Finite Group Theory (Math 214)

UCSC, Fall 2009

Robert Boltje

Contents

1 The Alternating Group

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

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

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

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

the group $\mathrm{Alt}(n)$ is generated by its 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 π_1 and π_2 be two 3-cycles in $\mathrm{Alt}(n)$. Then there exists $\sigma \in \mathrm{Sym}(n)$ with $\pi_2 = \sigma\pi_1\sigma^{-1}$. Since $n \geqslant 5$, there exists a transpositions $\tau \in \mathrm{Sym}(n)$ which is disjoint to π_1. Thus $\tau\pi_1\tau^{-1} = \pi_1$ so that also $(\sigma\tau)\pi_1(\sigma\tau)^{-1} = \pi_2$. but either σ or $\sigma\tau$ is an element of $\mathrm{Alt}(n)$. $\square$

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

Proof Assume that $1 < N \trianglelefteq \mathrm{Alt}(n)$. We have to show that $N = \mathrm{Alt}(n)$. By Lemma 1.1, it suffices to show that N contains some 3-cycle. We choose $1 \neq \sigma \in N$ and write $\sigma = \gamma_1 \cdots \gamma_r$ as product of disjoint cycles $\gamma_1, \ldots, \gamma_r$ in $\mathrm{Sym}(n)$ and distinguish the following 4 cases:

Case 1: One of the cycles γ_i has length at least 4. Then we can write $\gamma_i = (a,b,c,d,e_1,\ldots,e_s)$, with $s \geqslant 0$. With $\rho := (a,b,c)$ we have

$$\begin{aligned} N \ni \rho\sigma\rho^{-1}\sigma^{-1} &= (a,b,c)(a,b,c,d,e_1,\ldots,e_s)(a,c,b)(e_s,\ldots,e_1,d,c,b,a) \\ &= (a,b,d)\,. \end{aligned}$$

Case 2: All cycles γ_i have length at most 3 and one of them has length 3. We may assume that $\gamma_1 = (a,b,c)$ and that $r \geqslant 2$. Then $\gamma_2 = (d,e)$ or $\gamma_2 = (d,e,f)$. With $\rho := (a,b,d)$ we have

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

or

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

and, by Case 1, N contains a 3-cycle.

Case 3: All cycles γ_i are transpositions and $r \geqslant 3$. Then we can write $\sigma = (a,b)(c,d)(e,f)\cdots$ with pairwise distinct a,b,c,d,e,f. With $\rho := (a,c,e)$ we have

$$\begin{aligned} N \ni \rho\sigma\rho^{-1}\sigma^{-1} &= (a,c,e)(a,b)(c,d)(e,f)(a,e,c)(a,b)(c,d)(e,f) \\ &= (a,c,e)(b,f,d) \end{aligned}$$

and N contains a 3-cycle by Case 2.

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

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

and N contains a 3-cycle by Case 1. $\square$

2 The Frattini Subgroup

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

2.2 Proposition (Frattini-Argument) *Let G be a finite group, let N be a normal subgroup of G and let $P \in \mathrm{Syl}_p(N)$ for some prime p. Then $G = N \cdot N_G(P)$.*

Proof Let $g \in G$. Then $P \leqslant N$ implies $gPg^{-1} \leqslant gNg^{-1} = N$ and $gPg^{-1} \in \mathrm{Syl}_p(N)$. By Sylow's Theorem, there exists $n \in N$ such that $ngPg^{-1}n^{-1} = P$. This implies that $ng \in N_G(P)$ and $g \in n^{-1}N_G(P) \subseteq N \cdot N_G(P)$. $\square$

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

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

2.4 Lemma *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 $P \in \mathrm{Syl}_p(H)$ for some prime p. Then $PN/N \in \mathrm{Syl}_p(H/N)$. Since H/N is nilpotent, PN/N is normal in H/N (cf. [P, 8.7]) and also characteristic in H/N. Since also H/N is normal in G/N, PN/N is normal in G/N and further, PN is normal in G. Since $P \in \mathrm{Syl}_p(PN)$ and $PN \trianglelefteq G$, the Frattini Argument implies that $G = PN \cdot N_G(P) = NN_G(P) \leqslant \Phi(G)N_G(P)$ and therefore $G = N_G(P)\Phi(G)$. By Lemma 2.3, we have $N_G(P) = G$ and P is normal in G. $\square$

