective. Comparing orders, one also obtains that f is injective.

(vi) $\Rightarrow$ (vii): From (vi) we may assume that $G = P_1 \times \cdots \times P_r$ with p_i-groups P_i for pairwise distinct primes $p_1, \ldots, p_r$. Considering the Sylow p_i-subgroups of N one easily sees that $N = Q_1 \times \cdots \times Q_r$ with $Q_i \trianglelefteq P_i$ for $i = 1, \ldots, r$. Moreover $Q_{i_0} < P_{i_0}$ for some $i_0 \in \{1, \ldots, r\}$. By Theorem 2.9 we have $Z(P_{i_0}/Q_{i_0}) = R_{i_0}/Q_{i_0}$ with $Q_{i_0} < R_{i_0}$. Therefore,

$$Z(G/N) \geqslant (Q_1 \times \cdots \times R_{i_0} \times \cdots \times Q_r)/(Q_1 \times \cdots \times Q_r) > 1\,.$$

(vii) $\Rightarrow$ (viii): Using (vii), for all $i \in \mathbb{N}_0$ with $Z^i(G) < G$, we have $Z^{i+1}(G) > Z^i(G)$. Since G is finite, $Z^n(G) = G$ for some $n \in \mathbb{N}_0$.

(viii) $\Rightarrow$ (i): This follows from Remark 6.4(c).

(vi) $\Rightarrow$ (ix): We may assume that $G = P_1 \times \cdots \times P_r$ with p_i-groups P_i for pairwise distinct primes $p_1, \ldots, p_r$. If $x = (x_1, \ldots, x_r)$ and $y = (y_1, \ldots, y_r)$ are elements of G with coprime order, then for each $i = 1, \ldots, r$ we have $x_i = 1$ or $y_i = 1$. This implies immediately that $xy = yx$.

(ix) $\Rightarrow$ (v): Let p be a prime divisor of $|G|$ and let P be a p-Sylow subgroup of G. For any other prime divisor $q \neq p$ and any Sylow q-subgroup Q of G we have $Q \leqslant C_G(P) \leqslant N_G(P)$ by (ix). Therefore, $|N_G(P)|$ is divisible by $|Q|$. Moreover $P \leqslant N_G(P)$ and $N_G(P)$ is divisible by $|P|$. Altogether, $|N_G(P)|$ is divisible by $|G|$ and $N_G(P) = G$. □

6.8 Corollary *Each subgroup and each factor group of a finite nilpotent group is nilpotent.*

Proof This follows from Theorem 6.7 using the equivalences (i) $\iff$ (ix) and (i) $\iff$ (iv). □

6.9 Corollary *Let G be a finite group and let $N \leqslant Z(G)$. Then G is nilpotent if and only if G/N is nilpotent.*

Proof If G is nilpotent, then G/N is nilpotent by Corollary 6.8. Conversely, if G/N is nilpotent and $N/N = N_0/N \leqslant N_1/N \leqslant \cdots \leqslant N_r/N = G/N$ is a central series of G/N, then $1 \leqslant N_0 \leqslant N_1 \leqslant \cdots \leqslant N_r = G$ is a central series of G. □

6.10 Proposition (Frattini-Argument) *Let G be a finite group, $N \trianglelefteq G$, and let $P \leqslant N$ be a Sylow p-subgroup of N for some prime p. Then $G = N \cdot N_G(P)$.*

Proof Let $g \in G$. Then with $P \leqslant N$ also $gPg^{-1} \leqslant gNg^{-1} = N$ is a Sylow p-subgroup of N. By the Sylow Theorems there exists $n \in N$ such that $ngPg^{-1}n^{-1} = P$. This implies $ng \in N_G(P)$ and $g \in nN_G(P) \subseteq N \cdot N_G(P)$. □

6.11 Definition For a finite group G the intersection of all its maximal subgroups is called its *Frattini subgroup* and denoted by $\Phi(G)$. For the trivial group one sets $\Phi(1) = 1$. Note that $\Phi(G)$ is characteristic in G.

6.12 Lemma *If G is a finite group and $H \leqslant G$ such that $H \cdot \Phi(G) = G$, then $H = G$.*

Proof Assume that $H < G$. Then there exists a maximal subgroup U of G with $H \leqslant U$, and $G = H \cdot \Phi(G) \leqslant U \cdot U = U$ which is a contradiction. □

6.13 Proposition *Let G be a finite group and let H and N be normal subgroups of G such that $N \leqslant H \cap \Phi(G)$. If H/N is nilpotent, then every Sylow subgroup of H is normal in G; in particular, H is nilpotent.*

Proof Let P be a Sylow p-subgroup of H. Note that PN/N is a Sylow p-subgroup of H/N, since $PN/N \cong P/(P \cap N)$ is a p-group and the index $[H/N : PN/N] = [H : PN]$ is not divisible by p. Since H/N is nilpotent, PN/N is normal in H/N and as the only Sylow p-subgroup of H/N even characteristic in H/N. Since H/N is normal in G/N, this implies that PN/N is normal in G/N and $PN \trianglelefteq G$. Since P is also a Sylow p-subgroup of PN ($\leqslant H$), the Frattini Argument implies that $G = PN \cdot N_G(P) = N \cdot N_G(P)$. Since $N \leqslant \Phi(G)$, this implies $G = N_G(P)\Phi(G)$. Now Lemma 6.12 implies $G = N_G(P)$ and in particular $P \trianglelefteq H$. Finally Theorem 6.7 implies that H is nilpotent. □

6.14 Corollary (Frattini 1885) *For every finite group G, the Frattini subgroup $\Phi(G)$ is nilpotent.*

Proof This follows from Proposition 6.13 with $H := N := \Phi(G)$. □

6.15 Corollary *Let G be a finite group. If $G/\Phi(G)$ is nilpotent, then also G is nilpotent.*

Proof This follows from Proposition 6.13 with $H := G$ and $N := \Phi(G)$. □

6.16 Theorem *For every finite group G the following are equivalent:*
(i) *G is nilpotent.*
(ii) *$G/\Phi(G)$ is nilpotent.*
(iii) *$G' \leqslant \Phi(G)$.*
(iv) *$G/\Phi(G)$ is abelian.*

Proof (i) $\Rightarrow$ (ii): This is a consequence of Corollary 6.8.

(ii) $\Rightarrow$ (iii): If $G/\Phi(G)$ is nilpotent, then also G is nilpotent by Corollary 6.15. Let U be a maximal subgroup of G. Then U is normal in G by Theorem 6.7. Since G is solvable, also G/U is solvable and simple, and therefore abelian. This implies $G' \leqslant U$ and we can conclude that $G' \leqslant \Phi(G)$.

(iii) $\Rightarrow$ (iv): This is clear, since $G/\Phi(G)$ is isomorphic to $(G/G')/(\Phi(G)/G')$.

(iv) $\Rightarrow$ (i): This follows from Corollary 6.15, since every abelian group is nilpotent. □

7 p-Groups

7.1 Lemma *Let G be a group and let $H \leqslant Z(G)$ such that G/H is cyclic. Then G is abelian.*

Proof Let $x \in G$ with $\langle xH \rangle = G/H$. Every element of G can be written in the form $x^n h$ with $n \in \mathbb{N}_0$ and $h \in H$. For $n, n' \in \mathbb{N}_0$ and $h, h' \in H$ we have:

$$x^n h x^{n'} h' = x^n x^{n'} h h' = x^{n'} x^n h' h = x^{n'} h' x^n h\,,$$

and the lemma is proved. □

7.2 Corollary *If p is a prime and if G is a group of order p^2, then G is abelian.*

Proof By Theorem 2.9, we have $Z(G) > 1$ and there exists $H \leqslant Z(G)$ with $|G/H| \leqslant p$. Thus, G/H is cyclic and G is abelian by Lemma 7.1. □

7.3 Definition Let p be a prime. An abelian p-group G is called *elementary abelian*, if $x^p = 1$ for all $x \in G$. Equivalently, G is isomorphic to a direct product of cyclic groups of order p. If G has order p^n, we call n the *rank* of G.

7.4 Remark Let p be a prime. If G is an elementary abelian p-group, then G is a finite dimensional vector space over the field $\mathbb{Z}/p\mathbb{Z}$ in a natural way, namely by $(k + p\mathbb{Z}) \cdot x := x^k$ for $x \in G$ and $k \in \mathbb{Z}$. Conversely, each $\mathbb{Z}/p\mathbb{Z}$-vector space has an elementary abelian p-group as underlying group. Therefore, elementary abelian p-groups and finite dimensional $\mathbb{Z}/p\mathbb{Z}$-vector spaces are the same thing. Moreover, every $\mathbb{Z}/p\mathbb{Z}$-linear map between $\mathbb{Z}/p\mathbb{Z}$-vector spaces is a group homomorphism and every group homomorphism between elementary abelian p-groups is also a $\mathbb{Z}/p\mathbb{Z}$-linear map. Therefore $\mathrm{Aut}(G) \cong \mathrm{GL}_n(\mathbb{Z}/p\mathbb{Z})$ for any elementary abelian p-group G of rank n. Note also that a subgroup of an elementary abelian p-group G is the same thing as a subspace and that for $X \subseteq G$ the $\mathbb{Z}/p\mathbb{Z}$-span of X is the same as the subgroup generated by X.

7.5 Theorem *Let p be a prime and let G be a p-group. Then the following assertions hold:*

(i) $\Phi(G) = G' \cdot G^p$, *where* $G^p := \langle \{g^p \mid g \in G\} \rangle$. *If* $p = 2$, *one has* $\Phi(G) = G^2$.
(ii) $G/\Phi(G)$ *is elementary abelian.*
(iii) *For every* $N \trianglelefteq G$ *on has:* G/N *is elementary abelian* $\iff \Phi(G) \leqslant N$.
(iv) *If* $U \leqslant G$, *then* $\Phi(U) \leqslant \Phi(G)$.
(v) *If* $N \trianglelefteq G$, *then* $\Phi(G/N) = \Phi(G)N/N$.

Proof (i)–(iii): By Theorem 6.16 and since G is nilpotent, we have $G' \leqslant \Phi(G)$. Each maximal subgroup U of G is normal and of index p in G. Therefore, $(gU)^p = U$ and $g^p \in U$ for each $g \in G$. This implies that $G^p \leqslant \Phi(G)$, and we have $G' \cdot G^p \leqslant \Phi(G)$. This implies (ii); in fact, $G/\Phi(G)$ is abelian, since

$G' \leqslant \Phi(G)$ and $(g\Phi(G))^p = g^p\Phi(G) = \Phi(G)$, since $G^p \leqslant \Phi(G)$. Next we show (iii). If $\Phi(G) \leqslant N$, then $G/N \cong (G/\Phi(G))/(N/\Phi(G))$ is elementary abelian by (ii). Conversely, assume that G/N is elementary abelian and that $N \neq G$. Then N is the intersection of all maximal subgroups of G that contain N; in fact, the intersection of all hyperplanes of G/N is N/N. This implies that $N \leqslant \Phi(G)$ and (iii) is proved. From (iii) we now obtain $\Phi(G) \leqslant G' \cdot G^p$, since $G/(G' \cdot G^p)$ is elementary abelian. If $p = 2$ each commutator

$$xyx^{-1}y^{-1} = xy^2x^{-1}x^2x^{-1}y^{-1}x^{-1}y^{-1} = (xyx^{-1})^2x^2(x^{-1}y^{-1})^2$$

is a product of squares, and therefore $G' \leqslant G^2$. This implies $\Phi(G) = G^2$.

(iv) This follows from (i), since $U' \leqslant G'$ and $U^p \leqslant G^p$.

(v) We have $(G/N)^p = \langle\{g^pN \mid g \in G\}\rangle = G^PN/N$ and $(G/N)' = G'N/N$. Now (i) implies

$$\begin{aligned}\Phi(G/N) &= (G/N)^p \cdot (G/N)' = (G^pN/N) \cdot (G'N/N) \\ &= (G^pG'N)/N = \Phi(G)N/N\,,\end{aligned}$$

and the proof of the theorem is complete. □

7.6 Theorem (Burnside's Basis Theorem) *Let p be a prime and let G be a p-group with $|G/\Phi(G)| = p^d$, $d \in \mathbb{N}$. Then the following assertions hold:*

(i) *Let $n \in \mathbb{N}$ and $x_1, \ldots, x_n \in G$. Then*

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

(ii) *Each minimal generating set of G has d elements.*

(iii) *Each element $x \in G \setminus \Phi(G)$ occurs in some minimal generating set of G.*

Proof (i) With Lemma 6.12 we obtain

$$\begin{aligned}\langle x_1, \ldots, x_n\rangle = G &\iff \langle x_1, \ldots, x_n\rangle\Phi(G) = G \\ &\iff \langle x_1\Phi(G), \ldots, x_n\Phi(G)\rangle = G/\Phi(G)\,.\end{aligned}$$

(ii) Let $\{x_1, \ldots, x_n\}$ be a minimal generating set of G consisting of n elements. By (i) we have $\langle x_1\Phi(G), \ldots, x_n\Phi(G)\rangle = G/\Phi(G)$, and therefore $d \leqslant n$. Assume that $n > d$. Then there exists a proper subset of $\{x_1\Phi(G), \ldots, x_n\Phi(G)\}$ which still generates $G/\Phi(G)$. By (i) the corresponding proper subset of $\{x_1, \ldots, x_n\}$ then generates G. This contradicts the minimality of the set $\{x_1, \ldots, x_n\}$.

(iii) If $x \in G \setminus \Phi(G)$, then $x\Phi(G)$ is nonzero in the vector space $G/\Phi(G)$ and can be extended to a basis $x\Phi(G), x_2\Phi(G), \ldots, x_d\Phi(G)$. Then, by (i) and (ii), $\{x, x_2, \ldots, x_d\}$ is a minimal set of generators of G. □

7.7 Remark (a) Burnside's Basis Theorem implies that every p-group G with $|G/\Phi(G)| = p$ is cyclic.

(b) Part (ii) of Burnside's Basis Theorem does not hold for arbitrary finite groups. For example, the group $\mathbb{Z}/6\mathbb{Z}$ has the minimal generating sets $\{1+6\mathbb{Z}\}$ and $\{3+6\mathbb{Z}, 2+6\mathbb{Z}\}$.

7.8 Examples (a) We already know two non-isomorphic groups of order 8, namely the dihedral group D_8 and the quaternion group $Q_8 = \langle \begin{pmatrix} i & 0 \\ 0 & i \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \rangle$.

(b) Let p be an odd prime. We will construct a non-abelian group of order p^3 as a semidirect product $\mathbb{Z}/p^2\mathbb{Z} \rtimes \mathbb{Z}/p\mathbb{Z}$ with the following action. Recall that $\mathrm{Aut}(\mathbb{Z}/p^2\mathbb{Z}) \cong (\mathbb{Z}/p^2\mathbb{Z})^\times$ where $i + p^2\mathbb{Z} \in (\mathbb{Z}/p^2\mathbb{Z})^\times$ corresponds to the automorphism σ_i of $\mathbb{Z}/p^2\mathbb{Z}$ which raises every element to its i-th power. We have $|\mathrm{Aut}(\mathbb{Z}/p^2\mathbb{Z})| = p(p-1)$ and we observe that $1+p+p^2\mathbb{Z}$ is an element of order p in $(\mathbb{Z}/p^2\mathbb{Z})^\times$, since $(1+p+p^2\mathbb{Z})^p = (1+p)^p + p^2\mathbb{Z} = 1+p^2\mathbb{Z}$. Therefore, if $Y = \langle y \rangle$ is a cyclic group of order p^2 and $X = \langle x \rangle$ is a cyclic group of order p, there exists a non-trivial group homomorphism $\rho\colon X \to \mathrm{Aut}(Y)$ such that the corresponding action satisfies ${}^x y = y^{p+1}$. This gives rise to a semidirect product $Y \rtimes X$ of order p^3.

(c) Let p be an odd prime and let $n \in \mathbb{N}$. Then

$$E_{p^{2n+1}} := \{ \begin{pmatrix} 1 & \beta_1 & \cdots & \beta_n & \gamma \\ & 1 & & & \alpha_1 \\ & & \ddots & & \vdots \\ & & & 1 & \alpha_n \\ & & & & 1 \end{pmatrix} \mid \alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_n, \gamma \in \mathbb{Z}/p\mathbb{Z} \}$$

(with zeros in the empty spots) is a subgroup of $\mathrm{GL}_{n+1}(\mathbb{Z}/p\mathbb{Z})$ of order p^{2n+1}, since

$$\begin{pmatrix} 1 & \beta_1 & \cdots & \beta_n & \gamma \\ & 1 & & & \alpha_1 \\ & & \ddots & & \vdots \\ & & & 1 & \alpha_n \\ & & & & 1 \end{pmatrix} \begin{pmatrix} 1 & \beta_1' & \cdots & \beta_n' & \gamma' \\ & 1 & & & \alpha_1' \\ & & \ddots & & \vdots \\ & & & 1 & \alpha_n' \\ & & & & 1 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & \beta_1+\beta_1' & \cdots & \beta_n+\beta_n' & \gamma+\gamma'+\alpha_1'\beta_1+\cdots+\alpha_n'\beta_n \\ & 1 & & & \alpha_1+\alpha_1' \\ & & \ddots & & \vdots \\ & & & 1 & \alpha_n+\alpha_n' \\ & & & & 1 \end{pmatrix}.$$

The group $E_{p^{2n+1}}$ is called the *extra-special group* of order p^{2n+1} and exponent p. Let $z, x_i, y_i \in E_{p^{2n+1}}$, $i = 1, \ldots, n$, be defined as the elements with precisely one non-zero entry off the diagonal, namely the entry $\gamma = 1$ for z, $\alpha_i = 1$ for x_i, and $\beta_i = 1$ for y_i. Then it is easy to see that the following assertions hold:

(i) for all $i, j \in \{1, \dots, n\}$ one has

$$zx_i = x_i z,\ zy_i = y_i z,\ x_j x_i = x_i x_j,\ y_j y_i = y_i y_j,$$
$$y_j x_i = \begin{cases} x_i y_j, & \text{if } i \neq j, \\ x_i y_j z, & \text{if } i = j. \end{cases}$$

(ii) Every element $g \in E_{p^{2n+1}}$ can be written uniquely in the form

$$g = x_1^{a_1} \cdots x_n^{a_n} y_1^{b_1} \cdots y_n^{b_n} z^c$$

with $a_1, \dots, a_n, b_1, \dots, b_n, c \in \{0, 1, \dots, p-1\}$.

(iii) $g^p = 1$ for all $g \in E_{p^{2n+1}}$.

(iv) The subgroups $\langle x_1, \dots, x_n, z \rangle$ and $\langle y_1, \dots, y_n, z \rangle$ are normal and elementary abelian.

(v) $Z(E_{p^{2n+1}}) = E'_{p^{2n+1}} = \Phi(E_{p^{2n+1}}) = \langle z \rangle$.

(vi) If we identity $Z := \langle z \rangle$ with $\mathbb{Z}/p\mathbb{Z}$ via $z^i \leftrightarrow i + p\mathbb{Z}$ for $i \in \mathbb{Z}$, then the commutator defines a bilinear form on the $2n$-dimensional vector space $V = E_{p^{2n+1}}/Z$ by

$$V \times V \longrightarrow \mathbb{Z}/p\mathbb{Z}, \quad (gZ, hZ) \mapsto [g, h],$$

for $g, h \in E_{p^{2n+1}}$. This bilinear form is skew-symmetric ($[a, b] = -[b, a]$) and non-degenerate ($[a, b] = 0$ for all a implies $b = 0$).

For $n = 1$ we obtain a non-abelian group G of order p^3 and exponent p, which is generated by a central element z and two elements x, y such that $G = \langle x, z \rangle \rtimes \langle y \rangle$ under the action ${}^y x = xz$.

7.9 Lemma *Let G be a p-group and let $x, y \in G$.*
(a) If $G/Z(G)$ is abelian, then

$$[x, y]^i = [x^i, y] \text{ and } (xy)^i = x^i y^i [y^{-1}, x^{-1}]^{\binom{i}{2}},$$

for all $i \in \mathbb{N}_0$.
(b) If $G/Z(G)$ is elementary abelian, then $(xy)^p = x^p y^p$ for odd p and $(xy)^4 = x^4 y^4$ for $p = 2$.

Proof (a) Note that $[x, y], [y^{-1}, x^{-1}] \in G' \leqslant Z(G)$, since $G/Z(G)$ is abelian. We proof the two equations by induction on i. If $i = 0$ this is trivial. Assume the equations hold for some $i \in \mathbb{N}_0$. Then

$$[x, y]^{i+1} = [x, y][x, y]^i = [x, y][x^i, y] = \underbrace{xyx^{-1}y^{-1}}_{\in Z(G)} x^i y x^{-i} y^{-1}$$
$$= x^i (xyx^{-1}y^{-1}) y x^{-i} y^{-1} = x^{i+1} y x^{-i-1} y^{-1} = [x^{i+1}, y]$$

and

$$(xy)^{i+1} = (xy)^i xy = x^i y^i xy [y^{-1}, x^{-1}]^{\binom{i}{2}}$$

with

$$y^i x = x y^i y^{-i} x^{-1} y^i x = x y^i [y^{-i}, x^{-1}] = x y^i [y^{-1}, x^{-1}]^i \in Z(G)\,,$$

and we obtain

$$(xy)^{i+1} = x^{i+1} y^{i+1} [y^{-1}, x^{-1}]^{\binom{i+1}{2}}\,.$$

(b) Note that since $G/Z(G)$ is elementary abelian, we have $G^p \leqslant \Phi(G) \leqslant Z(G)$ by Theorem 7.5. By part (a) we have for odd p:

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

Since $p \mid \binom{p}{2}$, it suffices to show that $[y^{-1}, x^{-1}]^p = 1$. But again by (a), we have $[y^{-1}, x^{-1}]^p = [y^{-p}, x^{-1}] = 1$, since $y^{-p} \in G^p \leqslant Z(G)$.

Finally, for $p = 2$, part (a) implies

$$(xy)^4 = x^4 y^4 [y^{-1}, x^{-1}]^6 = x^4 y^4 [y^{-6}, x^{-1}] = x^4 y^4\,,$$

since $y^6 \in G^2 \leqslant Z(G)$. □

7.10 Theorem *Let p be a prime and let G be a non-abelian group of order p^3.*

(a) If $p = 2$, then $G \cong D_8$ or $G \cong Q_8$.

(b) If p is odd, then G is isomorphic to E_{p^3} or to the group constructed in Example 7.8(b).

Proof From Lemma 7.1 we have $|G/Z(G)| \geqslant p^2$ and from Theorem 2.9 we have $|Z(G)| \geqslant p$. This implies $|Z(G)| = p$. Lemma 7.1 also implies that $G/Z(G)$ is elementary abelian. With Theorem 7.5(iii) we have $1 < G' \leqslant \Phi(G) \leqslant Z(G)$, and therefore $G' = \Phi(G) = Z(G)$.

(a) Assume that $p = 2$. Then there exists an element of order 4 in G. In fact, if every element in G is of order 2, G is abelian, since then $[x, y] = xyx^{-1}y^{-1} = xyxy = (xy)^2 = 1$ for all $x, y \in G$. So let $y \in G$ be an element of order 4 and set $Y := \langle y \rangle$. Since Y has index 2 in G, it is normal in G and $Y \cap Z(G) > 1$ by Theorem 2.9. This implies that $Z(G) < Y$ and $Z(G) = \{1, y^2\}$.

(i) If there exists an element $x \in G \setminus$ of order 2, then $G \cong Y \rtimes X$ with $X := \{1, x\}$ and with the only possible non-trivial action $xyx^{-1} = y^{-1}$. Therefore $G \cong D_8$.

(ii) If there exists no element $x \in G \setminus Y$ of order 2, then we pick an element $x \in G \setminus Y$ of order 4. Everything we proved about y also holds for x. Therefore, $Z(G) = \{1, x^2\}$ and $x^2 = y^2$. Moreover $\langle x \rangle$ acts on Y via conjugation in the only non-trivial way: $xyx^{-1} = y^{-1}$. This implies $G = \{x^i y^j \mid 0 \leqslant i \leqslant 3, 0 \leqslant j \leqslant 1\}$ with $x^4 = 1$, $y^4 = 1$, $x^2 = y^2$, and $yx = xy^3 = yx^2x^{-1} = x^2yx^{-1} = x^2x^{-1}y^3 =$

$xy^3 = x^3y$, i.e. the multiplication in G coincides with the multiplication in Q_8 when we identify x with $\begin{pmatrix} i & 0 \\ 0 & i \end{pmatrix}$ and y with $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$. Therefore, $G \cong Q_8$.

(b) Now we assume that p is odd.

(i) We first consider the case that there exists an element $y \in G$ of order p^2. Then $Y := \langle y \rangle$ is a maximal subgroup of G and therefore normal in G. Moreover, $Z(G) \cap Y > 1$ so that $Z(G) = \langle y^p \rangle$. We claim that there exists an element $x \in G \setminus Y$ of order p such that $xyx^{-1} = y^{1+p}$ which then implies that G is isomorphic to the semidirect product of Example 7.8(b). We prove the claim. First choose any $x_1 \in G \setminus Y$. Then there exists $i \in \{1, \dots, p\}$ with $x_1^p = y^{pi}$, since $x_1^p \in G^p \leqslant \Phi(G) = Z(G) = \langle y^p \rangle$. By Lemma 7.9(b) we have $(x_1 y^{-i})^p = x_1^p y^{-ip} = 1$ and therefore the element $x_2 := x_1 y^{-i} \in G \setminus Y$ has order p. The conjugation of x_2 on Y is non-trivial. Therefore, the resulting homomorphism $\rho\colon X := \langle x_2 \rangle \to \mathrm{Aut}(Y) \cong (\mathbb{Z}/p\mathbb{Z})^\times$ has as image the Sylow p-subgroup $\langle 1 + p + p^2\mathbb{Z} \rangle$ of $(\mathbb{Z}/p^2\mathbb{Z})^\times$. In particular, $\rho(x_2^j) = 1 + p + p^2\mathbb{Z}$ for some $j \in \{1, \dots, p-1\}$ and the element $x := x_2^j$ satisfies our claim.

(ii) If there exists no element of order p^2 in G we denote by z a generator of $Z(G)$ and choose an element $x \in G \setminus Z(G)$. Then $X := \langle x, z \rangle$ is elementary abelian of order p^2 and also maximal in G. Let $y_1 \in G \setminus X$. Then $G \cong X \rtimes Y$ with $Y := \langle y_1 \rangle$ and with the conjugation action of Y on X. Since z is central, we have $y_1 z y_1^{-1} = z$. Moreover $y_1 x y_1^{-1} = x^i z^j$ for some $i, j \in \{0, \dots, p-1\}$. We have

$$\begin{aligned} x &= y_1^p x y_1^{-p} = y_1^{p-1} x^i z^j y_1^{-(p-1)} = y_1^{p-1} x^i y_1^{-(p-1)} z^j \\ &= y_1^{p-2} x^{i^2} z^{ij} y_1^{-(p-2)} z^j = y_1^{p-2} x^{i^2} y_1^{-(p-2)} z^{i+ij} = \cdots \\ &= x^{i^p} z^{j+ij+\cdots+i^{p-1}j}. \end{aligned}$$

This implies that $i^p \equiv 1 \mod p$. But we also know that $i^p = i^{p-1} \cdot i \equiv 1 \cdot i = i \mod p$. This implies $i = 1$. Since G is not abelian we have $j \neq 0$, and therefore $y_1 x y_1^{-1} = x z^j$ for some $j \in \{1, \dots, p-1\}$. Let $k \in \{1, \dots, p-1\}$ with $kj \equiv 1 \mod p$ and set $y := y_1^k$. Then $yzy^{-1} = 1$, $yxy^{-1} = y_1^k x y_1^{-k} = x z^{kj} = xz$ and we obtain $G \cong X \rtimes Y \cong E_{p^3}$ as described at the end of Example 7.8(c). $\square$

8 The Theorem of Schur-Zassenhaus

8.1 Definition Let π be a set of primes. We define π' as the set of primes not contained in π.

(a) Let $n \in \mathbb{N}$. If $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ is the prime factor decomposition of n, then the *π-part* n_π of n is defined as $\prod_{p_i \in \pi} p_i^{\alpha_i}$. Then $n = n_\pi n_{\pi'}$.

(b) A finite group G is called a *π-group*, if $|G|_\pi = |G|$. For an arbitrary finite group G we call a subgroup $H \leqslant G$ a *π-subgroup*, if H is a π-group. A subgroup $H \leqslant G$ is called a *Hall π-subgroup* of G if $|H|_\pi = |G|_\pi$. A subgroup $H \leqslant G$ is called a *Hall subgroup* of G if it is a Hall π-subgroup for some π. This is obviously equivalent to $\gcd(|H|, [G : H]) = 1$.

(c) For any element g of a finite group G there exist unique elements g_π and $g_{\pi'}$ of G such that $\langle g_\pi \rangle$ is a π-subgroup, $\langle g_{\pi'} \rangle$ is a π'-subgroup, and $g = g_\pi g_{\pi'}$. These elements are called the *π-part* and the *π'-part* of g. It is easy to see that $g_\pi, g_{\pi'} \in \langle g \rangle$. In particular, they commute.

(d) For every finite group G there exists a biggest normal π-subgroup of G. It will be denoted by $O_\pi(G)$.

8.2 Remark Let G be a finite group and let π be a set of primes. It is easy to see that $O_\pi(G)$ is characteristic in G. Considering the group Alt(5) and $\pi = \{2, 5\}$ or $\pi = \{3, 5\}$ one sees that in general Hall π-subgroups do not exist.

8.3 Theorem *Let G be a finite group. Then the following are equivalent:*

(i) *G is solvable.*

(ii) *For every $N \triangleleft G$ there exists a prime p such that $O_p(G/N) > 1$.*

Proof (i) $\Rightarrow$ (ii): We may assume that $N = 1$ and $G > 1$. Since G is solvable, there exists $n \in \mathbb{N}$ such that $G^{(n)} = 1$ and $G^{(n-1)} > 1$. Then $G^{(n-1)}$ is abelian. Let p be a prime divisor of $|G^{(n-1)}|$, then the set $U := \{x \in G^{(n-1)} \mid x^p = 1$ is a non-trivial characteristic p-subgroup of $G^{(n-1)}$ and therefore normal in G. This implies $O_p(G) \geqslant U > 1$.

(ii) $\Rightarrow$ (i): By (ii) there exist primes $p_1, \ldots, p_r$ and normal subgroups $N_0, N_1, \ldots, N_r$ of G such that $1 = N_0 < N_1 < \cdots < N_r = G$ and $N_i/N_{i-1} = O_{p_i}(G/N_{i-1})$ for each $i = 1, \ldots, r$. Since N_i/N_{i-1} is solvable for $i = 1, \ldots, r$, also G is solvable. □

8.4 Remark Let G be a finite group and let $N \trianglelefteq G$. Note that a subgroup $H \leqslant G$ is a complement of N in G if and only if each coset $gN \in G/N$ contains exactly one element in H. If U is a Hall π-subgroup of G for some π, then $H \leqslant G$ is a complement of U in G if and only if H is a Hall π'-subgroup of G.

8.5 Theorem (Schur-Zassenhaus) *Let G be a finite group and assume that $H \leqslant G$ is a normal Hall π-subgroup of G. Then:*

(a) *There exists a complement of H in G.*

(b) *If H or G/H is solvable, any two complements of H in G are conjugate in G.*

Proof PART 1: We prove (a) and (b) in the case that H is abelian.

(a) We denote the elements of $\bar{G} := G/H$ by $\alpha, \beta, \gamma, \ldots$ and have to find for each $\alpha \in \bar{G}$ a representative $k_\alpha \in \alpha$ such that $k_\alpha k_\beta = k_{\alpha\beta}$. Then the elements k_α, $\alpha \in \bar{G}$, form a subgroup and a complement of H in G.

First we choose arbitrary representatives $x_\alpha \in \alpha$ for each $\alpha \in \bar{G}$. Since $x_\alpha x_\beta H = x_\alpha H x_\beta H = \alpha\beta = x_{\alpha\beta} H$, there exists $f(\alpha, \beta) \in H$ such that $x_\alpha x_\beta = x_{\alpha\beta} f(\alpha, \beta)$ for all $\alpha, \beta \in \bar{G}$. This defines a function $f\colon \bar{G} \times \bar{G} \to H$. By associativity in G we obtain

$$x_\alpha(x_\beta x_\gamma) = x_\alpha\big(x_{\beta\gamma} f(\beta,\gamma)\big) = (x_\alpha x_{\beta\gamma}) f(\beta,\gamma) = x_{\alpha\beta\gamma} f(\alpha,\beta\gamma) f(\beta,\gamma)$$

and

$$(x_\alpha x_\beta) x_\gamma = x_{\alpha\beta} f(\alpha,\beta) x_\gamma = x_{\alpha\beta} x_\gamma \underbrace{x_\gamma^{-1} f(\alpha,\beta) x_\gamma}_{=: f(\alpha,\beta)^{x_\gamma}} = x_{\alpha\beta\gamma} f(\alpha\beta,\gamma) f(\alpha,\beta)^{x_\gamma} ,$$

which implies $f(\alpha,\beta\gamma) f(\beta,\gamma) = f(\alpha\beta,\gamma) f(\alpha,\beta)^{x_\gamma}$ for all $\alpha, \beta, \gamma \in \bar{G}$. If we fix β and γ in $\bar{G}$ and multiply these equations for varying $\alpha \in \bar{G}$ (note that H is abelian), then we obtain

$$\Big(\prod_{\alpha\in\bar{G}} f(\alpha,\beta\gamma)\Big) f(\beta,\gamma)^m = \Big(\prod_{\alpha\in\bar{G}} f(\alpha\beta,\gamma)\Big)\Big(\prod_{\alpha\in\bar{G}} f(\alpha,\beta)\Big)^{x_\gamma}$$

with $m := [G : H]$, or

$$g(\beta\gamma) f(\beta,\gamma)^m = g(\gamma) g(\beta)^{x_\gamma} ,$$

if we define the function $g\colon \bar{G} \to H$ by $g(\delta) := \prod_{\alpha\in\bar{G}} f(\alpha,\delta)$. Since H and $m = [G : H]$ are coprime, there exist $r, s \in \mathbb{Z}$ such that $rm + s|H| = 1$, and therefore $rm \equiv 1 \mod |H|$. If we set $h(\delta) := g(\delta)^{-r}$ for each $\delta \in \bar{G}$, we obtain

$$h(\beta\gamma) f(\beta,\gamma)^{-1} = h(\gamma) h(\beta)^{x_\gamma}$$

for all $\beta, \gamma \in \bar{G}$. Now we set $k_\alpha := x_\alpha h(\alpha)$ for $\alpha \in \bar{G}$ and obtain

$$\begin{aligned} k_\beta k_\gamma &= x_\beta h(\beta) x_\gamma h(\gamma) = x_\beta x_\gamma h(\beta)^{x_\gamma} h(\gamma) = x_{\beta\gamma} f(\beta,\gamma) h(\beta)^{x_\gamma} h(\gamma) \\ &= x_{\beta\gamma} f(\beta,\gamma) h(\beta\gamma) f(\beta,\gamma)^{-1} = x_{\beta\gamma} h(\beta\gamma) = k_{\beta\gamma} \end{aligned}$$

for all $\beta, \gamma \in \bar{G}$ and $K := \{k_\beta \mid \beta \in \bar{G}\}$ is a complement of H in G.

(b) Let K and K' be complements of H in G. Then for each $k \in K$ there exists a unique $k' \in K'$ such that $kH = k'H$. Therefore, there exists a function $b\colon K \to H$ such that $k' = kb(k)$ for all $k \in K$. For k_1 and k_2 in K we then have $(k_1k_2)' = k_1k_2b(k_1k_2)$ and $k_1'k_2' = k_1b(k_1)k_2b(k_2)$. But $(k_1k_2)' = k_1'k_2'$ since both lie in the same coset in G/H. Therefore, $k_1k_2b(k_1k_2) = k_1b(k_1)k_2b(k_2) = k_1k_2\big(b(k_1)^{k_2}\big)b(k_1)$ and

$$b(k_1k_2) = \big(b(k_1)^{k_2}\big) b(k_2)$$

for all $k_1, k_2 \in K$. We fix k_2 and multiply these equations for all $k_1 \in K$. This yields

$$\prod_{k_1 \in K} b(k_1 k_2) = \Big(\prod_{k_1 \in K} b(k_1) \Big)^{k_2} b(k_2)^m ,$$

since H is abelian. With $z := \prod_{k \in K} b(k)$ we then have $z = z^k b(k)^m$ for all $k \in K$. For $r \in \mathbb{Z}$ with $rm \equiv 1 \mod |H|$ we obtain $z^r = z^{rk} b(k)$. Now we set $y := z^r$ and have $y = y^k b(k)$ for all $k \in K$. Therefore,

$$y^{-1} k y = k (y^{-1})^k y = k (y^k)^{-1} y = k b(k) = k'$$

for all $k \in K$. This implies $y^{-1} K y = K'$.

PART 2: Now we assume that H is arbitrary. We will show (a) and (b) by induction on $|G|$. If $G = 1$, the assertions are trivial. Therefore, we assume $|G| > 1$ and we also assume that (a) and (b) hold for every group of order smaller than $|G|$. Finally we may assume that $|H| > 1$.

Claim 1: If $U < G$, then $U \cap H$ has a complement in U. *Proof:* $U \cap H$ is normal in U and a Hall π-subgroup of U. Moreover, $U/U \cap H \cong UH/H$ implies $[U : U \cap H] \mid [G : H]$. Therefore, $U \cap H$ is a normal Hall π-subgroup of U and, by induction, has a complement in U.

Claim 2: If $1 < N \lhd G$, then HN/N has a complement in G/N. *Proof:* HN/N is normal in G/N and $HN/N \cong H/H \cap N$ implies that HN/N is a π-subgroup of G/N. Moreover, $[G/N : HN/N] = [G : HN]$ is a π'-number and HN/N is a normal Hall π-subgroup of G/N. Now, by induction the claim follows.

Claim 3: If H has a subgroup $1 < N < H$ which is normal in G, then (a) and (b) hold. *Proof:* By Claim 2, $HN/N = H/N$ has a complement U/N in G/N, where $N \leqslant U \leqslant G$. One has $U < G$, since otherwise $U/N = G/N$ implies $H/N = N/N$ and $N = H$. By Claim 1, $U \cap H$ has a complement K in U. We show that K is also a complement of H in G. We have $KH = K(U \cap H)H = UH = G$ and $K \cap H = 1$, since $K \cong U/U \cap H \cong UH/H \leqslant G/H$ implies that K is a π'-group.

Now we show (b) under the assumption of Claim 3. Assume that K and K' are complements of H in G. Then KN/N and $K'N/N$ are complements of the normal Hall π-subgroup H/N or G/N in G/N. In fact, $(KN/N)(H/N) = KHN/N = G/N$ and $KN/N \cong K/K \cap N$ is a π'-group. With H or G/H also H/N or $(G/N)/(H/N) \cong G/H$ are solvable. By induction there exists $g \in G$ such that

$$KN/N = gN(K'N/N)g^{-1}N = gK'Ng^{-1}/N = gK'g^{-1}N/N ,$$

and therefore, $KN = gK'g^{-1}N$. But now K and $gK'g^{-1}$ are complements of the normal Hall π-subgroup N of KN in KN. Moreover, if H or G/H is solvable, then N or $KN/N \cong K \cong G/H$ are solvable. Again by induction, the groups K and $gK'g^{-1}$ are conjugate in KN. Therefore, K and K' are conjugate in G.

Claim 4: If $O_p(H) > 1$ for some prime p, then (a) and (b) hold. *Proof:* If $O_p(H) < H$, this follows from Claim 3, since $O_p(H)$ is characteristic in H and therefore normal in G. If $O_p(H) = H$, then H is a p-group and we can consider the characteristic subgroup $\Phi(H)$ of H which is again normal in G. By Claim 3 we may assume that $\Phi(H) = 1$. But then $H \cong H/\Phi(H)$ is elementary abelian and (a) and (b) have been proved in Part 1.

Claim 5: If H is solvable, then (a) and (b) hold. *Proof:* This follows immediately from Theorem 8.3 and Claim 4.

Proof of (a): Let p be a prime divisor of $|H|$ and let P be a Sylow p-subgroup of H. By Claim 4 we may assume that P is not normal in G. Then $U = N_G(P) < G$. By Claim 1 there exists a complement K of $U \cap H$ in U. The Frattini-Argument implies that $G = HU = H(U \cap H)K = HK$. Moreover, $K \cong U/U \cap H \cong UH/H = G/H$ is a π'-group. This implies that K is a complement of H in G.

Proof of (b): By Claim 5 we may assume that G/H is solvable. By Theorem 8.3, there exists a prime p such that $O_p(G/H) > 1$. Write $O_p(G/H) = R/H$ with $H < R \trianglelefteq G$. Let K and K' be two complements of H in G. Then we have $(K \cap R)H = KH \cap R = G \cap R = R$ with $H \cap (K \cap R) = 1$. Since $p \nmid |H|$ and $K \cap R \cong K \cap R/K \cap R \cap H \cong (K \cap R)H/H = R/H$ is a p-group, the group $K \cap R$ is a Sylow p-subgroup of R. Similarly, $K' \cap R$ is a Sylow p-subgroup of R. Therefore, there exists $g \in R$ such that $K \cap R = g(K' \cap R)g^{-1} = gK'g^{-1} \cap gRg^{-1} = gK'g^{-1} \cap R$. Set $V := N_G(K \cap R)$. Since $K \cap R \trianglelefteq K$ and $K \cap R = gK'g^{-1} \cap R \trianglelefteq gK'g^{-1}$, we have $\langle K, gK'g^{-1} \rangle \leqslant V$. We observe that K is a complement of the normal Hall π-subgroup $V \cap H$ of V in V, since $K(V \cap H) = V \cap KH = V \cap G = V$, $|K| = |G/H|$, and $|V \cap H| \mid |H|$. Similarly, $gK'g^{-1}$ is a complement of $V \cap H$ in V. Note that with G/H also $V/V \cap H \cong VH/H \leqslant G/H$ is solvable. If $V < G$, then K and $gK'g^{-1}$ are conjugate in V by induction, and K and K' are conjugate in G. Therefore, we may assume that $V = G$ and we set $M := K \cap R \trianglelefteq G$. Since K and $gK'g^{-1}$ are complements of H in G, K/M and $gK'g^{-1}/M$ are complements of the normal Hall π-subgroup HM/M of G/M in G/M; in fact, $(K/M)(HM/M) = KHM/M = G/M$ with K/M a π'-group and $HM/M \cong H/(H \cap M)$ a π-group, and similar for $gK'g^{-1}/M$. Moreover, $(G/M)/(HM/M) \cong G/HM \cong (G/H)/(HM/H)$ is solvable. By induction, K/M and $gK'g^{-1}/M$ are conjugate in G/M. But then also K and $gK'g^{-1}$ are conjugate in G. This implies that K and K' are conjugate in G and finishes the proof of the theorem. □

8.6 Remark Feit and Thompson proved the celebrated *Odd-Order-Theorem* stating that every finite group of odd order is solvable. Therefore, the solvability condition in Theorem 8.5(b) is always satisfied.

9 The π-Sylow Theorems

Throughout this Section let G denote a finite group and π a set of primes.

9.1 Definition (a) G is called *π-separated*, if G has a normal series

$$1 = G_0 \leqslant G_1 \leqslant \cdots \leqslant G_r = G$$

such that each factor G_i/G_{i-1}, $i = 1 \ldots, r$, is a π-group or a π'-group.

(b) G is called π-solvable, if G has a normal series whose factors consist of solvable π-groups and arbitrary π'-groups.

9.2 Remark (a) G is π-separated if and only if G is π'-separated.

(b) If G is π-solvable, then G is π-separated.

(c) With the Odd-Order-Theorem of Feit and Thompson we see that if G is π-separated, then G is π-solvable or π'-solvable.

(d) Subgroups and factor groups of π-separated (resp. π-solvable) groups are again π-separated (resp. π-solvable), cf. Exercise 31.

(e) If G is π-solvable and $1 \leqslant H_0 \trianglelefteq H_1 \leqslant G$ are subgroups such that H_1/H_0 is a π-group, then H_1/H_0 is solvable (cf. Exercise 31).

(f) One has: G is solvable $\iff$ G is π-solvable for all π. In fact, if G is solvable, then every chief factor is an elementary abelian p-group for some p. Therefore, G is π-solvable for every π. Conversely, if G is π-solvable for $\pi := \{p \mid p \mid |G|\}$, then the claim follows from part (e).

(g) If $N \trianglelefteq G$ and $H \leqslant G$ is a Hall π-subgroup of G, then HN/N is a Hall π-subgroup of G/N and $H \cap N$ is a Hall π-subgroup of N. In fact, $HN/N \cong H/(N \cap H$ and $H \cap N$ are π-groups and $[G/N : HN/N] = [G : HN] \mid [G : H]$ and $[N : H \cap N] = [HN : H] \mid [G : H]$ are π'-numbers.

9.3 Theorem (π-Sylow Theorem, Ph. Hall 1928)

(a) If G is π-separated, then there exist Hall π-subgroups and Hall π'-subgroups in G.

(b) If G is π-solvable, any two Hall π-subgroups and any two Hall π'-subgroups are conjugate in G.