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

Proof This follows from Lemma 2.4 with $H := N := \Phi(G)$. $\square$

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

Proof This follows from Lemma 2.4 with $H := G$ and $N := \Phi(G)$. $\square$

2.7 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 follows from [P, 8.8]
(ii)$\Rightarrow$(i): This follows from Corollary 2.6.
(ii)$\Rightarrow$(iii): Let $U < G$ be a maximal subgroup. Then $U/\Phi(G)$ is a maximal subgroup of the nilpotent group $G/\Phi(G)$. By [P, 8.8], $U/\Phi(G)$ is normal in $G/\Phi(G)$, and therefore U is normal in G. Since U is maximal in G, G/U has no subgroup different from U/U and G/U. This implies that G/U is a cyclic group of prime order. In particular, G/U is abelian. This implies that $G' \leqslant U$. Since this holds for every maximal subgroup U of G, we have $G' \leqslant \Phi(G)$.
(iii)$\Rightarrow$(iv): This follows from [P, 4.3(c)].
(iv)$\Rightarrow$(ii): This is clear. $\square$

3 The Fitting Subgroup

3.1 Remark Let p be a prime and let G be a finite group. If P and Q are normal p-subgroups of G then PQ is again a normal p-subgroup of G, since $|QP| = |P| \cdot |Q|/|P \cap Q|$. Therefore, the product of all normal p-subgroups of G is again a normal p-subgroup which we denote by $\mathrm{O}_p(G)$. By definition it is the largest normal p-subgroup of G. Clearly, O_p is also characteristic in G.

3.2 Definition Let G be a finite group. The *Fitting subgroup* $F(G)$ of G is defined as the product of the subgroups $\mathrm{O}_p(G)$, where p runs through the prime divisors of p. If $G = 1$ we set $F(G) := 1$.

3.3 Remark Let G be a finite group and let $p_1, \ldots, p_r$ denote the prime divisors of the finite group G. Then O_{p_i} is a Sylow p_i-subgroup of $F(G)$ for every $i = 1, \ldots, r$. Since $\mathrm{O}_{p_i}(G)$, $i = 1, \ldots, r$, is normal in G it is also normal in $F(G)$. It follows that $F(G)$ is nilpotent and that $F(G)$ is the direct product of the subgroups $\mathrm{O}_{p_1}, \ldots, \mathrm{O}_{p_r}(G)$. Moreover, since O_{p_i} is characteristic in G for all $i = 1, \ldots, r$, also $F(G)$ is characteristic in G.

3.4 Proposition *Let G be a finite group. Then $F(G)$ is the largest normal nilpotent subgroup of G; i.e., it is a normal nilpotent subgroup of G and contains every other normal nilpotent subgroup of G.*

Proof We have already seen in the previous remark that $F(G)$ is a normal nilpotent subgroup of G. Let N be an arbitrary normal nilpotent subgroup of G and let p be a prime divisor of $|N|$. Then N has a normal Sylow p-subgroup P. This implies that P is characteristic in N. Since N is normal G, we obtain that P is normal in G. Therefore, $P \leqslant \mathrm{O}_p(G) \leqslant F(G)$. Since N is the product of its Sylow p-subgroups, for the different prime divisors p of $|N|$, we obtain $N \leqslant F(G)$, as desired. $\square$

3.5 Corollary *Let N_1 and N_2 be normal nilpotent subgroups of a finite group G. Then N_1N_2 is again a normal nilpotent subgroup of G.*

Proof By Proposition 3.4, N_1 and N_2 are contained in $F(G)$. Therefore $N_1N_2 \leqslant F(G)$. since $F(G)$ is nilpotent, also its subgroup N_1N_2 is nilpotent. Clearly N_1N_2 is normal in G. $\square$

3.6 Definition A *minimal normal subgroup* of a finite group G is a normal subgroup M of G such that $M \neq 1$ and every normal subgroup N of G with is contained in M is equal to 1 or to M.

3.7 Proposition *Let G be a finite group.*

(a) *$C_G(F(G))F(G)/F(G)$ does not contain any solvable normal subgroup of $G/F(G)$ different from the trivial one.*

(b) *$\Phi(G) \leqslant F(G)$ and if G is solvable and non-trivial then $\Phi(G) < F(G)$.*

(c) *$F(G/\Phi(G)) = F(G)/\Phi(G)$ is abelian.*

(d) *If N is a minimal normal subgroup of G then $N \leqslant C_G(F(G))$. If moreover N is abelian then $N \leqslant Z(F(G))$.*

Proof (a) It suffices to show that $C_G(F(G))F(G)/F(G)$ contains no abelian normal subgroup of $G/F(G)$ different from 1. So let $N/F(G)$ be an abelian subgroup of $C_G(F(G))F(G)/F(G)$ which is normal in $G/F(G)$. Then $F(G)/leN$. We need to show that $F(G) = N$. Note that $N = F(G)C$ with $C = N \cap C_G(F(G))$. Since $N/C \cong F(G)/(F(G) \cap C)$ is nilpotent, there exists $l \in \mathbb{N}$ such that $Z_l(N/C) = 1$. Since $N \leqslant C(F(G))F(G)$, it follows that

$$Z_l(N) \leqslant C \cap N' \leqslant C \cap F(G) \leqslant Z(F(G)) \leqslant Z(N)\,.$$

This implies that $Z_{l+1}(N) = [Z_l(N), N] = 1$ and that N is nilpotent. Therefore, $N \leqslant F(G)$.