(c) If G is π-solvable, then any π-subgroup (resp. π'-subgroup) of G is contained in some Hall π-subgroup (resp. Hall π'-subgroup).

Proof We prove the statements by induction on $|G|$. If $G = 1$, all assertions are clearly true. Now let $G > 1$. Since G is π-separated, we have $O_\pi(G) > 1$ or $O_{\pi'}(G) > 1$. Let $N := O_\pi(G) > 1$ or $N := O_{\pi'}(G) > 1$.

(a) By induction there exists a Hall π-subgroup H/N of G/N. Then $[H : N]$ is a π-number and $[G : H]$ is a π'-number. If N is a π-group, then H is a Hall π-subgroup of G. If N is a π'-group, then by the Theorem of Schur-Zassenhaus it has a complement K in H. Therefore, K is π-group and $[G : K] = |G|/(|H|/|N|) = [G : H] \cdot |N|$ is a π'-number. Therefore, K is a Hall π-subgroup of G. Similarly, there exists a Hall π'-subgroup of G.

(b) Let $\mu = \pi$ or $\mu = \pi'$ and U and V be two Hall μ-subgroup of G. Then UN/N and VN/N are Hall μ-subgroups of G/N by Remark 9.2(g). By induction, there exists $g \in G$ such that $gUNg^{-1} = VN$ and so $gUg^{-1}N = VN$. If also N is a μ-group, then $|VN| = |V||N|/|V \cap N|$ is a μ-number and therefore, $VN = V$. This implies $N \leqslant V$, $gUg^{-1} \leqslant VN = V$, and $gUg^{-1} = V$. If N is a μ'-number, then $|gUg^{-1}| = |V|$ and $|N|$ are coprime. This implies $V \cap N = gUg^{-1} \cap N = 1$ so that V and gUg^{-1} are complements of the normal Hall μ-group N of $VN = gUg^{-1}N$. Now either $VN/N \cong V$ or N is a π-group and by Remark 9.2(e) solvable. By Schur-Zassenhaus, the complements gUg^{-1} and V are conjugate in VN. Therefore, U and V are conjugate in G.

(c) Let $\mu = \pi$ or $\mu = \pi'$ and let $U \leqslant G$ be a μ-subgroup. Moreover, let $H \leqslant G$ be a Hall μ-subgroup of G (which exists by (a)). Then $UN/N \cong U/(U \cap N)$ is a μ-subgroup of G/N and by induction and by (b) there exists $g \in G$ such that $UN \leqslant gHg^{-1}N$, since HN/N is a Hall μ-subgroup of G/N by Remark 9.2(g). If N is a μ-group, then $gHg^{-1}N = gHg^{-1}$ and $U \leqslant UN \leqslant gHg^{-1}N = gHg^{-1}$. If N is a μ'-group, then $U \cap N = 1$. Moreover, $UN = UN \cap gHg^{-1}N = (UN \cap gHg^{-1})N$ and $V \cap N = 1$, where $V := UN \cap gHg^{-1}$. Therefore, U and V are two complements of the normal Hall μ'-subgroup N of $UN = VN$. Moreover, N or $UN/N \cong U$ is a π-group and solvable by Remark 9.2(e). Therefore, by Schur-Zassenhaus, there exists $x \in UN$ such that $U = xVx^{-1} = x(UN \cap gHg^{-1})x^{-1} \leqslant (xg)H(xg)^{-1}$. □

9.4 Remark By the Odd-Order-Theorem of Feit-Thompson, it would be enough to require G to be π-separated in Theorem 9.3(b) and (c).

9.5 Corollary *Let G be solvable and let π be arbitrary. Then G has a Hall π-subgroup, any two Hall π-subgroups of G are conjugate in G, and any π-subgroup of G is contained in a Hall π-subgroup.*

Proof Clear with Theorem 9.3 and Remark 9.2(f). □

9.6 Lemma *Let $U, V \leqslant G$.*

(a) If $\mathcal{R} \subseteq U$ is a set of representatives for the cosets $U/U \cap V$, then $UV = \dot{\bigcup}_{x \in \mathcal{R}} xV$ and $|UV| = |U| \cdot |V|/|U \cap V|$.

(b) One has $UV \leqslant G$ if and only if $UV = VU$.

(c) One has $[G : U \cap V] \leqslant [G : U][G : V]$ with equality if and only if $UV = G$.

(d) If $[G : U]$ and $[G : V]$ are coprime, then $[G : U \cap V] = [G : U] \cdot [G : V]$ and $UV = G$.

Proof (a) Obviously, $xV \subseteq UV$ for each $x \in \mathcal{R}$. Conversely, if $u \in U$, then there exists $x \in \mathcal{R}$ and $y \in U \cap V$ such that $u = xy$. Therefore, $uV = xyV = xV$. Disjointness: Let $x, x' \in \mathcal{R}$ and let $v, v' \in V$ such that $xv = x'v'$. Then ${x'}^{-1}x = v'v^{-1} \in U \cap V$. This implies $x' = x$. The remaining formula follows from the established equality: $|UV| = |\mathcal{R}| \cdot |V| = |U||V|/|U \cap V|$.

(b) If UV is a subgroup of G, then $vu \in UV$ for all $u \in U$ and all $v \in V$. Therefore, $VU \subseteq UV$. By the formula in (a) one has $|UV| = |VU|$ and therefore $UV = VU$. Conversely, if $UV = VU$, then with $u, u' \in U$ and $v, v' \in V$ also $(uv)(u'v')^{-1} = uvv'^{-1}u'^{-1} \in UVU = UUV = UV$. This implies that UV is a subgroup of G.

(c) By (a) we have

$$[G : U \cap V] = \frac{|G|}{|U \cap V|} = \frac{|G| \cdot |UV|}{|U| \cdot |V|} \leqslant \frac{|G| \cdot |G|}{|U| \cdot |V|} = [G : U] \cdot [G : V]\,,$$

with equality if and only if $UV = G$.

(d) Since $[G : U] \mid [G : U \cap V]$ and $[G : V] \mid [G : U \cap V]$, and since $[G : U]$ and $[G : V]$ are coprime, we obtain $[G : U] \cdot [G : V] \mid [G : U \cap V]$. Now (c) implies (d). □

9.7 Lemma *If G has three solvable subgroups H_1, H_2, H_3 of pairwise coprime indices, then G is solvable.*

Proof We prove the assertion by induction on G. If $G = 1$, then G is solvable. Now we assume that $G > 1$. If $H_1 = 1$, then $H_2 = G$ and G is solvable. If $H_1 > 1$, then H_1 contains a normal p-subgroup $N > 1$, for some prime p by Theorem 8.3. Since $[G : H_2]$ and $[G : H_3]$ are coprime, one of them is not divisible by p. By symmetry we may assume that $p \nmid [G : H_2]$. Set $D := H_1 \cap H_2$. Then, by Lemma 9.6, we have $H_1H_2 = G$ and $[G : H_1] \cdot [G : H_2] = [G : D] = [G : H_1] \cdot [H_1 : D]$. This implies $[G : H_2] = [H_1 : D]$. Now $ND \leqslant H_1$ and $[ND : D] = [N : N \cap D]$ is a p-power which divides $[H_1 : D] = [G : H_2]$. This implies $ND = D$ and $N \leqslant D$.

For all $g \in G$ we have $gNg^{-1} \leqslant H_2$; in fact, since $G = H_1H_2 = H_2H_1$, there exist $h_1 \in H_1$ and $h_2 \in H_2$ such that $g = h_2h_1$ and we obtain $h_2h_1Nh_1^{-1}h_2^{-1} = h_2Nh_2^{-1} \leqslant h_2Dh_2^{-1} \leqslant H_2$. This implies that $1 < I := \langle \bigcup_{g \in G} gNg^{-1} \rangle \leqslant H_2$ and that I is a solvable normal subgroup of G. The group G/I has the solvable subgroups H_iI/I, $i = 1, 2, 3$, with pairwise coprime indices $[G/I : H_iI/I] = [G : H_iI] \mid [G : H_i]$. By induction, G/I is solvable, and with I also G is solvable. □

9.8 Remark A famous theorem of Burnside states that every finite group of order p^aq^b, with primes p and q and with $a, b \in \mathbb{N}_0$, is solvable. A purely group theoretical proof of this result is quite lengthy. There is a more elegant proof using representation theory which will be presented next quarter. We will use Burnside's Theorem in order to prove the following Theorem.

9.9 Theorem (Ph. Hall, 1937) *Let $|G| = p_1^{e_1} \cdots p_r^{e_r}$ be the prime factor decomposition of $|G|$. If there exists for each $i \in \{1, \ldots, r\}$ a Hall p_i'-subgroup of G, then G is solvable.*

Proof We prove the assertion by induction on r. If $r = 0$, then $G = 1$ and solvable. If $r = 1$, then G is a p-group and solvable. If $r = 2$, then G is solvable by Burnside's Theorem. Now assume that $r \geqslant 3$. For $i \in \{1, \ldots, r\}$ let U_i be a Hall p_i'-subgroup of G. For $i \neq j$ in $\{1, \ldots, r\}$, we set $V_{ij} := U_i \cap U_j$. Then, by Lemma 9.6(d), $[G : V_{ij}] = p_i^{e_i} p_j^{e_j}$ and $[U_i : V_{ij}] = p_j^{e_i}$. Therefore, each U_i satisfies the hypothesis of the theorem with $r - 1$ prime divisors. By induction, each U_i is solvable. By Lemma 9.7 with $H_i = U_i$, $i = 1, 2, 3$, it follows that G is solvable. □

9.10 Corollary *The following assertions are equivalent:*

(i) *G is solvable.*

(ii) *G has Hall π-subgroups for each π.*

(iii) *G has Hall p'-subgroups for each prime p.*

Proof (i) $\Rightarrow$ (ii): This follows from the π-Sylow Theorem.

(ii) $\Rightarrow$ (iii): This is trivial.

(iii) $\Rightarrow$ (i): This follows from Theorem 9.9. □

9.11 Theorem *Let G be solvable, let $p_1, \ldots, p_r$ be the prime divisors of G, and let H_i be a Hall p_i'-subgroup of G for $i = 1, \ldots, r$. Then for each $i = 1, \ldots, r$, the group $P_i := \bigcap_{j \neq i} H_j$ is a Sylow p_i-subgroup of G such that $P_i P_j = P_j P_i$ for all $i, j \in \{1, \ldots, r\}$.*

Proof We prove the theorem by induction on r. The assertion is clear for $r = 0$ and $r = 1$. If $r = 2$, by Lemma 9.6(d) and (b) we have $P_1 P_2 = G = P_2 P_1$. From now on we assume that $r \geqslant 3$ and that the assertion holds for all groups whose order has less than r distinct prime divisors. For every $\pi \subseteq \{p_1, \ldots, p_2\}$, the subgroup $\bigcap_{p_i \in \pi} H_i$ is a Hall π'-subgroup of G; in fact this follows from repeated use of Lemma 9.6(d). In particular, for $i \neq j$ in $\{1, \ldots, r\}$, the group $G_{ij} := \bigcap_{k \in \{1, \ldots, r\} \smallsetminus \{i,j\}} H_k$ is a Hall $\{p_i, p_j\}$-subgroup of G, and $P_i := G_{ij} \cap H_j$ (resp. $P_j := G_{ij} \cap H_i$) is a Sylow p_i-subgroup (resp. Sylow p_j-subgroup) of G_{ij} and of G. As in the case $r = 2$ we obtain $P_i P_j = G_{ij} = P_j P_i$. □

9.12 Definition Let $|G| = p_1^{e_1} \cdots p_r^{e_r}$ be the prime factor decomposition of $|G|$ with $p_1 < \cdots < p_r$.

(a) A tuple $(P_1, \ldots, P_r)$ consisting of Sylow p_i-subgroups P_i of G, $i = 1, \ldots, r$, is called a *Sylow system* of G if $P_i P_j = P_j P_i$ for all $i, j \in \{1, \ldots, r\}$.

(b) A tuple $(K_1, \ldots, K_r)$ consisting of Hall p_i'-subgroups of G, $i = 1, \ldots, r$, is called a *Sylow complement system* of G.

9.13 Proposition *Let $(P_1, \ldots, P_r)$ be a Sylow system of G, where P_i is a p_i-Sylow subgroup of G, and let $\pi \subseteq \{p_1, \ldots, p_r\}$. Then $\prod_{p_i \in \pi} P_i$ is a Hall π-subgroup of G.*

Proof The equalities $P_iP_j = P_jP_i$ for $i, j \in \{1, \dots, r\}$ imply by repeated use of Lemma 9.7(b) that $\prod_{p_i \in \pi} P_i$ is a subgroup of G. Moreover, by induction on $|\pi|$ it is easy to see that $\prod_{p_i \in \pi} P_i$ is a Hall π-subgroup of G. In fact, if $|\pi| = 0$ or $|\pi| = 1$, this is clear, and if $|\pi| > 1$ we choose $p_{i_0} \in \pi$ and set $\tilde{\pi} := \pi \setminus \{p_{i_0}\}$. Then, by induction, $\prod_{p_i \in \tilde{\pi}} P_i$ is a Hall $\tilde{\pi}$-subgroup of G so that $(\prod_{p_i \in \tilde{\pi}} P_i) \cap P_{i_0} = 1$. Now Lemma 9.6(a) implies that $\prod_{p_i \in \pi} P_i = (\prod_{p_i \in \tilde{\pi}} P_i)P_{i_0}$ is a Hall π-subgroup of G. □

9.14 Corollary *The following assertions are equivalent:*

(i) *G is solvable.*

(ii) *G has a Sylow system.*

(iii) *G has a Sylow complement system.*

Proof By Theorem 9.11, (i) implies (ii). Moreover, by Proposition 9.13, (ii) implies (iii). Finally, by Corollary 9.10, (iii) implies (i). □

9.15 Remark Let $\mathcal{S}$ denote the set of Sylow systems of G, let $\mathcal{K}$ denote the set of Sylow complement systems of G, and assume that $p_1 < \cdots < p_r$ are the prime divisors of $|G|$. Then, the maps

$$\begin{aligned} \mathcal{S} &\underset{\psi}{\overset{\varphi}{\rightleftarrows}} \mathcal{K} \\ (P_1, \dots, P_r) &\mapsto (\prod_{i \neq 1} P_i, \dots, \prod_{i \neq r} P_i) \\ (\bigcap_{i \neq 1} K_i, \dots, \bigcap_{i \neq r} K_i) &\mapsfrom (K_1, \dots, K_r) \end{aligned}$$

are well-defined inverse bijections. In fact, by Proposition 9.13, φ is well-defined, and by the arguments in the proof of Theorem 9.11, ψ is well-defined. If $(P_1, \dots, P_r) \in \mathcal{S}$, and $K_j := \bigcap_{i \neq j} P_i$, then $P_{i_0} \leqslant \bigcap_{j \neq i_0} K_j$ for all $i_0 = 1, \dots, r$. This implies $P_i = \bigcap_{j \neq i} K_j$, since both groups are Sylow p_i-subgroups of G. On the other hand, if $(K_1, \dots, K_r) \in \mathcal{K}$ and $P_j := \bigcap_{i \neq j} K_i$, then $\prod_{j \neq i_0} P_j \leqslant K_{i_0}$ for all $i_0 = 1, \dots, r$. This implies $\prod_{j \neq i} P_j = K_i$, since both groups are Hall p_i'-subgroups of G.

Note that $\mathcal{S}$ and $\mathcal{K}$ are G-sets under the conjugation action of G and that φ and ψ are isomorphisms of G-sets.

9.16 Theorem *(a) Let $(P_1, \dots, P_r)$ and $(Q_1, \dots, Q_r)$ be Sylow systems of G. Then there exists $g \in G$ such that $gP_ig^{-1} = Q_i$ for all $i \in \{1, \dots, r\}$.*

(b) Let $(K_1, \dots, K_r)$ and $(L_1, \dots, L_r)$ be Sylow complement systems of G. Then there exists $g \in G$ such that $gK_ig^{-1} = L_i$ for all $i \in \{1, \dots, r\}$.

Proof Let $|G| = p_1^{e_1} \cdots p_r^{e_r}$.

(b) By the π-Sylow theorem, for fixed $i \in \{1, \ldots, r\}$ all Hall p_i'-subgroups of G are conjugate in G. In particular, G has $[G : N_G(K_i)]$ Hall p_i'-subgroups and $[G : N_G(K_i)]$ divides $[G : K_i] = p^{e_i}$. Therefore, the number of Sylow complement systems of G is $k := \prod_{i=1}^{r} [G : N_G(K_i)]$. Since $[G : N_G(K_i)]$, $i = 1, \ldots, r$, are pairwise coprime, repeated application of Lemma 9.6(d) yields

$$k = \prod_{i=1}^{r} [G : N_G(K_i)] = [G : \bigcap_{i=1}^{r} N_G(K_i)] .$$

Therefore, the stabilizer of $(K_1, \ldots, K_r)$ in G has index k in G, which implies that the G-orbit of $(K_1, \ldots, K_r)$ contains all Sylow complement systems.

(a) This follows immediately from part (b) and Remark 9.15, since the maps φ and ψ are inverse isomorphisms of G-sets. □

10 The Transfer Map

Throughout this section, G denotes a finite group.

10.1 Definition Let $H' \leqslant K \trianglelefteq H \leqslant G$ (in particular, H/K is abelian) and let $\mathcal{R} \subseteq G$ be a set of representatives for G/H. Then, for each $g \in G$ there exist unique elements $\rho(G) \in \mathcal{R}$ and $\eta(g) \in H$ such that $g = \rho(g)\eta(h)$. The function

$$V_{H/K}^G \colon G \longrightarrow H/K\,, \quad g \mapsto \prod_{r\in\mathcal{R}} \eta(gr)K\,,$$

is called the *transfer map* from G to H/K (with respect to $\mathcal{R}$).

10.2 Proposition *Using the notation of Definition 10.1, the function $V_{H/K}^G$ is a group homomorphism which does not depend on the choice of $\mathcal{R}$.*

Proof Let $\mathcal{R}'$ be another set of representatives of G/H and let $\rho' \colon G \to \mathcal{R}'$ and $\eta \colon G \to H$ be such that $g = \rho'(g)\eta'(g)$ for all $g \in G$. Then there exists for each $r \in \mathcal{R}$ a unique $r' \in \mathcal{R}'$ such that $rH = r'H$ and also a unique $h_r \in H$ such that $r' = rh_r$. For any $x \in G$ we therefore have $\rho'(x) = \rho(x)h_{\rho(x)}$. This implies

$$\eta'(gr') = \rho'(gr')^{-1}gr' = \rho'(gr')^{-1}grh_r = h_{\rho(gr)}^{-1}\rho(gr)^{-1}grh_r = h_{\rho(gr)}^{-1}\eta(gr)h_r\,,$$

for all $g \in G$ and $r' \in \mathcal{R}'$. Therefore,

$$\begin{aligned}\prod_{r'\in\mathcal{R}'} \eta'(gr')K &= \prod_{r\in\mathcal{R}} h_{\rho(gr)}^{-1}\eta(gr)h_rK \\ &= \Big(\prod_{r\in\mathcal{R}} \eta(gr)K\Big)\Big(\prod_{r\in\mathcal{R}} h_{\rho(gr)}K\Big)^{-1}\Big(\prod_{r\in\mathcal{R}} h_rK\Big) \\ &= \prod_{r\in\mathcal{R}} \eta(gr)K\,,\end{aligned}$$

for all $g \in G$, since with r also $\rho(gr)$ runs through $\mathcal{R}$. This shows that $V_{H/K}^G$ does not depend on the choice of $\mathcal{R}$.

Next we show that $V_{H/K}^G$ is a homomorphism. Let $g_1, g_2 \in G$. Then, for every $r \in \mathcal{R}$ we have

$$\rho(g_1g_2r)H = g_1g_2rH = g_1\rho(g_2r)H = \rho(g_1\rho(g_2r))H\,,$$

and therefore, $\rho(g_1g_2r) = \rho(g_1\rho(g_2r))$. This implies

$$\begin{aligned} V_{H/K}^G(g_1g_2) &= \prod_{r\in\mathcal{R}} \rho(g_1g_2r)^{-1}g_1g_2rK = \prod_{r\in\mathcal{R}} \rho(g_1\rho(g_2r))^{-1}g_1g_2rK \\ &= \prod_{r\in\mathcal{R}} \rho(g_1\rho(g_2r))^{-1}g_1\rho(g_2r)\rho(g_2r)^{-1}g_2rK = \prod_{r\in\mathcal{R}} \eta(g_1\rho(g_2r))\eta(g_2r)K \\ &= \Big(\prod_{r\in\mathcal{R}} \eta(g_1\rho(g_2r))K\Big)\Big(\prod_{r\in\mathcal{R}} \eta(g_2r)K\Big) = \Big(\prod_{r\in\mathcal{R}} \eta(g_1r)K\Big)\Big(\prod_{r\in\mathcal{R}} \eta(g_2r)K\Big) \\ &= V_{H/K}^G(g_1)V_{H/K}^G(g_2)\,, \end{aligned}$$

and the proposition is proved. □

10.3 Remark Let $H' \leqslant K \trianglelefteq H \leqslant G$ be as in Definition 10.1. In order to calculate $V_{H/K}^G(g)$ for given $g \in G$, we can choose a set $\mathcal{R}$ of representatives which depends on g and makes the computation easier. Note that $\langle g\rangle$ acts on G/H by left translations. Let $r_1H, \dots, r_sH$ be a set of representatives of the $\langle g\rangle$-orbits and let d_i be the length of the orbit of r_iH, for $i = 1, \dots, s$. Then

$$\mathcal{R} := \{r_1, gr_1, \dots, g^{d_1-1}r_1, r_2, gr_2, \dots, r_s, gr_s, \dots, g^{d_s-1}r_s\} \subseteq G$$

is a set of representatives of G/H, $g^{d_i}r_i \in r_iH$, $r_i^{-1}g^{d_i}r_i \in H$ for all $i = 1, \dots, s$, and

$$V_{H/K}^G(g) = \prod_{i=1}^{s} r_i^{-1}g^{d_i}r_iK\,.$$

Note that $d_1 + \cdots + d_s = [G : H]$. If moreover, $r_i^{-1}g^{d_i}r_iK = g^{d_i}K$ for all $i = 1, \dots, s$ (which holds for example if $g \in Z(G)$ or if $H \leqslant Z(G)$), then we obtain

$$V_{H/K}^G(g) = g^{[G:H]}K\,.$$

This implies that $G \to Z(G)$, $g \mapsto g^{[G:Z(G)]}$, is a homomorphism.

10.4 Definition For $H \leqslant G$ we call the group

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

the *focal subgroup* of H with respect of G.

10.5 Remark Let $H \leqslant G$ and set $F := \mathrm{Foc}_G(H)$. Then it is clear that

$$H' \leqslant F \leqslant H \cap G' \leqslant H\,.$$

Therefore, $F \trianglelefteq H$ and H/F is abelian. For $r \in G$ and $h \in H$ with $[r,h] \in H$ we have

$$rhr^{-1}F = rhr^{-1}h^{-1}Fh = [r,h]Fh = Fh = hF\,.$$

With Remark 10.3 we therefore have

$$V_{H/F}^G(h) = h^{[G:H]}F$$

for all $h \in H$.

10.6 Proposition *Let $H \leqslant G$ and $F := \mathrm{Foc}_G(H)$. If $[G:H]$ and $[H:F]$ are coprime, then the following assertions hold:*

(a) $H \cap \ker(V_{H/F}^G) = H \cap G' = \mathrm{Foc}_G(H)$.

(b) $H\ker(V_{H/F}^G) = G$.

(c) $G/G' \cong HG'/G' \times \ker(V_{H/F}^G)/G'$.

(d) $G/\ker(V_{H/F}^G) \cong H/F$.

Proof (a) Since H/F is abelian, also $G/\ker(V_{H/F}^G)$ is abelian by the Homomorphism Theorem. This implies $G' \leqslant \ker(V_{H/F}^G) =: N$ and $F \leqslant H \cap G' \leqslant H \cap N$. On the other hand, if $h \in H \cap N$, then $1 = V_{H/F}^G(h) = h^{[G:H]}F$ by Remark 10.5. Since also $h^{[H:F]}F = 1$ and $[G:H]$ and $[H:F]$ are coprime, we obtain $hF = F$ and $h \in F$.

(b) By (a) we have

$$|G/N| \geqslant |HN/N| = |H/H \cap N| = |H/F| \geqslant |G/N|\,.$$

Therefore, we have equality everywhere and $HN = G$.

(c) By (b) we have $G/G' = (HG'/G')(N/G')$ and by (a) we have $N \cap HG' = (N \cap H)G' = FG' = G'$.

(d) From the proof of (b) we see that $V_{H/F}^G$ is surjective. □

10.7 Definition Let $H \leqslant G$. We set $H_0 := H$ and $H_i := \mathrm{Foc}_G(H_{i-1})$ for $i \in \mathbb{N}$. If $H_n = 1$ for some $n \in \mathbb{N}_0$, then we say that H is *hyperfocal* in G.

10.8 Remark (a) If $H \leqslant G$ is hyperfocal in G and $K \leqslant H$, then also K is hyperfocal in G. In fact, this follows immediately from $\mathrm{Foc}_G(U) \leqslant \mathrm{Foc}_G(V)$, whenever $U \leqslant V \leqslant G$. Moreover, if $H \leqslant U \leqslant G$ and H is hyperfocal in G, then H is also hyperfocal in U. This follows immediately from $\mathrm{Foc}_U(V) \leqslant \mathrm{Foc}_G(V)$, whenever $V \leqslant U \leqslant G$.

(b) Assume the notation from Definition 10.7. Obviously, $Z_i(H) \leqslant H_i$ for all $i \in \mathbb{N}_0$. Therefore, if H is hyperfocal in G, then H is nilpotent.

10.9 Theorem *If $H \leqslant G$ is a hyperfocal Hall subgroup of G, then G has a normal complement in G.*

Proof We proof the assertion by induction on G. If $G = 1$, this is obvious. Therefore, we assume that $G > 1$. We may assume that $H > 1$. Since H is hyperfocal in G, $F := \mathrm{Foc}_G(H) < H$. Using Proposition 10.6, this implies $G/N \cong H/F > 1$ with $N := \ker(V_{H/F}^G)$ and therefore, $N < G$. The subgroup $H \cap N$ is again a Hall subgroup of N (by Remark 9.2(g)) and hyperfocal in N (by Remark 10.8(b)). By induction, there exists a normal complement K of $H \cap N$ in N. As a normal Hall subgroup of N, K is characteristic in N and therefore normal in G. Moreover, $H \cap K = 1$, since if H is a Hall π-subgroup of G, then K is a π'-subgroup of G, and finally, by Proposition 10.6, $HK = H(H \cap N)K = HN = G$. □

10.10 Theorem *Let H be a nilpotent Hall subgroup of G. If any two elements of H which are conjugate in G are also conjugate in H, then H has a normal complement in G.*

Proof We set $H_0 := H$ and $H_i := \mathrm{Foc}_G(H_{i-1})$ for $i \in \mathbb{N}$. By Theorem 10.9, it suffices to show that $H_i = Z_i(H)$ for all $i \in \mathbb{N}_0$. We prove this by induction on i. For $i = 0$, this is clear. So let $i > 0$. By Remark 10.8(b), we have $Z_i(H) \leqslant H_i$. Conversely, if $g \in G$ and $h \in H_{i-1}$ such that $[g,h] \in H_{i-1}$, then $ghg^{-1} \in H_{i-1} \leqslant H$. By the hypothesis in the theorem there exists $k \in H$ such that $ghg^{-1} = khk^{-1}$. From this we obtain

$$[g,h] = ghg^{-1}h^{-1} = khk^{-1}h^{-1} = [k,h] \in [H, H_{i-1}] = [H, Z_{i-1}(H)] = Z_i(H)\,,$$

and the result follows. □

10.11 Lemma *Let P be a Sylow p-subgroup of G and let $A, B \subseteq P$ be subsets such that $xAx^{-1} = A$ and $xBx^{-1} = B$ for all $x \in P$. If there exists $g \in G$ such that $gAg^{-1} = B$, then there also exists $n \in N_G(P)$ such that $nAn^{-1} = B$.*

Proof Let $g \in G$ with $gAg^{-1} = B$. Then $P \leqslant N_G(A) = \{x \in G \mid xAx^{-1} = A\} \leqslant G$ and $P \leqslant N_G(B) = N_G(gAg^{-1}) = gN_G(A)g^{-1} \leqslant G$. Therefore, P and $g^{-1}Pg$ are Sylow p-subgroups of $N_G(A)$ and there exists $y \in N_G(A)$ with $yg^{-1}Pgy^{-1} = P$. Therefore, $n := gy^{-1} \in N_G(P)$ and $nAn^{-1} = gy^{-1}Ayg^{-1} = gAg^{-1} = B$. □

10.12 Theorem (Burnside) *Let P be a Sylow p-subgroup of G such that $N_G(P) = C_G(P)$ ($\iff P \leqslant Z(N_G(P))$). Then P has a normal complement in G. In particular, G is not simple, unless $P = 1$ or $|G| = p$.*

Proof Since $P \leqslant N_G(P) = C_G(P)$, P is abelian. By Lemma 10.11, any two elements $x, y \in P$ which are conjugate in G are also conjugate in $N_G(P) = C_G(P)$ and therefore equal. Now Theorem 10.10 implies the assertion. □

10.13 Theorem *If p is the smallest prime divisor of $|G|$ and if a Sylow p-subgroup P of G is cyclic, then P has a normal complement in G.*

Proof If P is cyclic of order p^n, then $|\mathrm{Aut}(P)| = p^{n-1}(p-1)$. The homomorphism $N_G(P) \to \mathrm{Aut}(P)$, mapping $n \in N_G(P)$ to the conjugation with n, induces a monomorphism $N_G(P)/C_G(P) \to \mathrm{Aut}(P)$. Since p is the smallest prime divisor of G, this implies that $N_G(P)/C_G(P)$ is a p-group. On the other hand, $P \leqslant C_G(P)$, since P is abelian, and $N_G(P)/C_G(P)$ is a p'-group. This implies $N_G(P) = C_G(P)$ and Theorem 10.12 completes the proof. □

10.14 Remark (a) If G has a cyclic Sylow 2-subgroup $P > 1$, then P has a normal complement K in G. In particular, G is not simple, unless $|G| = 2$. Since K has odd order, it is solvable by the Odd-Order-Theorem. Therefore, with $G/K \cong P$ also G is solvable. Using representation theory, one can also show that a finite group with a generalized quaternion Sylow 2-subgroup is not simple.

(b) Theorem 10.13 implies that every group of order $2n$, with n odd, has a normal subgroup of order n.

10.15 Theorem *If all Sylow subgroups of G are cyclic, then G is solvable.*

Proof We prove the theorem by induction on $|G|$. The case $G = 1$ is trivial and we may assume that $G > 1$. Let p be the smallest prime divisor of $|G|$ and let P be a Sylow p-subgroup of G. Then P has a normal complement K by Theorem 10.13. Again, every Sylow subgroup of K is cyclic, and by induction K is solvable. Therefore, with $G/K \cong P$, also G is solvable. □

10.16 Corollary *If G is a group of square free order (i.e., $|G| = p_1 \cdots p_r$ with pairwise distinct primes $p_1, \ldots, p_r$), then G is solvable.*

Proof This is immediate with Theorem 10.15. □

10.17 Theorem *If G is a non-abelian simple group and p is the smallest prime divisor of $|G|$. Then $|G|$ is divisible by 12 or by p^3.*

Proof Let P be a Sylow p-subgroup of G. By Theorem 10.13, P is not cyclic. Therefore, $|P| \geqslant p^2$. If $|P| \geqslant p^3$ we are done. Therefore we assume from now on that $|P| = p^2$. Since P is not cyclic, P is elementary abelian. Therefore, $\mathrm{Aut}(P) \cong \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ and $|N_G(P)/C_G(P)|$ divides $|\mathrm{Aut}(P)| = p(p-1)^2(p+1)$. From Theorem 10.12 we know that $|N_G(P)/C_G(P)| > 1$. Since p is the smallest prime dividing $|G|$ and since $P \leqslant C_G(P)$, we obtain that $|N_G(P)/C_G(P)|$ divides $p+1$. Since p is the smallest prime dividing $|G|$, also $p+1$ has to be prime and we obtain $p = 2$ and $|N_G(P)/C_G(P)| = 3$. This implies that $|G|$ is divisible by 12. □

11 p-Nilpotent Groups

11.1 Definition Let p be a prime. A finite group G is called *p-nilpotent*, if a Sylow p-subgroup of G has a normal complement.

11.2 Remark Let G be a finite group and let p be a prime.

(a) We have

$$\begin{array}{ccc} G \text{ is nilpotent} & \Rightarrow & G\ p\text{-nilpotent} \\ \Downarrow & & \Downarrow \\ G \text{ is solvable} & \Rightarrow & G\ p\text{-solvable} \end{array}$$

(b) Obviously the following statements are equivalent:

(i) G is p-nilpotent.

(ii) Each Sylow p-subgroup of G has a normal complement.

(iii) G has a normal Hall p'-subgroup.

(iv) $G/O_{p'}(G)$ is a p-group.

(v) G has a normal p'-subgroup K such that G/K is a p-group.

(c) If G is p-nilpotent, then $O_{p'}(G)$ is a normal complement of every Sylow p-subgroup of G.

(d) If G is p-nilpotent for every prime p dividing $|G|$, then G is nilpotent. In fact, the homomorphism

$$G \longrightarrow \prod_{p||G|} G/O_{p'}(G), \quad g \mapsto \left(gO_{p'}(G)\right)_{p||G|},$$

has kernel $\bigcap_{p||G|} O_{p'}(G) = 1$, and since both groups have the same order, it is an isomorphism.

(e) If G is p-nilpotent, then every subgroup and every factor group of G is p-nilpotent (cf. Exercise 41).

11.3 Theorem (Frobenius) *Let p be a prime, let G be a finite group, and let P be a Sylow p-subgroup of G. Then the following statements are equivalent:*

(i) *G is p-nilpotent.*

(ii) *For each p-subgroup $Q > 1$ of G, the normalizer $N_G(Q)$ is p-nilpotent.*

(iii) *For each p-subgroup $Q > 1$ of G, the quotient $N_G(Q)/C_G(Q)$ is a p-group.*

(iv) *For each p-subgroup $Q > 1$ of G and each Sylow p-subgroup R of $N_G(Q)$, one has $N_G(Q) = C_G(Q)R$.*

(v) *For each subgroup Q of P and each $g \in G$ with $gQg^{-1} \leqslant P$, there exist $c \in C_G(Q)$ and $x \in P$ such that $g = xc$.*

(vi) *For any two elements $x, y \in P$ and each element $g \in G$ with $y = gxg^{-1}$, there exists an element $u \in P$ such that $y = uxu^{-1}$.*

Proof We may assume that $p \mid |G|$.

(i) $\Rightarrow$ (ii): This follows from Remark 11.2(e).

(ii) $\Rightarrow$ (iii): Let $Q > 1$ be a p-subgroup of G and set $K := O_{p'}(N_G(Q))$. Then, by (ii), $N_G(Q)/K$ is a p-group. In order to prove (iii), it suffices to show that $K \leqslant C_G(Q)$. But for $k \in K$ and $x \in Q$ one has $[k,x] = kxk^{-1}x^{-1} \in K \cap Q = 1$ and therefore, $K \leqslant C_G(Q)$.

(iii) $\Rightarrow$ (iv): Let $Q > 1$ be a p-subgroup of G and let R be a Sylow p-subgroup of $N_G(Q)$. Then $R \cdot C_G(Q)/C_G(Q)$ is a Sylow p-subgroup of $N_G(Q)/C_G(Q)$ by Remark 9.2(g). This implies $N_G(Q)/C_G(Q) = R \cdot C_G(Q)/C_G(Q)$, since $N_G(Q)/C_G(Q)$ is a p-group.

(iv) $\Rightarrow$ (v): Let $Q \leqslant P$ and let $g \in G$ such that $gQg^{-1} \leqslant P$. We may assume that $Q > 1$. By induction on $[P : Q]$ we will show that there exist $c \in C_G(Q)$ and $x \in P$ such that $g = xc$. If $[P : Q] = 1$, then $P = Q$ and $gQg^{-1} \leqslant P$ implies $gQg^{-1} = P$ so that $g \in N_G(P)$. But $N_G(P) = P \cdot C_G(P)$ by (iv) and we can write g in the desired way. From now on we assume that $Q < P$. Then also $gQg^{-1} < P$. For $R_1 := N_P(Q)$ and $R_2 := N_{g^{-1}Pg}(Q)$ we then have $Q < R_1 \leqslant P$ and $Q < R_2 \leqslant g^{-1}Pg$. Let R be a Sylow p-subgroup of $N_G(Q)$ with $R_1 \leqslant R$. Since $N_G(Q) = C_G(Q)R$ (by (iv)), there exists $c \in C_G(Q)$ such that $cR_2c^{-1} \leqslant R$. Let $y \in G$ such that $yRy^{-1} \leqslant P$. Then, by induction applied to $R_1 \leqslant P$ and $yR_1y^{-1} \leqslant P$, there exist $c_1 \in C_G(R_1)$ and $x_1 \in P$ such that $y = x_1c_1$. Similarly, for $gR_2g^{-1} \leqslant P$ and $ycR_2c^{-1}y^{-1} \leqslant yRy^{-1} \leqslant P$, there exist elements $c_2 \in C_G(gR_2g^{-1})$ and $x_2 \in P$ such that $ycg^{-1} = x_2c_2$. Since $C_G(gR_2g^{-1}) = gC_G(R_2)g^{-1}$, there exists $c_3 \in C_G(R_2)$ with $c_2 = gc_3g^{-1}$. This implies $ycg^{-1} = x_2gc_3g^{-1}$, thus $yc = x_2gc_3$, and finally $g = x_2^{-1}ycc_3^{-1} = x_2^{-1}x_1c_1cc_3^{-1}$ with $x_2^{-1}x_1 \in P$ and $c_1cc_3 \in C_G(Q)$.

(v) $\Rightarrow$ (vi): Let $x, y \in P$ and let $g \in G$ such that $y = gxg^{-1}$. If we set $Q := \langle x \rangle$, then $Q \leqslant P$ and $gQg^{-1} = \langle y \rangle \leqslant P$. By (v), there exist $c \in C_G(Q) = C_G(x)$ and $u \in P$ such that $g = uc$, and we have $uxu^{-1} = ucxc^{-1}u^{-1} = gxg^{-1} = y$.

(vi) $\Rightarrow$ (i): This follows from Theorem 10.10. $\square$

11.4 Remark Let G be a finite group and let p be a prime.

(a) One says that a subgroup H of G *controls the fusion of p-subgroups of G*, if there exists a Sylow p-subgroup P of G such that

- $P \leqslant H$ and
- for each $Q \leqslant P$ and each $g \in G$ with $gQg^{-1} \leqslant P$ there exist $h \in H$ and $c \in C_G(Q)$ such that $g = hc$.

In view of Frobenius' Theorem, the p-nilpotent groups are exactly those, for which already the Sylow p-subgroups control the fusion of p-subgroups.

(b) The *rank* of an abelian p-group is defined as the minimal number of generators. For an arbitrary p-group P one defines the *Thompson subgroup* $J(P)$ as the subgroup of P generated by all abelian subgroups of P of maximal rank.

Let p be odd and let P be a Sylow p-subgroup of G. J. Thompson showed that G is p-nilpotent if and only if $C_G(Z(P))$ and $N_G(J(P))$ are p-nilpotent.

12 Group Extensions and Parameter Systems

In this section we will try to find a way to describe for given finite groups K and G all possible groups H which have a normal subgroup which is isomorphic to K and whose factor group is isomorphic to G. We fix K and G throughout this section. We do not require G or K to be finite.

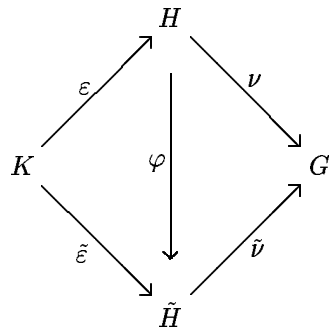
12.1 Definition A *group extension* of G by K is a *short exact sequence*

$$1 \longrightarrow K \xrightarrow{\varepsilon} H \xrightarrow{\nu} G \longrightarrow 1\,,$$

i.e., H is a group, and at each of the three groups K, H, G, the image of the incoming map is equal to the kernel of the outgoing map. Equivalently, ε is injective, $\mathrm{im}(\varepsilon) = \ker(\nu)$, and ν is surjective. We say that the above group extensions is *equivalent* to the group extension

$$1 \longrightarrow K \xrightarrow{\tilde{\varepsilon}} \tilde{H} \xrightarrow{\tilde{\nu}} G \longrightarrow 1$$

if and only if there exists an isomorphism $\varphi\colon H \to \tilde{H}$ such that the diagram



commutes. Obviously, this defines an equivalence relation on the set $\mathrm{ext}(G,K)$ of extensions of G by K. The set of equivalence classes of $\mathrm{ext}(G,K)$ is denoted by $\mathrm{Ext}(G,K)$.

12.2 Remark (a) If $1 \longrightarrow K \xrightarrow{\varepsilon} H \xrightarrow{\nu} G \longrightarrow 1$ is a group extension of G by K, then H has the normal subgroup $\varepsilon(K)$ with factor group $H/\varepsilon(K) = H/\ker(\nu) \cong G$. Conversely, whenever H is a group having a normal subgroup N such that $N \cong K$ and $H/N \cong G$, then there is a group extension $1 \longrightarrow K \xrightarrow{\varepsilon} H \xrightarrow{\nu} G \longrightarrow 1$, where ε is the composition of the isomorphism $K \cong N$ and the inclusion $N \leqslant H$, and ν is the composition of the natural epimorphism $H \twoheadrightarrow H/N$ and the isomorphism $H/N \cong G$. Moreover, if $1 \longrightarrow K \xrightarrow{\varepsilon} H \xrightarrow{\nu} G \longrightarrow 1$ and $1 \longrightarrow K \xrightarrow{\tilde{\varepsilon}} \tilde{H} \xrightarrow{\tilde{\nu}} G \longrightarrow 1$ are equivalent extensions then H and $\tilde{H}$ are isomorphic by definition. Warning: the converse is not true. There are examples of group extensions of K by G which are not equivalent but involve isomorphic groups H and $\tilde{H}$.

(b) Two group extensions $1 \longrightarrow K \xrightarrow{\varepsilon} H \xrightarrow{\nu} G \longrightarrow 1$ and $1 \longrightarrow K \xrightarrow{\tilde{\varepsilon}} \tilde{H} \xrightarrow{\tilde{\nu}} G \longrightarrow 1$ are already equivalent if there exists a homomorphism $\varphi\colon H \to \tilde{H}$ which makes the diagram in Definition 12.1 commutative. In fact, it is easy to see that in this case φ has to be an isomorphism.

12.3 Proposition *Let $1 \longrightarrow K \xrightarrow{\varepsilon} H \xrightarrow{\nu} G \longrightarrow 1$ be a group extension of G by K. For each $x \in G$, let $h_x \in H$ be such that $\nu(h_x) = x$. Then the following hold:*

(a) *For every $h \in H$ there exist unique elements $x \in G$ and $a \in K$ such that $h = h_x\varepsilon(a)$.*

(b) *For every $x \in G$ and $a \in K$ there exists a unique element $\alpha_x(a) \in K$ such that $\varepsilon(\alpha_x(a)) = h_x\varepsilon(a)h_x^{-1}$. Moreover, $\alpha_x \in \mathrm{Aut}(K)$.*

(c) *For every $x, y \in G$ there exists a unique element $\kappa(x,y) \in K$ such that $h_xh_y = \varepsilon(\kappa(x,y))h_{xy}$. In particular, $h_1 = \varepsilon(\kappa(1,1))$. Moreover, $\alpha_x \circ \alpha_y = c_{\kappa(x,y)}\alpha_{xy}$, where $c_a \in \mathrm{Aut}(K)$ denotes the conjugation automorphism $k \mapsto aka^{-1}$ for $a \in K$.*

(d) *For every $x, y, z \in G$ on has $\kappa(x,y)\kappa(xy,z) = \alpha_x(\kappa(y,z))\kappa(x,yz)$.*

(e) *Let also $h'_x \in H$ be such that $\nu(h'_x) = x$ for all $x \in G$. Then there exists a unique function $g\colon K \to G$ such that $h'_x = h_x \cdot \varepsilon(g(x))$ for all $x \in G$. If $\alpha'\colon G \to \mathrm{Aut}(K)$ and $\kappa'\colon G \times G \to K$ are constructed from h'_x, $x \in G$, then*

$$\alpha'_x = c_{f(x)} \circ \alpha_x \quad \text{and} \quad \kappa'(x,y) = f(x) \cdot \alpha_x(f(y)) \cdot \kappa(x,y) \cdot f(xy)^{-1}$$

for all $x, y \in G$, where $f\colon G \to K$ is defined by $f(x) := \alpha_x(g(x))$ for all $x \in G$.

Proof (a) Let $h \in H$ and set $x := \nu(h)$. Then $\nu(h_x^{-1}h) = \nu(h_x)^{-1}\nu(h) = x^{-1}x = 1$ and there exists $a \in K$ such that $\varepsilon(a) = h_x^{-1}h$. Assume that also $h = h_y\varepsilon(b)$ for $y \in G$ and $b \in K$. Then $x = \nu(h) = \nu(h_y)\nu(\varepsilon(b)) = y \cdot 1 = y$ and therefore $\varepsilon(a) = \varepsilon(b)$. Since ε is injective, also $a = b$.