(b) Since $\Phi(G)$ is nilpotent (cf. Corollary 2.5) and normal in G, we have $\Phi(G) \leqslant F(G)$. Assume moreover that G is solvable and $G \neq 1$. Then $G/\Phi(G)$ is solvable and $\Phi(G) < G$. There exists an abelian normal subgroup $1 \neq M/\Phi(G) \trianglelefteq G/\Phi(G)$. Since $M/\Phi(G)$ is abelian (and hence nilpotent), Lemma 2.4 (with $H = M$ and $N = \Phi(G)$) implies that M is nilpotent. But then $M \leqslant F(G)$. Therefore, $\Phi(G) < M \leqslant F(G)$.

(c) Since $F(G)$ is nilpotent also $F(G)/\Phi(G)$ is nilpotent. Moreover, $F(G)/\Phi(G)$ is normal in $G/\Phi(G)$. Therefore $F(G)/\Phi(G) \leqslant F(G/\Phi(G))$. Conversely, we can write $F(G/\Phi(G)) = H/\Phi(G)$ with $\Phi(G) \leqslant H \trianglelefteq G$. Since $H/\Phi(G)$ is nilpotent, Lemma 2.4 (with $N = \Phi(G)$) implies that H is nilpotent and therefore $H \leqslant F(G)$. Thus, $F(G/\Phi(G)) = H/\Phi(G) \leqslant F(G)/\Phi(G)$. Since $F(G)$ is normal in G, we have $\Phi(F(G)) \leqslant \Phi(G) \leqslant F(G)$. Since $F(G)$ is nilpotent, Theorem 2.7 implies that $F(G)/\Phi(F(G))$ is abelian. But $F(G)/\Phi(G)$ is isomorphic to a factor group of $F(G)/\Phi(F(G))$ and therefore also abelian.

(d) Since N is a minimal normal subgroup, we either have $N \cap F(G) = 1$ or $N \cap F(G) = N$. If N is abelian then, N is nilpotent and $N \leqslant F(G)$. It follows that $1 \neq N \cap Z(F(G)) \trianglelefteq G$ (see homework problem), and the minimiality of N implies $N \leqslant Z(F(G))$. If N is not abelian then $N \cap F(G) = 1$ (since otherwise $N \leqslant F(G)$ implies $1 < N' < N$ with $N' \underset{\text{char}}{\trianglelefteq} N \trianglelefteq G$ and thus $N' \trianglelefteq G$, a contradiction). But $N \cap F(G) = 1$ implies $[N, F(G)] \leqslant N \cap F(G) = 1$ and $N \leqslant C_G(F(G))$. $\square$

4 p-Groups

4.1 Lemma *Let G be a group and assume there exists $H \leqslant Z(G)$ 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 $n \in \mathbb{Z}$ and $h \in H$. For $n, n' \in \mathbb{Z}$ 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. □

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

Proof By [P, 5.10], we have $Z(G) > 1$. Therefore, $|G/Z(G)|$ divides p so that $G/Z(G)$ is cyclic. Now Lemma 4.1 applies. □

4.3 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 is elementary abelian of order p^n, we call n the *rank* of G.

4.4 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 defining the scalar multiplication $(k + p\mathbb{Z}) \cdot x := x^k$ 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.

4.5 Theorem *Let p be a prime and let G be a p-group. Then:*

(a) *$\Phi(G) = G' \cdot G^p$, where $G^p := \langle \{g^p \mid g \in G\} \rangle$. If $p = 2$, one has $\Phi(G) = G^2$.*

(b) *$G/\Phi(G)$ is elementary abelian.*
(c) *For every $N \trianglelefteq G$ on has: G/N is elementary abelian $\iff \Phi(G) \leqslant N$.*
(d) *If $U \leqslant G$, then $\Phi(U) \leqslant \Phi(G)$.*
(e) *If $N \trianglelefteq G$, then $\Phi(G/N) = \Phi(G)N/N$.*

Proof (a)–(c): By Theorem 2.7 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 (b); 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 (c). If $\Phi(G) \leqslant N$, then $G/N \cong (G/\Phi(G))/(N/\Phi(G))$ is elementary abelian by (b). 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 (c) is proved. From (c) 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 $\Phi(G) = G^2$.