(b) For $x \in G$ and $a \in K$, we have $h_x\varepsilon(a)h_x^{-1} \in \ker(\nu) = \mathrm{im}(\varepsilon)$. Therefore, there exists $b \in K$ with $\varepsilon(b) = h_x\varepsilon(a)h_x^{-1}$. Since ε is injective, $b \in K$ is unique. We set $\alpha_x(a) := b$.

Let $a, b \in K$ and $x \in G$. Then $\alpha_x(a)\alpha_x(b) \in K$ and

$$\begin{aligned}\varepsilon(\alpha_x(a)\alpha_x(b)) &= \varepsilon(\alpha_x(a))\varepsilon(\alpha_x(b)) = h_x\varepsilon(a)h_x^{-1}h_x\varepsilon(b)h_x^{-1} \\ &= h_x\varepsilon(ab)h_x^{-1} = \varepsilon(\alpha_x(ab))\,.\end{aligned}$$

Since ε is injective, we have $\alpha_x(a)\alpha_x(b) = \alpha_x(ab)$ and α_x is a group homomorphism from K to K. If $\alpha_x(a) = 1$, then $1 = \varepsilon(\alpha_x(a)) = h_x\varepsilon(a)h_x^{-1}$ and therefore, $\varepsilon(a) = 1$. Since ε is injective, also $a = 1$. This shows that α_x is injective. Finally, let $b \in K$ be arbitrary. Then $h_x^{-1}\varepsilon(b)h_x \in \ker(\nu) = \mathrm{im}(\varepsilon)$ and there exists $a \in K$ such that $h_x^{-1}\varepsilon(b)h_x = \varepsilon(a)$. This implies $b = \alpha_x(a)$ and α_x is surjective.

(c) Let $x, y \in G$. Then $\nu(h_xh_yh_{xy}^{-1})) = xy(xy)^{-1} = 1$ and there exists a unique element $a \in K$ such that $\varepsilon(a) = h_xh_yh_{xy}^{-1}$. We set $\kappa(x,y) := a$. For

$x, y \in G$ and $a \in K$ we then have

$$\begin{aligned}\varepsilon(\alpha_x(\alpha_y(a))) &= h_x\varepsilon(\alpha_y(a))h_x^{-1} = h_xh_y\varepsilon(a)h_y^{-1}h_x^{-1}\\ &= h_xh_yh_{xy}^{-1}h_{xy}\varepsilon(a)h_{xy}^{-1}h_{xy}h_y^{-1}h_x^{-1}\\ &= \varepsilon(\kappa(x,y))h_{xy}\varepsilon(a)h_{xy}^{-1}\varepsilon(\kappa(x,y))^{-1}\\ &= \varepsilon(\kappa(x,y))\varepsilon(\alpha_{xy}(a))\varepsilon(\kappa(x,y))^{-1}\\ &= \varepsilon(\kappa(x,y)\alpha_{xy}(a)\kappa(x,y)^{-1})\,,\end{aligned}$$

and the injectivity of ε implies $(\alpha_x \circ \alpha_y)(a) = (c_{\kappa(x,y)} \circ \alpha_{xy})(a)$.

(d) Let $x, y, z \in G$. Then

$$\begin{aligned}\varepsilon\big(\kappa(x,y)\kappa(xy,z)\big)h_{xyz} &= \varepsilon(\kappa(x,y))\varepsilon(\kappa(xy,z))h_{(xy)z} = \varepsilon(\kappa(x,y))h_{xy}h_z\\ &= (h_xh_y)h_z\end{aligned}$$

and

$$\begin{aligned}\varepsilon\big(\alpha_x(\kappa(y,z))\kappa(x,yz)\big)h_{xyz} &= \varepsilon(\alpha_x(\kappa(y,z)))\varepsilon(\kappa(x,yz))h_{x(yz)}\\ &= h_x\varepsilon(\kappa(y,z))h_x^{-1}h_xh_{yz} = h_x\varepsilon(\kappa(y,z))h_{yz}\\ &= h_x(h_yh_z)\,.\end{aligned}$$

Now the injectivity of ε implies the desired equation.

(e) Let $x \in G$. Since $\nu(h_x^{-1}h'_x) = x^{-1}x = 1$, there exists a unique element $g(x) \in K$ such that $\varepsilon(g(x)) = h_x^{-1}h'_x$. Moreover, for each $a \in K$ and $x \in G$ we have

$$\varepsilon(\alpha'_x(a)) = h'_x\varepsilon(a){h'_x}^{-1} = h_x\varepsilon(g(x)ag(x)^{-1})h_x^{-1}\,,$$

which implies $\alpha'_x(a) = \alpha_x(g(x)ag(x)^{-1})$ and $\alpha'_x = c_{\alpha_x(g(x))} \circ \alpha_x = c_{f(x)} \circ \alpha_x$. Moreover, for all $x, y \in G$ we have

$$\begin{aligned}\varepsilon(\kappa'(x,y)) &= h'_x \cdot h'_y \cdot {h'_{xy}}^{-1}\\ &= h_x \cdot \varepsilon(g(x)) \cdot h_y \cdot \varepsilon(g(y)) \cdot \varepsilon(g(xy))^{-1} \cdot h_{xy}^{-1}\\ &= h_x \cdot \varepsilon(g(x)) \cdot h_x^{-1} \cdot h_x \cdot h_y \cdot h_{xy}^{-1} \cdot h_{xy} \cdot \varepsilon(g(y)g(xy)^{-1}) \cdot h_{xy}^{-1}\\ &= \varepsilon(\alpha_x(g(x))) \cdot \varepsilon(\kappa(x,y)) \cdot \varepsilon(\alpha_{xy}(g(y)g(xy)^{-1}))\\ &= \varepsilon\big[\alpha_x(g(x)) \cdot \kappa(x,y) \cdot \alpha_{xy}(g(y)) \cdot \alpha_{xy}(g(xy))^{-1}\big]\\ &= \varepsilon\big[f(x) \cdot \kappa(x,y) \cdot \alpha_{xy}(g(y)) \cdot \kappa(x,y)^{-1} \cdot \kappa(x,y) \cdot f(xy)^{-1}\big]\\ &= \varepsilon\big[f(x) \cdot \alpha_x(\alpha_y(g(y))) \cdot \kappa(x,y) \cdot f(xy)^{-1}\big]\\ &= \varepsilon\big[f(x) \cdot \alpha_x(f(y)) \cdot \kappa(x,y) \cdot f(xy)^{-1}\big]\,.\end{aligned}$$

Since ε is injective, this implies the desired equation. □

12.4 Definition (a) A *parameter system* of G in K is a pair (α, κ) of maps $\alpha\colon G \to \mathrm{Aut}(K)$, $x \mapsto \alpha_x$, and $\kappa\colon G \times G \to K$ with the following properties:

(i) For every $x, y \in G$ one has $\alpha_x \circ \alpha_y = c_{\kappa(x,y)} \circ \alpha_{xy}$.

(ii) For every $x, y, z \in G$ one has $\kappa(x,y)\kappa(xy,z) = \alpha_x(\kappa(y,z))\kappa(x,yz)$.

We call α the *automorphism system* and κ the *factor system* of (α, κ), and we denote the set of parameter systems of G in K by $\mathrm{par}(G,K)$.

(b) The set $F(G,K)$ of functions from G to K is a group under the multiplication $(fg)(x) := f(x)g(x)$ for $f, g\colon G \to K$ and $x \in G$. If $(\alpha, \kappa) \in \mathrm{par}$ and $f\colon G \to K$ we set ${}^f(\alpha, \kappa) := (\alpha', \kappa')$ with

$$\alpha'_x := c_{f(x)} \circ \alpha_x\,, \quad \text{and} \quad \kappa'(x,y) := f(x)\alpha_x(f(y))\kappa(x,y)f(xy)^{-1}\,,$$

for $x, y \in G$. As the next lemma shows, this defines a group action of $F(G,K)$ on the set $\mathrm{par}(G,K)$. We call two parameter systems of G in K *equivalent* if they belong to the same $F(G,K)$-orbit and we denote the set of equivalence classes by $\mathrm{Par}(G,K)$.

12.5 Lemma *(a) Let $(\alpha, \kappa) \in \mathrm{par}(G,K)$. Then $\alpha_1 = c_{\kappa(1,1)}$, $\kappa(1,1) = \kappa(1,z)$, and $\kappa(x,1) = \alpha_x(\kappa(1,1))$ for all $x, z \in G$.*

(b) The definition of ${}^f(\alpha, \kappa)$ in Definition 12.4(b) defines a group action of $F(G,K)$ on $\mathrm{par}(G,K)$.

Proof (a) By Proposition 12.3(c), we have $\alpha_1 \circ \alpha_1 = c_{\kappa(1,1)} \circ \alpha_1$ which implies $\alpha_1 = c_{\kappa(1,1)}$. For $z \in G$, this and Proposition 12.3(d) imply

$$\kappa(1,1)\kappa(1\cdot 1, z) = \alpha_1(\kappa(1,z))\kappa(1, 1\cdot z) = \kappa(1,1)\kappa(1,z)\kappa(1,1)^{-1}\kappa(1,z)\,.$$

Therefore, $\kappa(1,z) = \kappa(1,1)$. For $x \in G$, Proposition 12.3(d) implies $\kappa(x, 1\cdot 1)\kappa(x\cdot 1, 1) = \alpha_x(\kappa(1,1))\kappa(x, 1\cdot 1)$. This implies $\kappa(x,1) = \alpha_x(\kappa(1,1))$.

(b) Let $f, g \in F(G,K)$ and $\kappa \in \mathrm{par}(G,K)$. We set $(\alpha', \kappa') := {}^f(\alpha, \kappa)$ and $(\alpha'', \kappa'') := {}^g(\alpha', \kappa')$. For all $x, y \in G$, we then have

$$\alpha''_x = c_{g(x)} \circ \alpha'_x = c_{g(x)} \circ c_{f(x)} \circ \alpha_x = c_{g(x)f(x)} \circ \alpha_x = c_{(fg)(x)} \circ \alpha_x$$

and

$$\begin{aligned}\kappa''(x,y) &= g(x)\alpha'_x(g(y))\kappa'(x,y)g(xy)^{-1} \\ &= g(x)f(x)\alpha_x(g(y))f(x)^{-1}f(x)\alpha_x(f(y))\kappa(x,y)f(xy)^{-1}g(xy)^{-1} \\ &= (gf)(x)\cdot\alpha_x((gf)(y))\cdot\kappa(x,y)\cdot(gf)(xy)^{-1}\,.\end{aligned}$$

This implies that $(\alpha'', \kappa'') = {}^{gf}(\alpha, \kappa)$. If $f = 1$, then $\alpha'_x = \alpha_x$ by definition and $\kappa'(x,y) = \alpha_x(1)\kappa(x,y) = \kappa(x,y)$ for all $x, y \in G$. Therefore, ${}^1(\alpha, \kappa) = (\alpha, \kappa)$. We still have to show that (α', κ') is again a parameter system. For $x, y, z \in G$, we have

$$\begin{aligned}\alpha'_x \circ \alpha'_y &= c_{f(x)} \circ \alpha_x \circ c_{f(y)} \circ \alpha_y = c_{f(x)} \circ \alpha_x \circ c_{f(y)} \circ \alpha_x^{-1} \circ \alpha_x \circ \alpha_y \\ &= c_{f(x)} \circ c_{\alpha_x(f(y))} \circ c_{\kappa(x,y)} \circ \alpha_{xy} = c_{f(x)\alpha_x(f(y))\kappa(x,y)} \circ c^{-1}_{f(xy)} \circ \alpha'_{xy} \\ &= c_{\kappa'(x,y)} \circ \alpha'_{xy}\end{aligned}$$

and

$$\begin{aligned}
&\kappa'(x,y)\kappa'(xy,z)\\
&= f(x)\alpha_x(f(y))\kappa(x,y)f(xy)^{-1}f(xy)\alpha_{xy}(f(z))\kappa(xy,z)f(xyz)^{-1}\\
&= f(x)\alpha_x(f(y))\kappa(x,y)\alpha_{xy}(f(z))\kappa(x,y)^{-1}\kappa(x,y)\kappa(xy,z)f(xyz)^{-1}\\
&= f(x)\alpha_x(f(y))\alpha_x(\alpha_y(f(z)))\alpha_x(\kappa(y,z))\kappa(x,yz)f(xyz)^{-1}\\
&= f(x)\alpha_x\big(f(y)\alpha_y(f(z))\kappa(y,z)f(yz)^{-1}\big)\alpha_x(f(yz))\kappa(x,yz)f(xyz)^{-1}\\
&= \alpha'_x(\kappa'(y,z))f(x)\alpha_x(f(yz))\kappa(x,yz)f(xyz)^{-1}\\
&= \alpha'_x(\kappa'(y,z))\kappa'(x,yz)\,.
\end{aligned}$$

This implies that $(\alpha',\kappa') \in \mathrm{par}(G,K)$. □

12.6 Proposition *Let $(\alpha,\kappa) \in \mathrm{par}(G,K)$. Then the set $K \times G$ together with the multiplication*

$$(a,x)(b,y) := (a \cdot \alpha_x(b) \cdot \kappa(x,y), xy)\,, \quad \text{for } a,b \in K,\ x,y \in G,$$

is a group with identity element $(\kappa(1,1)^{-1},1)$ and inverse element $(a,x)^{-1} = (\kappa(1,1)^{-1}\kappa(x^{-1},x)^{-1}\alpha_{x^{-1}}(a)^{-1}, x^{-1})$. Moreover, the functions $\varepsilon\colon K \to K \times G$, $a \mapsto (\kappa(1,1)^{-1}a,1)$, and $\nu\colon K \times G \to G$, $(a,x) \mapsto x$, are group homomorphisms such that $1 \longrightarrow K \xrightarrow{\varepsilon} H \xrightarrow{\nu} G \longrightarrow 1$ is a group extension of G by K.

Proof First we prove associativity. Let $a,b,c \in K$ and $x,y,z \in G$. Then

$$\begin{aligned}
[(a,x)(b,y)](c,z) &= (a\alpha_x(b)\kappa(x,y), xy)(c,z)\\
&= (a\alpha_x(b)\kappa(x,y)\alpha_{xy}(c)\kappa(xy,z), xyz)
\end{aligned}$$

and

$$\begin{aligned}
(a,x)[(b,y)(c,z)] &= (a,x)(b\alpha_y(c)\kappa(y,z), yz)\\
&= (a\alpha_x(b\alpha_y(c)\kappa(y,z))\kappa(x,yz), xyz)\\
&= (a\alpha_x(b)\alpha_x(\alpha_y(c))\alpha_x(\kappa(y,z))\kappa(x,yz), xyz)\\
&= (a\alpha_x(b)\kappa(x,y)\alpha_{xy}(c)\kappa(x,y)^{-1}\kappa(x,y)\kappa(xy,z), xyz)\\
&= (a\alpha_x(b)\kappa(x,y)\alpha_{xy}(c)\kappa(xy,z), xyz)\,.
\end{aligned}$$

Next we show that $(\kappa(1,1)^{-1},1)$ is a left identity element. In fact, for $b \in K$ and $y \in G$ we have

$$\begin{aligned}
(\kappa(1,1)^{-1},1)(b,y) &= (\kappa(1,1)^{-1}\alpha_1(b)\kappa(1,y), 1\cdot y)\\
&= (\kappa(1,1)^{-1}\kappa(1,1)b\kappa(1,1)^{-1}\kappa(1,y), y) = (b,y)\,.
\end{aligned}$$

Moreover, for $b \in K$ and $y \in G$ we have

$$\begin{aligned}
&(\kappa(1,1)^{-1}\kappa(y^{-1},y)^{-1}\alpha_{y^{-1}}(b)^{-1}, y^{-1})(b,y)\\
&= (\kappa(1,1)^{-1}\kappa(y^{-1},y)^{-1}\alpha_{y^{-1}}(b)^{-1}\alpha_{y^{-1}}(b)\kappa(y^{-1},y), y^{-1}y)\\
&= (\kappa(1,1)^{-1},1)\,.
\end{aligned}$$

This shows that H is a group.

For $a, b \in K$ we have

$$\begin{aligned}\varepsilon(a)\varepsilon(b) &= (\kappa(1,1)^{-1}a, 1)(\kappa(1,1)^{-1}b, 1)\\ &= (\kappa(1,1)^{-1}a\alpha_1(\kappa(1,1)^{-1}b)\kappa(1,1), 1\cdot 1)\\ &= (\kappa(1,1)^{-1}a\kappa(1,1)\kappa(1,1)^{-1}b\kappa(1,1)^{-1}\kappa(1,1), 1)\\ &= (\kappa(1,1)^{-1}ab, 1) = \varepsilon(ab)\,,\end{aligned}$$

which shows that ε is a homomorphism. Obviously, ε is injective. For all $a, b \in K$ and $x, y \in G$, we have

$$\nu((a,x)(b,y)) = \nu(a\alpha_x(b)\kappa(x,y), xy) = xy = \nu(a,x)\nu(b,y)\,,$$

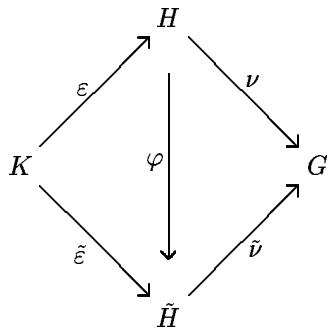
which shows that ν is a homomorphism. Obviously, ν is surjective. Finally, for $a \in K$ and $x \in G$ we have

$$(a,x) \in \ker(\nu) \iff x = 1 \iff (a,x) \in \varepsilon(K)\,,$$

and the proof is complete. □

12.7 Theorem (Schreier) *The constructions in Proposition 12.3 and Proposition 12.6 induce mutually inverse bijections between* $\mathrm{Ext}(G,K)$ *and* $\mathrm{Par}(G,K)$.

Proof First assume that $1 \longrightarrow K \xrightarrow{\varepsilon} H \xrightarrow{\nu} G \longrightarrow 1$ and $1 \longrightarrow K \xrightarrow{\tilde{\varepsilon}} \tilde{H} \xrightarrow{\tilde{\nu}} G \longrightarrow 1$ are equivalent group extensions of G by K. Then there exists an isomorphism $\varphi\colon H \to \tilde{H}$ such that the diagram



is commutative. For each $x \in G$ let $h_x \in H$ such that $\nu(h_x) = x$ and assume that $\alpha\colon G \to \mathrm{Aut}(K)$ and $\kappa\colon G \times G \to K$ is constructed as in Proposition 12.3; i.e.,

$$\varepsilon(\alpha_x(a)) = h_x\varepsilon(a)h_x^{-1} \quad \text{and} \quad h_xh_y = \varepsilon(\kappa(x,y))h_{xy}$$

for all $x, y \in G$ and $a \in K$. We set $\tilde{h}_x := \varphi(h_x)$ for each $x \in G$. Then, $\tilde{\nu}(\tilde{h}_x) = \tilde{\nu}(\varphi(h_x)) = \nu(h_x) = x$ for each x and we can use the elements $\tilde{h}_x$ in

order to construct a parameter system $(\tilde{\alpha}, \tilde{\kappa})$ associated to the group extension $1 \longrightarrow K \xrightarrow{\tilde{\varepsilon}} \tilde{H} \xrightarrow{\tilde{\nu}} G \longrightarrow 1$. But applying φ to the two above equations we obtain

$$\tilde{\varepsilon}(\alpha_x(a)) = \tilde{h}_x \tilde{\varepsilon}(a) \tilde{h}_x^{-1} \quad \text{and} \quad \tilde{h}_x \tilde{h}_y = \tilde{\varepsilon}(\kappa(x,y)) \tilde{h}_{xy}^{-1} .$$

This implies that $\tilde{\alpha} = \alpha$ and $\tilde{\kappa} = \kappa$. Therefore, the construction in Proposition 12.3 induces a map

$$\Phi \colon \operatorname{Ext}(G,K) \longrightarrow \operatorname{Par}(G,K) .$$

Next let $(\alpha, \kappa) \in \operatorname{par}(G,K)$, $f \in F(G,K)$, and set $(\tilde{\alpha}, \tilde{\kappa}) := {}^f(\alpha, \kappa)$. Moreover, let $1 \longrightarrow K \xrightarrow{\varepsilon} H \xrightarrow{\nu} G \longrightarrow 1$ and $1 \longrightarrow K \xrightarrow{\tilde{\varepsilon}} \tilde{H} \xrightarrow{\tilde{\nu}} G \longrightarrow 1$ be the group extensions associated to (α, κ) and $(\tilde{\alpha}, \tilde{\kappa})$ by the construction in Proposition 12.6. We want to show that they are equivalent. We define $\varphi \colon H \to \tilde{H}$ by

$$\varphi(a,x) := \big(da\alpha_x(d)^{-1} f(x)^{-1}, x\big) \quad \text{with} \quad d := \kappa(1,1)^{-1} f(1)^{-1} \kappa(1,1) .$$

For all $a, b \in K$ and $x, y \in G$ we have

$$\begin{aligned}
\varphi(a,x)\varphi(b,y) &= (da\alpha_x(d)^{-1} f(x)^{-1}, x) \cdot (db\alpha_y(d)^{-1} f(y)^{-1}, y) \\
&= (da\alpha_x(d)^{-1} f(x)^{-1} \tilde{\alpha}_x(db\alpha_y(d)^{-1} f(y)^{-1}) \tilde{\kappa}(x,y), xy) \\
&= (da\alpha_x(d)^{-1} f(x)^{-1} f(x) \alpha_x(db\alpha_y(d)^{-1} f(y)^{-1}) f(x)^{-1} \cdot \\
&\qquad \cdot f(x)\alpha_x(f(y))\kappa(x,y) f(xy)^{-1}, xy) \\
&= (da\alpha_x(b)\alpha_x(\alpha_y(d))^{-1} \kappa(x,y) f(xy)^{-1}, xy)
\end{aligned}$$

and

$$\begin{aligned}
\varphi((a,x)(b,y)) &= \varphi(a\alpha_x(b)\kappa(x,y), xy) \\
&= (da\alpha_x(b)\kappa(x,y)\alpha_{xy}(d)^{-1} f(xy)^{-1}, xy) \\
&= (da\alpha_x(b)\kappa(x,y)\alpha_{xy}(d)^{-1} \kappa(x,y)^{-1} \kappa(x,y) f(xy)^{-1}, xy) \\
&= (da\alpha_x(b)\alpha_x(\alpha_y(d))^{-1} \kappa(x,y) f(xy)^{-1}, xy) .
\end{aligned}$$

This implies that φ is a homomorphism. Moreover, for $a \in K$ and $x \in G$, we have

$$\begin{aligned}
\varphi(\varepsilon(a)) = \varphi(\kappa(1,1)^{-1} a, 1) &= (d\kappa(1,1)^{-1} a\alpha_1(d)^{-1} f(1)^{-1}, 1) \\
&= (\kappa(1,1)^{-1} f(1)^{-1} a\kappa(1,1) d^{-1} \kappa(1,1)^{-1} f(1)^{-1}, 1) \\
&= (\kappa(1,1)^{-1} f(1)^{-1} a, 1)) = (\tilde{\kappa}(1,1)^{-1} a, 1) = \tilde{\varepsilon}(a)
\end{aligned}$$

and

$$\tilde{\nu}(\varphi(a,x)) = \tilde{\nu}(da\alpha_x(d)^{-1} f(x)^{-1}, x) = x = \nu(x) .$$

Together with Remark 12.2(b), this implies that the two group extensions $1 \longrightarrow K \xrightarrow{\varepsilon} H \xrightarrow{\nu} G \longrightarrow 1$ and $1 \longrightarrow K \xrightarrow{\tilde{\varepsilon}} \tilde{H} \xrightarrow{\tilde{\nu}} G \longrightarrow 1$ are equivalent. Therefore, the construction in Proposition 12.6 induces a map

$$\Psi\colon \operatorname{Par}(G,K) \longrightarrow \operatorname{Ext}(G,K)\,.$$

Finally, we show that Φ and Ψ are mutually inverse bijections. Let $1 \longrightarrow K \xrightarrow{\varepsilon} H \xrightarrow{\nu} G \longrightarrow 1$ be a group extension and, for each $x \in G$, let $h_x \in H$ be such that $\nu(h_x) = x$. Moreover, let (α,κ) be the parameter system defined in Proposition 12.3 from h_x, $x \in G$, and let $1 \longrightarrow K \xrightarrow{\tilde{\varepsilon}} \tilde{H} \xrightarrow{\tilde{\nu}} G \longrightarrow 1$ be the group extension constructed from (α,κ) according to Proposition 12.6. We show that the two group extensions $1 \longrightarrow K \xrightarrow{\varepsilon} H \xrightarrow{\nu} G \longrightarrow 1$ and $1 \longrightarrow K \xrightarrow{\tilde{\varepsilon}} \tilde{H} \xrightarrow{\tilde{\nu}} G \longrightarrow 1$ are equivalent. In fact, let $\varphi\colon \tilde{H} \to H$ be defined by

$$\varphi(a,x) := \varepsilon(\kappa(1,1)a\kappa(x,1)^{-1})h_x\,,$$

for all $a,b \in K$ and $x,y \in G$. Then

$$\begin{aligned}\varphi((a,x)(b,y)) &= \varphi(a\alpha_x(b)\kappa(x,y),xy)\\ &= \varepsilon\big(\kappa(1,1)a\alpha_x(b)\kappa(x,y)\kappa(xy,1)^{-1}\big)h_{xy}\\ &= \varepsilon\big(\kappa(1,1)a\alpha_x(b)\alpha_x(\kappa(y,1))^{-1}\kappa(x,y)\big)h_{xy}\\ &= \varepsilon\big(\kappa(1,1)a\alpha_x(b)\alpha_x(\kappa(y,1))^{-1}\big)h_xh_y\end{aligned}$$

and

$$\begin{aligned}\varphi(a,x)\varphi(b,y) &= \varepsilon\big(\kappa(1,1)a\kappa(x,1)^{-1}\big)h_x\varepsilon\big(\kappa(1,1)b\kappa(y,1)^{-1}\big)h_y\\ &= \varepsilon\big(\kappa(1,1)a\kappa(x,1)^{-1}\big)\varepsilon\big(\alpha_x(\kappa(1,1)b\kappa(y,1)^{-1})\big)h_xh_y\\ &= \varepsilon\big(\kappa(1,1)a\kappa(x,1)^{-1}\alpha_x(\kappa(1,1))\alpha_x(b)\alpha_x(\kappa(y,1))^{-1}\big)h_xh_y\\ &= \varepsilon\big(\kappa(1,1)a\alpha_x(b)\alpha_x(\kappa(y,1))^{-1}\big)h_xh_y\,.\end{aligned}$$

This shows that φ is a homomorphism. Moreover, for $a \in K$ and $x \in G$ we have

$$\begin{aligned}\varphi(\tilde{\varepsilon}(a)) &= \varphi(\kappa(1,1)^{-1}a,1) = \varepsilon(\kappa(1,1)\kappa(1,1)^{-1}a\kappa(1,1)^{-1})h_1\\ &= \varepsilon(a)\varepsilon(\kappa(1,1))^{-1}h_1 = \varepsilon(a)\,,\end{aligned}$$

by Proposition 12.3(c), and

$$\nu(\varphi(a,x)) = \nu(\varepsilon(\kappa(1,1)a\kappa(x,1)^{-1})h_x) = \nu(h_x) = x = \tilde{\nu}(a,x)\,.$$

Therefore, the two group extensions $1 \longrightarrow K \xrightarrow{\varepsilon} H \xrightarrow{\nu} G \longrightarrow 1$ and $1 \longrightarrow K \xrightarrow{\tilde{\varepsilon}} \tilde{H} \xrightarrow{\tilde{\nu}} G \longrightarrow 1$ are equivalent, and $\Psi \circ \Phi = \mathrm{id}$.

Now let $(\alpha,\kappa) \in \operatorname{par}(G,K)$ and let $1 \longrightarrow K \xrightarrow{\varepsilon} H \xrightarrow{\nu} G \longrightarrow 1$ be the group extension constructed in Proposition 12.6. We set

$$h_x := (\kappa(1,1)^{-1}\kappa(x,1),x) \in H\,,$$

for $x \in G$ and observe that $\nu(h_x) = x$. Let $x \in G$ and $a \in K$, then

$$\begin{aligned} h_x\varepsilon(a) &= (\kappa(1,1)^{-1}\kappa(x,1),x)\cdot(\kappa(1,1)^{-1}a,1) \\ &= (\kappa(1,1)^{-1}\kappa(x,1)\alpha_x(\kappa(1,1))^{-1}\alpha_x(a)\kappa(x,1),x) \\ &= (\kappa(1,1)^{-1}\alpha_x(a)\kappa(x,1),x) \end{aligned}$$

and

$$\begin{aligned} \varepsilon(\alpha_x(a))h_x &= (\kappa(1,1)^{-1}\alpha_x(a),1)\cdot(\kappa(1,1)^{-1}\kappa(x,1),x) \\ &= (\kappa(1,1)^{-1}\alpha_x(a)\alpha_1(\kappa(1,1)^{-1}\kappa(x,1))\kappa(1,x),x) \\ &= (\kappa(1,1)^{-1}\alpha_x(a)\kappa(x,1)\kappa(1,1)^{-1}\kappa(1,x),x) \\ &= (\kappa(1,1)^{-1}\alpha_x(a)\kappa(x,1),x)\,. \end{aligned}$$

Moreover, for all $x, y \in G$ we have

$$\begin{aligned} h_xh_y &= (\kappa(1,1)^{-1}\kappa(x,1),x)\cdot(\kappa(1,1)^{-1}\kappa(y,1),y) \\ &= (\kappa(1,1)^{-1}\kappa(x,1)\alpha_x(\kappa(1,1))^{-1}\alpha_x(\kappa(y,1))\kappa(x,y),xy) \\ &= (\kappa(1,1)^{-1}\alpha_x(\kappa(y,1))\kappa(x,y),xy) \\ &= (\kappa(1,1)^{-1}\kappa(x,y)\kappa(xy,1),xy) \end{aligned}$$

and

$$\begin{aligned} \varepsilon(\kappa(x,y))h_{xy} &= (\kappa(1,1)^{-1}\kappa(x,y),1)\cdot(\kappa(1,1)^{-1}\kappa(xy,1),xy) \\ &= (\kappa(1,1)^{-1}\kappa(x,y)\alpha_1(\kappa(1,1)^{-1}\kappa(xy,1))\kappa(1,xy),xy) \\ &= (\kappa(1,1)^{-1}\kappa(x,y)\kappa(xy,1)\kappa(1,1)^{-1}\kappa(1,xy),xy) \\ &= (\kappa(1,1)^{-1}\kappa(x,y)\kappa(xy,1),xy) \end{aligned}$$

This shows that the parameter system constructed from the group extension $1 \longrightarrow K \xrightarrow{\varepsilon} H \xrightarrow{\nu} G \longrightarrow 1$ equals (α,κ). Therefore $\Phi\circ\Psi = \mathrm{id}$, and the proof is complete. □

12.8 Proposition *Let $1 \longrightarrow K \xrightarrow{\varepsilon} H \xrightarrow{\nu} G \longrightarrow 1$ be a group extension of G by K. Then the following are equivalent:*

(i) *There exists a homomorphism $\sigma\colon G \to H$ such that $\nu\circ\sigma = \mathrm{id}_G$.*

(ii) *$\varepsilon(K)$ has a complement in H.*

Proof (i) $\Rightarrow$ (ii): Let $\sigma\colon G \to H$ be a homomorphism satisfying $\nu\circ\sigma = \mathrm{id}_G$. We show that $\sigma(G)$ is a complement of $\varepsilon(K) = \ker(\nu)$ in H. Let $h \in \ker(\nu)\cap\sigma(G)$. Then $h = \sigma(x)$ for some $x \in G$ and we obtain $x = \nu\sigma(x) = \nu(h) = 1$ and $h = \sigma(x) = 1$. Now let $h \in H$ be arbitrary. Then $h = h\sigma(\nu(h))^{-1}\sigma(\nu(h))$ with $h\sigma(\nu(h))^{-1} \in \ker(\nu)$ and $\sigma(\nu(h)) \in \sigma(G)$.

(ii) $\Rightarrow$ (i): Let C be a complement of $\varepsilon(K) = \ker(\nu)$ in H. Then the map $\gamma\colon C \to H/\varepsilon(K)$, $c \mapsto c\varepsilon(K)$ is an isomorphism. By the homomorphism

theorem, also the map $\bar{\nu}\colon H/\varepsilon(K) \to G$, $h\varepsilon(K) \mapsto \nu(h)$, is an isomorphism. Now the map

$$\sigma\colon G \xrightarrow{\bar{\nu}^{-1}} H/\varepsilon(K) \xrightarrow{\gamma^{-1}} C \xrightarrow{\iota} H$$

satisfies $\nu(\sigma(x)) = (\nu \circ \iota \circ \gamma^{-1} \circ \bar{\nu}^{-1})(x) = x$. In fact, we can write $x = \bar{\nu}(\gamma(c))$ for a unique $c \in C$. Then it suffices to show that $\nu(\iota(c) = \bar{\nu}(\gamma(c))$. But $\bar{\nu}(\gamma(c)) = \bar{\nu}(c\ker(\nu)) = \nu(c) = \nu(\iota(c))$. □

12.9 Remark (a) If the conditions in Proposition 12.8 is satisfied, then we say that the group extension $1 \longrightarrow K \xrightarrow{\varepsilon} H \xrightarrow{\nu} G \longrightarrow 1$ *splits* and that σ is a *splitting map*.

(b) If $1 \longrightarrow K \xrightarrow{\varepsilon} H \xrightarrow{\nu} G \longrightarrow 1$ splits and $\sigma\colon G \to H$ satisfies $\nu \circ \sigma = \mathrm{id}_G$, then we may use the elements $h_x := \sigma(x)$, $x \in G$, in order to construct a corresponding parameter system. Since $h_x h_y = h_{xy}$ for all $x, y \in G$, one has $\kappa(x, y) = 1$ for all $x, y \in G$. Moreover, this implies that $\alpha\colon G \to \mathrm{Aut}(K)$ is a homomorphism.

Conversely, if $\alpha\colon G \to \mathrm{Aut}(K)$ is a homomorphism and $\kappa(x, y) = 1$ for all $x, y \in G$, then (α, κ) is a parameter system of G in K and the corresponding group extension is given by the semidirect product of G with K under the action defined by α.

13 Group Extensions with Abelian Kernel and Group Cohomology

Throughout this section we fix two groups A and G and we assume that A is abelian.

13.1 Definition Let $\alpha\colon G \to \mathrm{Aut}(K)$, $x \mapsto \alpha_x$ be a homomorphism. We write the corresponding left action exponentially: $\alpha_x(a) = {}^x a$ for $x \in G$ and $a \in A$. For $n \in \mathbb{N}_0$, we denote by $F(G^n, A)$ the abelian group of functions $f\colon G^n \to A$ under the multiplication $(fg)(x_1, \ldots, x_n) = f(x_1, \ldots, x_n)g(x_1, \ldots, x_n)$, for $f, g \in F(G^n, A)$ and $x_1, \ldots, x_n \in G$. If $n = 0$ we set $G^n := \{1\}$. For each $n \in \mathbb{N}_0$ there is a group homomorphism

$$\partial^n := \partial^n_\alpha\colon F(G^n, A) \longrightarrow F(G^{n+1}, A)$$

given by

$$\begin{aligned}(\partial^n_\alpha(f))((x_0, \ldots, x_n) := {}^{x_0}f(x_1, \ldots, x_{n+1}) \cdot \\ \cdot \Big(\prod_{i=1}^{n-1} f(x_0, \ldots, x_{i-1}x_i, \ldots, x_n)^{(-1)^i}\Big) \cdot \\ \cdot f(x_0, \ldots, x_{n-1})^{(-1)^n}\,,\end{aligned}$$

for $f \in F(G^n, A)$ and $(x_0, \ldots, x_n) \in G^{n+1}$. For $n = 0$ we interpret this as $(\partial^0(f))(x) := {}^x f(1) \cdot f(1)^{-1}$. It is not difficult to see that $\partial^{n+1} \circ \partial^n = 1$ for $n \in \mathbb{N}_0$. This implies that $\mathrm{im}(\partial^n) \leqslant \ker(\partial^{n+1}) \leqslant F(G^{n+1}, A)$, for all $n \in \mathbb{N}_0$. We write

$$B^n(G, A) := B^n_\alpha(G, A) := \mathrm{im}(\partial^{n-1}_\alpha)$$

and

$$Z^n(G, A) := Z^n_\alpha(G, A) := \ker(\partial^n_\alpha)\,,$$

for $n \in \mathbb{N}_0$, where we set $B^0(G, A) := B^0_\alpha(G, A) := 1$. The elements of $B^n_\alpha(G, A)$ are called *n-coboundaries* and the elements of $Z^n_\alpha(G, A)$ are called *n-cocycles* of G with coefficients in A (under the action α). Finally, we set

$$H^n(G, A) := H^n(G, A) := Z^n_\alpha(G, A)/B^n_\alpha(G, A)\,.$$

The group $H^n_\alpha(G, A)$ is called the *n-th cohomology group* of G with coefficients in A (under the action α) and its elements are called *cohomology classes.* If $f \in Z^n(G, A)$, we denote its cohomology class by $[f] \in H^n(G, A)$.

13.2 Remark Let $\alpha\colon G \to \mathrm{Aut}(A)$ be a homomorphism.

(a) We can identify $F(G^0, A)$ with A under the map $f \mapsto f(1)$. With this identification, we obtain

$$Z^0(G, A) = A^G := \{a \in A \mid {}^x a = a \text{ for all } x \in G\}\,,$$

the subgroup of G-fixed points of A. Since $B^0(G,A) = 1$, we obtain $H^0(G,A) \cong A^G$.

(b) A function $f\colon G \to A$ is in $Z^1(G,A)$, if and only if

$$f(xy) = {}^x f(y) \cdot f(x)$$

for all $x, y \in G$. The 1-cocycles of G with coefficients in A are also called the *crossed homomorphisms* from G to A. If the action of G on A is trivial, then the crossed homomorphisms are exactly the homomorphisms. A function $f\colon G \to A$ is a 1-boundary, if and only if there exists an element $a \in A$ such that

$$f(x) = {}^x a \cdot a^{-1},$$

for all $x \in G$. These functions are called the *principal* crossed homomorphisms. If G acts trivially on A, then they are all trivial and $H^0(G,A) \cong \mathrm{Hom}(G,A)$.

(c) A function $f\colon G^2 \to A$ is a 2-cocycle, if and only if

$${}^x f(y,z) f(x,yz) = f(xy,z) f(x,y),$$

for all $x, y, z \in G$, and it is a 2-coboundary, if and only if there exists a function $g\colon G \to A$ such that

$$f(x,y) = {}^x g(y) g(x) g(xy)^{-1},$$

for all $x, y \in G$.

(d) A function $f\colon G^3 \to A$ is a 3-cocycle, if and only if

$${}^w f(x,y,z) f(w,xy,z) f(w,x,y) = f(wx,y,z) f(w,x,yz)$$

for all $w, x, y, z \in G$. Moreover, f is a 3-coboundary, if and only if there exists a function $g\colon G^2 \to A$ such that

$$f(x,y,z) = {}^x g(y,z) g(xy,z)^{-1} g(x,yz) g(x,y)^{-1}$$

for all $x, y, z \in G$.

(e) If A is of finite exponent, i.e., if there exists $e \in \mathbb{N}$ such that $a^e = 1$ for all $a \in A$, then obviously, $f^e = 1$ for all $f \in F(G^n, A)$ and all $n \in \mathbb{N}_0$. In particular, each coboundary and each cohomology class has an order which divides e.

13.3 Example Let $1 \longrightarrow A \xrightarrow{\varepsilon} H \xrightarrow{\nu} G \longrightarrow 1$ be a group extension, let $h_x \in H$ with $\nu(h_x) = x$ for all $x \in G$, and let $(\alpha, \kappa) \in \mathrm{par}(G,A)$ be the parameter system as defined in Proposition 12.3. Then

$$\varepsilon(\alpha_x(a)) = h_x \varepsilon(a) h_x^{-1}, \quad h_x h_y = \varepsilon(\kappa(x,y)) h_{xy},$$
$$\alpha_x \circ \alpha_x = c_{\kappa(x,y)} \circ \alpha_{xy}, \quad \text{and} \quad \alpha_x(\kappa(y,z))\kappa(x,yz) = \kappa(xy,z)\kappa(x,y),$$

for all $a \in A$ and $x, y, z \in G$. Since A is abelian, the map $\alpha\colon G \to \mathrm{Aut}(A)$ is a homomorphism. Moreover, κ is a 2-cocycle of G with coefficients in A under the

action defined by α. If $(\alpha', \kappa') \in \mathrm{par}(G, A)$ is equivalent to (α, κ), then there exists a function $f\colon G \to A$ such that

$$\alpha'_x = c_{\alpha_x(f(x))} \circ \alpha_x \quad \text{and} \quad \kappa'(x,y) = f(x)\alpha_x(f(y))\kappa(x,y)f(xy)^{-1}\,,$$

for all $x, y \in G$. Again, since A is abelian, this implies $\alpha' = \alpha$. Moreover, we can see that κ and κ' belong to the same cohomology class. Altogether we see that two parameter systems (α, κ) and (α', κ') are equivalent, if and only if $\alpha = \alpha'$ and $[\kappa] = [\kappa'] \in H^2_\alpha(G, A)$. Therefore, we obtain bijections

$$\mathrm{Ext}(G, A) \cong \mathrm{Par}(G, A) \cong \dot{\bigcup_{\alpha \in \mathrm{Hom}(G, \mathrm{Aut}(A))}} H^2_\alpha(G, A)\,.$$

Note that, for every $\alpha \in \mathrm{Hom}(G, \mathrm{Aut}(A))$, the set $\mathrm{Ext}_\alpha(G, A)$ of equivalence classes of extensions of G by A, which have α as their automorphism system, are in bijection to $H^2_\alpha(G, A)$ and therefore also form an abelian group. With this notation we have

$$\mathrm{Ext}(G, A) = \dot{\bigcup_{\alpha \in \mathrm{Hom}(G, \mathrm{Aut}(A))}} \mathrm{Ext}_\alpha(G, A)\,.$$

For every $\alpha \in \mathrm{Hom}(G, \mathrm{Aut}(A))$, the identity element in $\mathrm{Ext}_\alpha(G, A)$ is given by the semidirect product of G by A under the action α.

13.4 Proposition *Let $\alpha\colon G \to \mathrm{Aut}(A)$ be a homomorphism and assume that G is finite. Then $[f]^{|G|} = 1$ for all n-cocycles $f \in Z^n_\alpha(G, A)$ and all $n \in \mathbb{N}$.*

Proof Let $n \in \mathbb{N}$, let $f \in Z^n_\alpha(G, A)$, and let $x_0, \ldots, x_n \in G$. Then

$$\begin{aligned} &f(x_0, \ldots, x_{n-1})^{(-1)^{n-1}} \\ &= {}^{x_0}f(x_1, \ldots, x_n) \cdot \Big(\prod_{i=1}^{n-1} f(x_0, \ldots, x_{i-1}x_i, \ldots, x_n)^{(-1)^i}\Big)\,. \end{aligned}$$

If we fix $x_0, \ldots, x_{n-1} \in G$ and multiply the above equations for the different elements $x_n \in G$, we obtain

$$\begin{aligned} &f(x_0, \ldots, x_{n-1})^{(-1)^{n-1}|G|} \\ &= {}^{x_0}\Big(\prod_{x_n \in G} f(x_1, \ldots, x_n)\Big) \cdot \prod_{i=1}^{n-1} \Big(\prod_{x_n \in G} f(x_0, \ldots, x_{i-1}x_i, \ldots, x_n)\Big)^{(-1)^i}\,. \end{aligned}$$

If we define $g\colon G^{n-1} \to A$ by $g(x_1, \ldots, x_{n-1}) := \prod_{x \in G} f(x_1, \ldots, x_{n-1}, x)$, then the above equation shows that

$$f^{|G|} = \partial^{n-1}(g^{(-1)^{n-1}})\,,$$

and $[f]^{|G|} = 1$ in $H^n(G, A)$. □

13.5 Corollary *Let G and A be finite groups of coprime orders. Then $H^n_\alpha(G,A) = 1$ for all $\alpha \in \mathrm{Hom}(G, \mathrm{Aut}(A))$ and all $n \in \mathbb{N}$.*

Proof Let $k := |G|$ and $l := |A|$. Then there exist elements $r, s \in \mathbb{Z}$ such that $1 = rk + sl$. From Remark 13.2(e) and Proposition 13.4 we know that $[f]^k = 1$ and $[f]^l = 1$ for all $f \in Z^n_\alpha(G,A)$ and all $n \in \mathbb{N}$. Therefore also $[f] = [f]^1 = [f]^{rk+sl} = ([f]^k)^r([f]^l)^s = 1$. □

13.6 Remark The above corollary together with Proposition 12.8 and Remark 12.9 implies that every group extension of G by A splits, if G and A have coprime orders. In particular, every group extension of G by A is a semidirect product. This is exactly the first statement of Schur-Zassenhaus on the existence of a complement of a normal Hall subgroup A in the special case, that A is abelian. It is enlightening to read the proof of this theorem in that special case again.

14 Group Extensions with Non-Abelian Kernel

Throughout this section we fix groups G and K.

14.1 Remark An automorphism $f \in \mathrm{Aut}(K)$ is called an *inner* automorphism, if $f = c_a$ for some $a \in K$. The set $\mathrm{Inn}(K)$ of inner automorphisms is the image of the homomorphism $c\colon K \to \mathrm{Aut}(K)$, $a \mapsto c_a$. Therefore, $\mathrm{Inn}(K)$ is a subgroup of $\mathrm{Aut}(K)$. It is even a normal subgroup, since $f \circ c_a \circ f^{-1} = c_{f(a)}$ for all $f \in \mathrm{Aut}(K)$ and all $a \in K$. We call the quotient $\mathrm{Out}(K) := \mathrm{Aut}(K)/\mathrm{Inn}(K)$ the group of *outer* automorphisms of K.

For each $(\alpha, \kappa) \in \mathrm{par}(G, K)$ one has $\alpha_x \circ \alpha_y = c_{\kappa(x,y)} \circ \alpha_{xy}$ for all $x, y \in G$. This shows that the function $\omega\colon G \to \mathrm{Out}(K)$, $x \mapsto \alpha_x \mathrm{Inn}(K)$, is a group homomorphism. We call ω the *pairing* induced by the automorphism system α. If (α', κ') is an equivalent parameter system, then $\alpha'_x = c_{f(x)} \circ \alpha_x$ for some function $f\colon G \to K$, which shows that the pairing ω' induced by α' is equal to ω. Therefore, each element in $\mathrm{Par}(G, K)$ defines a pairing $\omega\colon G \to \mathrm{Out}(K)$. By Schreier's Theorem also every element in $\mathrm{Ext}(G, K)$ defines a pairing. If K is abelian, then $\mathrm{Inn}(K) = 1$ and $\mathrm{Out}(K) = \mathrm{Aut}(K)/\mathrm{Inn}(K) \cong \mathrm{Aut}(K)$, and we do not have to distinguish between automorphism systems and pairings.

For each $\omega \in \mathrm{Hom}(G, \mathrm{Out}(K))$ we denote by $\mathrm{ext}_\omega(G, K)$ (resp. $\mathrm{par}_\omega(G, K)$) the set of extensions of G by K (resp. parameter systems of G in K) which induce the pairing ω, and by $\mathrm{Ext}_\omega(G, K)$ (resp. $\mathrm{Par}_\omega(G, K)$) the set of equivalence classes of extensions of G by K (resp. parameter systems of G in K) which induce the pairing ω. Then we have

$$\mathrm{Ext}(G, K) = \dot{\bigcup_{\omega \in \mathrm{Hom}(G, \mathrm{Out}(K))}} \mathrm{Ext}_\omega(G, K)$$

and

$$\mathrm{Par}(G, K) = \dot{\bigcup_{\omega \in \mathrm{Hom}(G, \mathrm{Out}(K))}} \mathrm{Par}_\omega(G, K)\,,$$

and Schreier's Theorem gives an isomorphism between $\mathrm{Ext}_\omega(G, K)$ and $\mathrm{Par}_\omega(G, K)$ for each $\omega \in \mathrm{Hom}(G, \mathrm{Out}(K))$. It may happen that $\mathrm{Ext}_\omega(G, K)$ is empty. In the sequel we will find out, exactly when this happens, and we will also give a description of $\mathrm{Ext}_\omega(G, K)$ in the case, where it is non-empty. Both results will use group cohomology of G with coefficients in $Z(K)$.

For each automorphism $f \in \mathrm{Aut}(K)$, the restriction $f|_{Z(K)}$ defines an automorphism of $Z(K)$, since $Z(K)$ is characteristic in K. This defines a group homomorphism $\mathrm{res}^K_{Z(K)}\colon \mathrm{Aut}(K) \to \mathrm{Aut}(Z(K))$ whose kernel contains $\mathrm{Inn}(K)$. By the homomorphism theorem, we obtain a homomorphism $\mathrm{Out}(K) \to \mathrm{Aut}(K)$, $f\mathrm{Inn}(K) \mapsto f|_{Z(K)}$, which we denote again by $\mathrm{res}^K_{Z(K)}$.

If $\omega \in \mathrm{Hom}(G, \mathrm{Out}(K))$, then its composition with $\mathrm{res}^K_{Z(K)}$ gives a homomorphism $\zeta := \mathrm{res}^K_{Z(K)} \circ \omega\colon G \to \mathrm{Aut}(Z(K))$. We will show that $\mathrm{Par}_\omega(G, K)$ is already determined by ζ.

In the sequel we will write $[\alpha,\kappa]$ for the equivalence class of any element $(\alpha,\kappa)\in \mathrm{par}(G,K)$.

14.2 Theorem *Let $\omega\in \mathrm{Hom}(G,\mathrm{Out}(K))$ with $\mathrm{Par}_\omega(G,K)\neq\emptyset$ and let $\zeta := \mathrm{res}^K_{Z(K)}\circ\omega\in \mathrm{Hom}(G,\mathrm{Aut}(Z(K)))$. Then the function*

$$Z^2_\zeta(G,Z(K))\times \mathrm{par}_\omega(G,K)\to \mathrm{par}_\omega(G,K)\,,\quad (\gamma,(\alpha,\kappa))\mapsto(\alpha,\gamma\kappa)\,,$$

with

$$(\gamma\kappa)(x,y) := \gamma(x,y)\kappa(x,y)\,,$$

for $x,y\in G$, defines an action of the group $Z^2_\zeta(G,Z(K))$ on the set $\mathrm{par}_\omega(G,K)$. Moreover, this action induces an action of $H^2_\zeta(G,Z(K))$ on $\mathrm{Par}_\omega(G,K)$ which is transitive and free. In particular, for any element $(\alpha,\kappa)\in\mathrm{par}_\omega(G,K)$, the map

$$H^2_\zeta(G,Z(K))\longrightarrow \mathrm{Par}_\omega(G,K)\,,\quad [\gamma]\longmapsto {}^{[\gamma]}[\alpha,\kappa]=[\alpha,\gamma\kappa]\,,$$

is a bijection.

Proof We first show that for $\gamma\in Z^2_\zeta(G,Z(K))$ and $(\alpha,\kappa)\in\mathrm{par}_\omega(G,K)$ also $(\alpha,\gamma\kappa)\in\mathrm{par}_\omega(G,K)$. In fact, for all $x,y,z\in G$ we have

$$\begin{aligned}(\gamma\kappa)(x,y)\cdot(\gamma\kappa)(xy,z) &= \gamma(x,y)\kappa(x,y)\gamma(xy,z)\kappa(xy,z)\\ &= \gamma(x,y)\gamma(xy,z)\kappa(x,y)\kappa(xy,z)\\ &= \zeta_x(\gamma(y,z))\gamma(x,yz)\alpha_x(\kappa(y,z))\kappa(x,yz)\\ &= \alpha_x(\gamma(y,z)\kappa(y,z))\gamma(x,yz)\kappa(x,yz)\\ &= \alpha_x((\gamma\kappa)(y,z))(\gamma\kappa)(x,yz)\,,\end{aligned}$$

since $\alpha(z)=\zeta(z)$ for each $z\in Z(K)$, and

$$\begin{aligned}c_{(\gamma\kappa)(x,y)}\circ\alpha_{xy} &= c_{\gamma(x,y)\kappa(x,y)}\circ\alpha_{xy}\\ &= c_{\gamma(x,y)}\circ c_{\kappa(x,y)}\circ\alpha_{xy}\\ &= c_{\kappa(x,y)}\circ\alpha_{xy}=\alpha_x\circ\alpha_y\,,\end{aligned}$$

since $\gamma(x,y)\in Z(K)$. Moreover, for all $(\alpha,\kappa)\in\mathrm{par}_\omega(G,K)$ and $\gamma,\delta\in Z^2_\zeta(G,Z(K))$ we have

$${}^{\delta}\big({}^{\gamma}(\alpha,\kappa)\big)={}^{\delta}(\alpha,\gamma\kappa)=(\alpha,\delta\gamma\kappa)={}^{\delta\gamma}(\alpha,\kappa)$$

and ${}^{1}(\alpha,\kappa)=(\alpha,\kappa)$ so that we have established an action of $Z^2_\zeta(G,Z(K))$ on $\mathrm{par}_\omega(G,K)$.

Next, let $(\alpha,\kappa),(\alpha',\kappa')\in\mathrm{par}_\omega(G,K)$ be equivalent and let $\gamma\in Z^2_\zeta(G,Z(K))$. Then there exists a function $f\colon G\to K$ such that

$$\alpha'_x=c_{f(x)}\circ\alpha_x\quad\text{and}\quad \kappa'(x,y)=f(x)\alpha_x(f(y))\kappa(x,y)f(xy)^{-1}\,,$$

for all $x, y \in G$. Multiplication of the last equation with $\gamma(x,y)$ yields

$$\gamma(x,y)\kappa'(x,y) = f(x)\alpha_x(f(y))\gamma(x,y)\kappa(x,y)f(xy)^{-1}\,,$$

which shows that also ${}^{\gamma}(\alpha,\kappa) = (\alpha,\gamma\kappa)$ and ${}^{\gamma}(\alpha',\kappa') = (\alpha',\gamma\kappa')$ are equivalent. Therefore, we obtain an action of $Z^2_\zeta(G,Z(K))$ on $\mathrm{Par}_\omega(G,K)$.

Now let $(\alpha,\kappa) \in \mathrm{par}_\omega(G,K)$ and let $\gamma \in B^2_\zeta(G,Z(K))$. We will show that ${}^{\gamma}(\alpha,\kappa)$ is equivalent to (α,κ). In fact, there exists a function $f\colon G \to Z(K)$ such that $\gamma(x,y) = \zeta_x(f(y))f(xy)^{-1}f(x) = \alpha_x(f(y))f(xy)^{-1}f(x)$ for all $x,y \in G$. With this function we have

$$\alpha_x = c_{f(x)} \circ \alpha_x$$

and

$$(\gamma\kappa)(x,y) = \gamma(x,y)\kappa(x,y) = f(x)\alpha_x(f(y))\kappa(x,y)f(xy)^{-1}\,,$$

for all $x,y \in G$ and the claim is proven. Therefore, we have an action of $H^2_\zeta(G,Z(K))$ on $\mathrm{Par}_\omega(G,K)$.

Now we show that this action is free. Let $\gamma_1,\gamma_2 \in Z^2_\zeta(G,Z(K))$ and $(\alpha,\kappa) \in \mathrm{par}_\omega(G,K)$ such that ${}^{\gamma_1}(\alpha,\kappa)$ and ${}^{\gamma_2}(\alpha,\kappa)$ are equivalent. Set $\gamma := \gamma_1^{-1}\gamma_2$. Then ${}^{\gamma}(\alpha,\kappa) = (\alpha,\kappa)$ is equivalent to (α,κ). Therefore, there exists a function $f\colon G \to K$ such that $\alpha_x = c_{f(x)} \circ \alpha_x$ and $\gamma(x,y)\kappa(x,y) = f(x)\alpha_x(f(y))\kappa(x,y)f(xy)^{-1}$ for all $x,y \in G$. This implies that $c_{f(x)} = \mathrm{id}_K$ for all $x \in K$ so that $f(x) \in Z(K)$ for all $x \in K$. Using this we also obtain $\gamma(x,y) = f(x)\alpha_x(f(y))f(xy)^{-1} = f(x)\zeta_x(f(y))f(xy)^{-1}$. Therefore, $\gamma \in B^2_\zeta(G,Z(K))$ and $[\gamma_1] = [\gamma_2] \in H^2_\zeta(G,Z(K))$.

Finally, we show that the action of $H^2_\zeta(G,Z(K))$ on $\mathrm{Par}_\omega(G,K)$ is transitive. Let $(\alpha,\kappa),(\beta,\lambda) \in \mathrm{par}_\omega(G,K)$. We will show that there exists $\gamma \in Z^2_\zeta(G,Z(K))$ such that (α,κ) and ${}^{\gamma}(\beta,\lambda)$ are equivalent. For each $x \in G$ we have $\alpha_x\mathrm{Inn}(K) = \omega(x) = \beta_x\mathrm{Inn}(K)$. Thus, there exists an element $f(x) \in K$ such that $c_{f(x)} \circ \alpha_x = \beta_x$. We set $\kappa'(x,y) := f(x)\alpha_x(f(y))\kappa(x,y)f(xy)^{-1}$ for all $x,y \in G$. Then $(\beta,\kappa') \in \mathrm{par}_\omega(G,K)$ and (α,κ) is equivalent to (β,κ'). Since also $(\beta,\lambda) \in \mathrm{par}_\omega(G,K)$, we obtain $c_{\kappa'(x,y)} \circ \beta_{xy} = \beta_x \circ \beta_y = c_{\lambda(x,y)} \circ \beta_{xy}$ and $c_{\kappa'(x,y)} = c_{\lambda(x,y)}$ for all $x,y \in K$. This implies that $\gamma(x,y) := \kappa'(x,y)\lambda(x,y)^{-1} \in Z(K)$ for all $x,y \in G$. We show that $\gamma \in Z^2_\zeta(G,Z(K))$. In fact, for $x,y,z \in G$ we have

$$\begin{aligned}
\gamma(x,y)\gamma(xy,z) &= \kappa'(x,y)\lambda(x,y)^{-1}\gamma(xy,z)\\
&= \kappa'(x,y)\gamma(xy,z)\lambda(x,y)^{-1}\\
&= \kappa'(x,y)\kappa'(xy,z)\lambda(xy,z)^{-1}\lambda(x,y)^{-1}\\
&= \beta_x(\kappa'(y,z))\kappa'(x,yz)\lambda(x,yz)^{-1}\beta_x(\lambda(y,z))^{-1}\\
&= \beta_x(\kappa'(y,z))\gamma(x,yz)\beta_x(\lambda(y,z))^{-1}\\
&= \beta_x(\kappa'(y,z)\lambda(y,z)^{-1})\gamma(x,yz)\\
&= \zeta_x(\gamma(y,z))\gamma(x,yz)\,.
\end{aligned}$$

This implies that $(\beta, \kappa') = {}^{\gamma}(\beta, \lambda)$ and that (α, κ) is equivalent to $(\beta, \kappa') = {}^{\gamma}(\beta, \lambda)$. This completes the proof of the Theorem. □

14.3 Theorem *Assume that* $Z(K) = 1$. *Then* $|\mathrm{Par}_\omega(G, K)| = 1$ *for every* $\omega\colon G \to \mathrm{Out}(K)$.

Proof For each $x \in G$ we choose $\alpha_x \in \mathrm{Aut}(K)$ such that $\omega(x) = \alpha_x \mathrm{Inn}(K)$. For all $x, y \in G$ we have $\alpha_x \alpha_y \mathrm{Inn}(K) = \omega(x)\omega(y) = \omega(xy) = \alpha_{xy}\mathrm{Inn}(K)$. Therefore, there exist elements $\kappa(x, y) \in K$, such that $\alpha_x \circ \alpha_y = c_{\kappa(x,y)} \circ \alpha_{xy}$ for all $x, y \in G$. For all $x, y, z \in G$ we obtain

$$\begin{aligned} c_{\kappa(x,y)\kappa(xy,z)} \circ \alpha_{xyz} &= c_{\kappa(x,y)} \circ c_{\kappa(xy,z)} \circ \alpha_{xyz} \\ &= c_{\kappa(x,y)} \circ \alpha_{xy} \circ \alpha_z \\ &= \alpha_x \circ \alpha_y \circ \alpha_z \\ &= \alpha_x \circ c_{\kappa(y,z)} \circ \alpha_{yz} \\ &= \alpha_x \circ c_{\kappa(y,z)} \circ \alpha_x^{-1} \circ \alpha_x \circ \alpha_{yz} \\ &= c_{\alpha_x(\kappa(y,z))} \circ c_{\kappa(x,yz)} \circ \alpha_{x(yz)} \\ &= c_{\alpha_x(\kappa(y,z))\kappa(x,yz)} \circ \alpha_{xyz}\,, \end{aligned}$$

and therefore, $c_{\kappa(x,y)\kappa(xy,z)} = c_{\alpha_x(\kappa(y,z))\kappa(x,yz)}$. Since $Z(K) = 1$, this implies $\kappa(x, y)\kappa(xy, z) = \alpha_x(\kappa(y, z))\kappa(x, yz)$ for all $x, y, z \in G$. Therefore, $(\alpha, \kappa) \in \mathrm{par}_\omega(G, K)$, and $\mathrm{Par}_\omega(G, K)$ is not empty. On the other hand, by Theorem 14.2, $\mathrm{Par}_\omega(G, K)$ is in bijection to $H^2_\zeta(G, Z(K))$, where $\zeta := \mathrm{res}^K_{Z(K)} \circ \omega$. Again since $Z(K) = 1$, we have $F(G^2, Z(K)) = 1$ and also $H^2_\zeta(G, Z(K)) = 1$. □

14.4 Theorem *Let* $\omega\colon G \to \mathrm{Out}(K)$ *be a group homomorphism and let* $\zeta := \mathrm{res}^K_{Z(K)} \circ \omega \in \mathrm{Hom}(G, \mathrm{Aut}(Z(K)))$. *Moreover, for each* $x \in G$, *let* $\alpha_x \in \mathrm{Aut}(K)$ *be an automorphism with* $\omega(x) = \alpha_x \mathrm{Inn}(K)$. *Then the following assertions hold:*

(a) *For all* $x, y \in G$ *there exists an element* $\chi(x, y) \in K$ *such that* $\alpha_x \circ \alpha_y = c_{\chi(x,y)} \circ \alpha_{xy}$.

(b) *Let* $\chi(x, y) \in K$ *be chosen as in (a). Then, for all* $x, y, z \in G$ *the element* $\vartheta(x, y, z) := \alpha_x(\chi(y, z))\chi(x, yz)\chi(xy, z)^{-1}\chi(x, y)^{-1}$ *lies in* $Z(K)$, *and the function* $\vartheta\colon G^3 \to Z(K)$ *is an element of* $Z^3_\zeta(G, Z(K))$.

(c) *The cohomology class* $[\vartheta] \in H^3_\zeta(G, Z(K))$ *of the element* $\vartheta \in Z^3_\zeta(G, Z(K))$ *defined in (b) does not depend on the choices of* $\alpha_x \in \mathrm{Aut}(K)$ *and* $\chi(x, y) \in K$ *for* $x, y \in G$.

Proof (a) For all $x, y \in G$ we have

$$\alpha_x \alpha_y \mathrm{Inn}(K) = \omega(x)\omega(y) = \omega(xy) = \alpha_{xy}\mathrm{Inn}(K)\,,$$

which implies that $\alpha_x \alpha_y \alpha_{xy}^{-1} \in \mathrm{Inn}(K)$.

(b) For all $x, y, z \in G$ we have

$$\begin{aligned}
&c_{\vartheta(x,y,z)} \\
&= c_{\alpha_x(\chi(y,z))} \circ c_{\chi(x,yz)} \circ c^{-1}_{\chi(xy,z)} \circ c^{-1}_{\chi(x,y)} \\
&= \alpha_x \circ c_{\chi(y,z)} \circ \alpha_x^{-1} \circ \alpha_x \circ \alpha_{yz} \circ \alpha^{-1}_{xyz} \circ \alpha_{xyz} \circ \alpha_z^{-1} \circ \alpha^{-1}_{xy} \circ \alpha_{xy} \circ \alpha_y^{-1} \circ \alpha_x^{-1} \\
&= \alpha_x \circ \alpha_y \circ \alpha_z \circ \alpha^{-1}_{yz} \circ \alpha_{yz} \circ \alpha_z^{-1} \circ \alpha_y^{-1} \circ \alpha_x^{-1} \\
&= \mathrm{id}_K \,,
\end{aligned}$$

which implies that $\vartheta(x, y, z) \in Z(K)$.

Next we show that $\vartheta \in Z^3_\zeta(G, Z(K))$. Let $x, y, z, w \in G$. Then

$$\begin{aligned}
&\zeta_x(\vartheta(y,z,w))\vartheta(x,yz,w)\vartheta(x,y,z) \\
&= \alpha_x(\alpha_y(\chi(z,w)))\alpha_x(\chi(y,zw))\alpha_x(\chi(yz,w))^{-1}\alpha_x(\chi(y,z))^{-1}\vartheta(x,yz,w)\cdot \\
&\qquad \cdot \vartheta(x,y,z) \\
&= \alpha_x(\alpha_y(\chi(z,w)))\alpha_x(\chi(y,zw))\alpha_x(\chi(yz,w))^{-1}\vartheta(x,yz,w)\alpha_x(\chi(y,z))^{-1}\cdot \\
&\qquad \cdot \vartheta(x,y,z) \\
&= \alpha_x(\alpha_y(\chi(z,w)))\alpha_x(\chi(y,zw))\alpha_x(\chi(yz,w))^{-1}\cdot \\
&\qquad \cdot \alpha_x(\chi(yz,w))\chi(x,yzw)\chi(xyz,w)^{-1}\chi(x,yz)^{-1}\alpha_x(\chi(y,z))^{-1}\cdot \\
&\qquad \cdot \alpha_x(\chi(y,z))\chi(x,yz)\chi(xy,z)^{-1}\chi(x,y)^{-1} \\
&= \alpha_x(\alpha_y(\chi(z,w)))\alpha_x(\chi(y,zw))\chi(x,yzw)\chi(xyz,w)^{-1}\chi(xy,z)^{-1}\chi(x,y)^{-1} \\
&= \alpha_x(\alpha_y(\chi(y,w)))\alpha_x(\chi(y,zw))\chi(x,yzw)\chi(xy,zw)^{-1}\chi(x,y)^{-1}\cdot \\
&\qquad \cdot \chi(x,y)\chi(xy,zw)\chi(xyz,w)^{-1}\chi(xy,z)^{-1}\chi(x,y)^{-1} \\
&= \alpha_x(\alpha_y(\chi(z,w)))\vartheta(x,y,zw)\chi(x,y)\chi(xy,zw)\chi(xyz,w)^{-1}\chi(xy,z)^{-1}\chi(x,y)^{-1} \\
&= \chi(x,y)\alpha_{xy}(\chi(z,w))\chi(xy,zw)\chi(xyz,w)^{-1}\cdot \\
&\qquad \cdot \chi(xy,z)^{-1}\chi(x,y)^{-1}\vartheta(x,y,zw) \\
&= \chi(x,y)\vartheta(xy,z,w)\chi(x,y)^{-1}\vartheta(x,y,zw) \\
&= \vartheta(xy,z,w)\vartheta(x,y,zw)\,.
\end{aligned}$$

(c) If, for each $x \in G$, also $\alpha'_x \in \mathrm{Aut}(K)$ is chosen such that $\alpha'_x \mathrm{Inn}(K) = \omega(x)$, and if, for each $x, y \in G$, an element $\chi'(x, y) \in K$ is chosen such that $\alpha'_x \circ \alpha'_y = c_{\chi'(x,y)} \circ \alpha'_{xy}$, then there exists a function $f\colon G \to K$ such that $\alpha'_x = c_{f(x)} \circ \alpha_x$. This implies

$$\begin{aligned}
\alpha'_x \circ \alpha'_y &= c_{f(x)} \circ \alpha_x \circ c_{f(y)} \circ \alpha_y \\
&= c_{f(x)} \circ \alpha_x \circ c_{f(y)} \circ \alpha_x^{-1} \circ \alpha_x \circ \alpha_y \\
&= c_{f(x)} \circ c_{\alpha_x(f(y))} \circ c_{\chi(x,y)} \circ \alpha_{xy} \\
&= c_{f(x)\alpha_x(f(y))\chi(x,y)} \circ c^{-1}_{f(xy)} \circ \alpha'_{xy} \\
&= c_{f(x)\alpha_x(f(y))\chi(x,y)f(xy)^{-1}} \circ \alpha'_{xy}\,,
\end{aligned}$$

and we obtain

$$\chi'(x,y) = f(x)\alpha_x(f(y))\chi(x,y)f(xy)^{-1}g(x,y)$$

for all $x, y \in G$ with a function $g\colon G \times G \to Z(K)$. For all $x, y, z \in G$, the corresponding function

$$\vartheta'(x,y,z) := \alpha'_x(\chi'(y,z))\chi'(x,yz)\chi'(xy,z)^{-1}\chi'(x,y)^{-1}$$

then satisfies

$$\begin{aligned}
&\vartheta'(x,y,z)\\
&= f(x)\alpha_x\big(f(y)\alpha_y(f(z))\chi(y,z)f(yz)^{-1}g(y,z)\big)f(x)^{-1}\cdot\\
&\qquad\cdot f(x)\alpha_x(f(yz))\chi(x,yz)f(xyz)^{-1}g(x,yz)\cdot\\
&\qquad\cdot g(xy,z)^{-1}f(xyz)\chi(xy,z)^{-1}\alpha_{xy}(f(z))^{-1}f(xy)^{-1}\cdot\\
&\qquad\cdot g(x,y)^{-1}f(xy)\chi(x,y)^{-1}\alpha_x(f(y))^{-1}f(x)^{-1}\\
&= f(x)\alpha_x(f(y))\alpha_x(\alpha_y(f(z)))\alpha_x(\chi(y,z))\cdot\\
&\qquad\cdot\chi(x,yz)\chi(xy,z)^{-1}\alpha_{xy}(f(z)^{-1})\chi(x,y)^{-1}\alpha_x(f(y)^{-1})f(x)^{-1}\cdot\\
&\qquad\cdot\alpha_x(g(y,z))g(x,yz)g(xy,z)^{-1}g(x,y)^{-1}\\
&= f(x)\alpha_x(f(y))\alpha_x(\alpha_y(f(z)))\vartheta(x,y,z)\chi(x,y)\alpha_{xy}(f(z)^{-1})\cdot\\
&\qquad\cdot\chi(x,y)^{-1}\alpha_x(f(y)^{-1})f(x)^{-1}(\partial^2_\zeta(g))(x,y,z)\\
&= f(x)\alpha_x(f(y))\alpha_x(\alpha_y(f(z)))\alpha_x(\alpha_y(f(z)^{-1}))\cdot\\
&\qquad\cdot\alpha_x(f(y)^{-1})f(x)^{-1}\vartheta(x,y,z)(\partial^2_\zeta(g))(x,y,z)\\
&= \vartheta(x,y,z)(\partial^2_\zeta(g))(x,y,z)\,,
\end{aligned}$$

which shows that the cohomology classes $[\vartheta]$ and $[\vartheta']$ coincide. □

14.5 Definition Let $\omega\colon G \to \mathrm{Out}(K)$ be a homomorphism and let $\zeta := \mathrm{res}^K_{Z(K)} \circ \omega \in \mathrm{Hom}(G, \mathrm{Aut}(Z(K)))$. The element $[\vartheta] \in H^3_\zeta(G, Z(K))$ defined in Theorem 14.4 is called the *obstruction* of ω.

14.6 Theorem *Let $\omega\colon G \to \mathrm{Out}(K)$ be a group homomorphism and let $\zeta := \mathrm{res}^K_{Z(K)} \in \mathrm{Hom}(G, \mathrm{Aut}(Z(K)))$. Then $\mathrm{Par}_\omega(G,K) \neq \emptyset$ if and only if the obstruction $[\vartheta] \in H^3_\zeta(G, Z(K))$ of ω is trivial.*

Proof First assume that $\mathrm{Par}_\omega(G,K) \neq \emptyset$ and let $(\alpha, \kappa) \in \mathrm{par}_\omega(G,K)$. Then we have $\omega(x) = \alpha_x\mathrm{Inn}(K)$, $\alpha_x \circ \alpha_y = c_{\kappa(x,y)} \circ \alpha_{xy}$, and $\alpha_x(\kappa(y,z))\kappa(x,yz)\kappa(xy,z)^{-1}\kappa(x,y)^{-1} = 1$, for all $x, y, z \in G$. This implies that we may define the obstruction $[\vartheta]$ of ω using the elements $\alpha_x \in \mathrm{Aut}(K)$ and $\kappa(x,y) \in K$ for $x, y \in G$, and that $[\vartheta] = 1$.

Conversely, if we choose elements $\alpha_x \in \mathrm{Aut}(K)$ such that $\omega(x) = \alpha_x\mathrm{Inn}(K)$ for all $x \in G$, and elements $\chi(x,y) \in K$ such that $\alpha_x \circ \alpha_y = c_{\chi(x,y)} \circ \alpha_{xy}$

for all $x, y \in G$, then we obtain the obstruction $[\vartheta] \in H^3_\zeta(G, Z(K))$ of ω from the 3-cocycle $\vartheta(x,y,z) := \alpha_x(\chi(y,z))\chi(x,yz)\chi(xy,z)^{-1}\chi(x,y)^{-1} \in Z(K)$, for $x, y, z \in G$. Since $[\vartheta] = 1$, there exists an element $\varphi\colon G \times G \to Z(K)$ such that $\vartheta = \partial^2_\zeta(\varphi)$. We set $\kappa(x,y) := \varphi(x,y)^{-1}\chi(x,y)$ for $x, y \in G$ and show that $(\alpha, \kappa) \in \mathrm{par}_\omega(G, K)$. In fact, for all x, y, z in G we have

$$\alpha_x \circ \alpha_y = c_{\kappa(x,y)} \circ \alpha_{xy}$$

and

$$\begin{aligned}
\kappa(x,y)\kappa(xy,z) &= \varphi(x,y)^{-1}\chi(x,y)\varphi(xy,z)^{-1}\chi(xy,z) \\
&= \varphi(x,y)^{-1}\varphi(xy,z)^{-1}\chi(x,y)\chi(xy,z) \\
&= \varphi(x,yz)^{-1}\alpha_x(\varphi(y,z))^{-1}(\partial^2_\zeta(\varphi))(x,y,z)\chi(x,y)\chi(xy,z) \\
&= \varphi(x,yz)^{-1}\alpha_x(\varphi(y,z))^{-1}\vartheta(x,y,z)\chi(x,y)\chi(xy,z) \\
&= \varphi(x,yz)^{-1}\alpha_x(\varphi(y,z))^{-1}\alpha_x(\chi(y,z))\chi(x,yz) \\
&= \alpha_x(\kappa(y,z))\kappa(x,yz)\,,
\end{aligned}$$

which completes the proof. □

15 Exercises

1. Let $n \in \mathbb{N}$. Show that two elements of $\sigma, \tau \in \mathrm{Sym}(n)$ are conjugate (i.e., there exists $\rho \in \mathrm{Sym}(n)$ with $\tau = \rho\sigma\rho^{-1}$) if and only if they have the same cycle type.

2. Let $\sigma = \pi_1 \cdots \pi_r \in \mathrm{Sym}(n)$ with pairwise disjoint cycles $\pi_1, \ldots, \pi_r$ of lengths $k_1, \ldots, k_r$. What is the order of σ?

3. What are the orders of the subgroups of Alt(5)? (You may use GAP)

4. Let $2 \leqslant n \in \mathbb{N}$, let $i \in \{1, \ldots, n\}$, and set $H_i := \{\sigma \in \mathrm{Sym}(n) | \sigma(i) = i\}$.
(a) Show that H_i is a subgroup of $\mathrm{Sym}(n)$ which is isomorphic to $\mathrm{Sym}(n-1)$.
(b) Show that for each $i, j \in \{1, \ldots, n\}$, the subgroups H_i and H_j of $\mathrm{Sym}(n)$ are conjugate.
(c) Show that $H(i)$ is a maximal subgroup of $\mathrm{Sym}(n)$.

5. Let G be a group and let M_1 and M_2 be G-sets. Moreover, let $\rho_1 \colon G \to \mathrm{Sym}(M_1)$ and $\rho_2 \colon G \to \mathrm{Sym}(M_2)$ denote the corresponding group homomorphisms. Show that M_1 and M_2 are isomorphic G-sets if and only if there exists a bijection $f \colon M_1 \to M_2$ such that $\rho_2(g) = f \circ \rho_1(g) \circ f^{-1}$ for all $g \in G$.

6. Write down the other generators of Rubik's group Ru, calculate its order with GAP, and factorize its order into primes.

7. Let $C \subset \mathbb{R}^3$ be a cube with the origin at its center.
(a) Show that the group of rotations $\{g \in \mathrm{SO}(3) \mid g(C) = C\}$ leaving the cube invariant is isomorphic to Sym(4). (Hint: Consider the 4 diagonals of the cube.)
(b) Show that the group of all symmetries $\{g \in \mathrm{O}(3) \mid g(C) = C\}$ is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathrm{Sym}(4)$.

8. Let U, V be subgroups of a finite group G. Show that

$$|UV| = \frac{|U| \cdot |V|}{|U \cap V|}.$$

(Here, $UV := \{uv \mid u \in U, v \in V\}$, which is in general not a subgroup of G.)

9. In the tableau

2	1	3	4
5	6	7	8
9	10	11	12
13	14	15	

one is allowed to shift any square bordering the empty square to the empty square. Find out if it is possible to obtain the constellation

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	

from the first one.

10. (a) Give an example of a normal subgroup G in a group Γ which has no complement in Γ.

(b) Show that any two complements of a normal subgroup G in a group Γ are isomorphic.

(c) Give an example of a group Γ and a subgroup S which has two non-isomorphic normal complements in Γ.

11. Let G and S be groups and suppose that S acts on G via group automorphisms. Show that the resulting semidirect product $G \rtimes S$ is abelian if and only if G and S are abelian and the action of S on G is trivial.

12. Write a function in GAP which attaches to a group G a field .normalSubgroups containing a list of all normal subgroups of G in ascending order and which prints a list of the orders of the normal subgroups on the screen.

13. Let K be a field with at least 3 elements, let $n \in \mathbb{N}$, and let $G := \mathrm{GL}_n(K)$. Moreover, let $T \leqslant G$ be the subgroup of diagonal invertible matrices. Show that $N_G(T) = \mathrm{Mon}_n(K)$.

14. Let p be an odd prime. Show that there exist exactly two isomorphism classes of non-abelian groups of order p^3 and describe them as semidirect products. Hint: Distinguish between the cases that there exists an element of order p^2 or not.

15. (a) Let p be a prime and let $G := \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$. Show that G has exactly $p+1$ subgroups of order p.

(b) A group of 25 mathematicians meets for a 6 day conference. Between the morning and afternoon lectures they have lunch together in a room with 5 tables and 5 chairs at each table. The organizer would like to assign every day new places at the tables in such a way that each participant has eaten with any other one at least once at the same table. Is this possible?

16. Show that every simple group G of order 60 is isomorphic to $\mathrm{Alt}(5)$. Hint: Consider a Sylow 2-subgroup, show that its normalizer H has index 5, and use the translation action of G on G/H.

17. Find a composition series of the Rubik group Ru. What are the composition factors of Ru?

18. Compute the composition factors, the chief factors, and the characteristic factors of Sym(4).

19. Let G be a group and let $N_1, \ldots, N_k \lhd G$ be normal subgroups such that

(i) G/N_i is a simple group for all $i = 1, \ldots, k$.

(ii) $\bigcap_{i=1}^{k} N_i = 1$.

(iii) $U_i := \bigcap_{j \in \{1,\ldots,k\} \smallsetminus \{i\}} N_j \neq 1$ for all $i = 1, \ldots, k$.

Show that the following assertions hold:

(a) For all partitions $I \dot{\cup} J = \{1, \ldots, k\}$ one has

$$\prod_{i \in I} U_i = \bigcap_{j \in J} N_j \,.$$

(b) The map

$$G \longrightarrow G/N_1 \times \cdots \times G/N_k \,, \quad g \mapsto (gN_1, \ldots, gN_k) \,,$$

is an isomorphism. Hint: Use induction on k to prove (a) and use (a) to prove (b).

20. Let S be a group and let G be a finite simple S-group. Show that there exists a simple group H such that $G \cong H \times \cdots \times H$. Hint: Use exercise 19.

21. Let G be a finite group.

(a) Let G and H be nilpotent groups. Show that also $G \times H$ is nilpotent.

(b) Let N_1 and N_2 be normal subgroups of G such that G/N_1 and G/N_2 are nilpotent. Show that also $G/(N_1 \cap N_2)$ is nilpotent.

(c) Show that there exists a normal subgroup N of G with the following property: G/N is nilpotent and for every normal subgroup U of G such that G/U is nilpotent one has $N \leqslant U$.

22. Let G be a group and let $H \leqslant N \leqslant G$. Show that

(a) if N is characteristic in G and H is characteristic in N, then H is characteristic in G,

(b) if N is normal in G and H is characteristic in N, then H is normal in G.

23. Let G be a finite group. For $n \geqslant 3$ and subsets $X_1, \ldots, X_n$, of G one defines inductively $[X_1, \ldots, X_n] := [X_1, [X_2, \ldots, X_n]]$.

(a) Show that for any three subgroups $A, B, C \leqslant G$ satisfying $A \leqslant N_G(B) \cap N_G(C)$ one has $[AB, C] = [A, C][B, C]$.

(b) Show that if A and B are normal subgroups of G with $[A,\dots,A]=1$ and $[B,\dots,B]=1$ (where one takes m copies of A and n copies of B), then $[AB,\dots,AB]=1$ where one takes $m+n-1$ copies of AB.

(c) Show that if A,B are nilpotent normal subgroups of G, then also AB is a nilpotent normal subgroup of G.

(d) Show that G has a normal nilpotent subgroup $F(G)$ which contains every other normal nilpotent subgroup of G. This group $F(G)$ is called the *Fitting subgroup* of G.

24. Let G be a finite group.

(a) Show that there exists a solvable normal subgroup of G which contains every other solvable normal subgroup of G. This subgroup is called the *solvable radical* of G.

(b) Show that there exists a normal subgroup of G with solvable factor group such that every other normal subgroup with solvable factor group contains that group.

(c) Is there in general an abelian normal subgroup of G containing every other abelian normal subgroup of G?

25. Let $2 \leqslant n \in \mathbb{N}$ and set

$$G := \langle N, S \mid N^{2^n} = 1, S^2 = N^{2^{n-1}}, SNS^{-1} = N^{-1} \rangle .$$

(a) Show that G has order 2^{n+1}. (G is called the *generalized quaternion group* of order 2^{n+1}.)

(b) Show that G has only one subgroup of order 2.

(c) Calculate the upper central series of G.

(d) Calculate the lower central series of G.

26. Proof the assertions (i)–(vi) in Example 7.8(c) on the extra-special p-group $E_{p^{2n+1}}$ of exponent p for $n \in \mathbb{N}$.

27. Let π be a set of primes and let G be a group.

(a) Show that for every $g \in G$ there exist unique element $g_\pi, g_{\pi'} \in G$ such that g_π has π-order, $g_{\pi'}$ has π'-order, and $g = g_\pi g_{\pi'}$. Show also that $g_\pi, g_{\pi'} \in \langle g \rangle$.

(b) Show that there exists a biggest normal π-subgroup of G.

(c) Let $\pi = \{p\}$. Show that $O_p(G)$ is the intersection of the Sylow p-subgroups of G.

28. Let H be a non-abelian simple finite group and let $G := H \times \cdots \times H$ with n copies of H. Show that $\mathrm{Aut}(G) \cong \mathrm{Mon}_n(\mathrm{Aut}(H))$.

29. Let G be a finite group and let p be a prime. A p-subgroup P of G is called *p-radical* in G, if $O_p(N_G(P)) = P$.

(a) Show that every Sylow p-subgroup of G is p-radical in G.

(b) Show that $O_p(G)$ is a p-radical subgroup of G and that $O_p(G)$ is contained in every p-radical subgroup of G.

30. Write a function in GAP that calculates for a given finite group G and a given prime p representatives of the conjugacy classes of p-radical subgroups of G. Send the function via Email to boltje@math.ucsc.edu to enter a competition for the fastest function. (GAP has a function "PCore" which comes in useful.)

31. Let G be a finite group and let π be a set of primes.

(a) Show that if G is π-separated, then every subgroup and factor group of G is π-separated.

(b) Show that if G is π-solvable, then every subgroup and factor group of G is π-solvable.

(c) Assume that G is π-solvable and that $1 \leqslant H_0 \trianglelefteq H_1 \leqslant G$ such that H_1/H_0 is a π-group, then H_1/H_0 is solvable.

32. Let G be a finite group. Show the equivalence of the following statements:

(i) G is solvable.

(ii) Every chief factor of G is elementary abelian.

(iii) Every characteristic factor of G is elementary abelian.

33. Show that if a finite group G is π-solvable for some set π of primes, then G is also π_0-solvable for all subsets $\pi_0 \subseteq \pi$.

34. Let G and H be finite groups. Show that the following are equivalent:

(i) Every subgroup of $G \times H$ is of the form $U \times V$ for subgroups $U \leqslant G$ and $V \leqslant H$.

(ii) G and H have coprime order.

35. Let K be a finite field of characteristic p, let $n \in \mathbb{N}$, and set $G := \mathrm{GL}_n(K)$.

(a) Compute the order of G.

(b) Let $U \leqslant G$ be the subset of upper diagonal matrices with entries 1 on the diagonal. Show that U is a Sylow p-subgroup of G.

(c) Show that $N_G(U)$ equals the subgroup B of upper triangular matrices.

(d) Determine $N_G(B)$.

36. Let $n \in \mathbb{N}$. Show that every group of order n is cyclic if and only if $(n, \varphi(n)) = 1$, where φ is the Euler phi-function.

37. Let G be a finite group and let $F(G)$ be its Fitting subgroup (cf. Exercise 23).

(a) Show that the solvable radical (cf. Exercise 24) of $C_G(F(G)) \cdot F(G)/F(G)$ is trivial. (Hint: Assume that the solvable radical is non-trivial. Deduce the existence

of a subgroup $S \trianglelefteq G$ such that $F(G) < S \leqslant C_G(F(G)) \cdot F(G)$ and $S/F(G)$ is abelian. Then deduce the contradiction that S is nilpotent.)

(b) Show that if G is solvable, then $C_G(F(G)) = Z(F(G))$ and that $G/Z(F(G))$ is isomorphic to a subgroup of $\mathrm{Aut}(F(G))$.

38. Let G be a finite group and let N be a minimal normal subgroup of G (i.e., $1 < N \trianglelefteq G$ such that for all $1 < M \trianglelefteq G$ with $M \leqslant N$ one has $M = N$). Show that $F(G) \leqslant C_G(N)$.

39. Let G be a finite group. For $1 \leqslant K \trianglelefteq H \trianglelefteq G$ with $K \trianglelefteq G$ on defines $C_G(H/K)$ by $C_G(H/K)/K = C_{G/K}(H/K)$, i.e., $C_G(H/K) = \{g \in G \mid ghg^{-1} \in hK \text{ for all } h \in H\} = \{g \in G \mid [g, H] \leqslant K\}$.

(a) Show that, with H and K as above, one has $C_G(H/K) \trianglelefteq G$.

(b) Let $1 = G_0 < G_1 < \cdots < G_r = G$ be a chief series of G. Show that $F(G) = \bigcap_{i=1}^{r} C_G(G_i/G_{i-1})$.

(c) Show that, with a chief series as in (b), $G/F(G)$ is isomorphic to a subgroup of $\times_{i=1}^{r} \mathrm{Aut}(G_i/G_{i-1})$.

40. Let $G := \mathrm{Sym}(4)$ and $H := O_2(G)$. Compute the transfer map $V_{H/1}^{G}\colon G \to H/1$.

41. Let p be a prime and let G be a finite p-nilpotent group. Show that every subgroup and every factor group of G is also p-nilpotent (without using Frobenius' Theorem).

42. Let G be a finite group, let p be a prime, and let N be a normal p'-subgroup of G. Show that for every p-subgroup P of G one has $N_{G/N}(PN/N) = N_G(P)N/N$ and $C_{G/N}(PN/N) = C_G(P)N/N$.

43. Let G be a finite group, let p be a prime, and let $H \leqslant G$ be a subgroup which controls the fusion of p-subgroups of G; i.e., there exists a Sylow p-subgroup S of G such that

- $S \leqslant H$ and
- for each $P \leqslant S$ and each $g \in G$ with $gPg^{-1} \leqslant S$ there exist $h \in H$ and $c \in C_G(P)$ with $g = hc$.

Let $g \in G$ and $H \leqslant U \leqslant G$. Show that also gHg^{-1} and U control the fusion of p-subgroups of G.

44. Let G be a finite group, let p be a prime, and let $H \leqslant G$. Show that the following statements are equivalent:

(i) H controls the fusion of p-subgroups of G.

(ii) $p \nmid [G : H]$, and for each Sylow p-subgroup S of H, each $P \leqslant S$, and each $g \in G$ with $gPg^{-1} \leqslant S$ there exist $h \in H$ and $c \in C_G(P)$ such that $g = hc$.

(iii) $p \nmid [G : H]$, and for each p-subgroup P of H and each $g \in G$ with $gPg^{-1} \leqslant H$, there exist $h \in H$ and $c \in C_G(P)$ with $g = hc$.

(iv) $p \nmid [G : H]$, and for all p-subgroups of P of H one has $N_G(P) = N_H(P)C_G(P)$.

(v) $p \nmid [G : H]$, and for each p-subgroup P of H, the images of $N_H(P)$ and $N_G(P)$ under the map $\varphi\colon N_G(P) \to \mathrm{Aut}(P)$ with $\varphi(n)(x) := nxn^{-1}$, $n \in N_G(P)$, $x \in P$, coincide.

45. Show that if G has an abelian Sylow p-subgroup P , then $H := N_G(P)$ controls the fusion of p-subgroups of G.