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

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

4.6 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:*

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

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

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

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

Proof (a) With Lemma 2.3 we obtain

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

(b) Let $\{x_1, \ldots, x_n\}$ be a minimal generating set of G consisting of n elements. By (a) 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 (a) the corresponding proper subset of $\{x_1, \ldots, x_n\}$ then generates G. This contradicts the minimality of the set $\{x_1, \ldots, x_n\}$.

(c) If $x \in G \smallsetminus \Phi(G)$, 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 (a) and (b), $\{x, x_2, \ldots, x_d\}$ is a minimal set of generators of G. □

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

(b) Part (b) 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 $\{3 + 6\mathbb{Z}, 2 + 6\mathbb{Z}\}$.

4.8 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. In Lemma 4.12 we will need the following property of $Y \rtimes X$ which is now easy to verify:

$$\{a \in Y \rtimes X \mid a^p = 1\} = \langle x, y^p \rangle\,. \tag{4.8.a}$$

(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 $\mathrm{GL}_{n+2}(\mathbb{Z}/p\mathbb{Z})$ 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 $i, j \in \{1, \ldots, n\}$ 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 $a_1, \ldots, a_n, b_1, \ldots, b_n, c \in \{0, 1, \ldots, p-1\}$.

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

(iv) The subgroups $\langle x_1, \ldots, x_n, z\rangle$ and $\langle y_1, \ldots, y_n, z\rangle$ 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 identify $Z := \langle z\rangle$ 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 ${}^y x = xz$.

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

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

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 prove 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

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

and

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

with

$$y^i x = xy^i y^{-i} x^{-1} y^i x = xy^i [y^{-i}, x^{-1}] = xy^i [y^{-1}, x^{-1}]^i\,,$$

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 4.5. 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

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

since $y^6 \in G^2 \leqslant Z(G)$. $\square$

4.10 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 4.8(b).

(c) If G is isomorphic to the group in Example 4.8(b) then $f\colon G \mapsto G$, $a \mapsto a^p$, is a group homomorphism with image $Z(G)$ and elementary abelian kernel of rank 2.

Proof From Lemma 4.1 we have $|G/Z(G)| \geqslant p^2$ and from [P, 5.10] we have $|Z(G)| \geqslant p$. This implies $|Z(G)| = p$. Lemma 4.1 also implies that $G/Z(G)$ is elementary abelian. With Theorem 4.5(a) and (c) 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 $x \in G \smallsetminus Y$ 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 $x \in G \smallsetminus Y$ of order 2, then we pick an element $x \in G \smallsetminus Y$ 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 $x \in G \smallsetminus Y$ of order p such that $xyx^{-1} = y^{1+p}$ which then implies that G is isomorphic to the semidirect product of Example 4.8(b). We prove the claim. First choose any $x_1 \in G \smallsetminus Y$. Then there exists $i \in \{1, \ldots, p\}$ with $x_1^p = y^{pi}$, since $x_1^p \in G^p \leqslant \Phi(G) = Z(G) = \langle y^p \rangle$. By Lemma 4.9(b) we have $(x_1 y^{-i})^p = x_1^p y^{-ip} = 1$ and therefore the element $x_2 := x_1 y^{-i} \in G \smallsetminus Y$ 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 $j \in \{1, \ldots, p-1\}$ 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 $x \in G \smallsetminus Z(G)$. Then $X := \langle x, z \rangle$ is elementary abelian of order p^2 and also maximal in G. Let $y_1 \in G \smallsetminus X$. 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 $i, j \in \{0, \ldots, p-1\}$. Since the classes of y_1 and x commute in $G/Z(G)$, we obtain $i = 1$. Since G is not abelian we have $j \neq 0$, and therefore $y_1 x y_1^{-1} = xz^j$ for some $j \in \{1, \ldots, p-1\}$. Let $k \in \{1, \ldots, p-1\}$ with $kj \equiv 1 \mod p$ and set $y := y_1^k$. Then $yzy^{-1} = 1$, $yxy^{-1} = y_1^k x y_1^{-k} = xz^{kj} = xz$ and we obtain $G \cong X \rtimes Y \cong E_{p^3}$ as described at the end of Example 4.8(c).

(c) We may assume that $G = Y \rtimes X$ with the notation from Example 4.8(b). By Lemma 4.9(b), the map f is a homomorphism. Obviously, $\langle x, y^p \rangle \leqslant \ker(f)$ and $Z(G) = \langle y^p \rangle \leqslant \mathrm{im}(f) \leqslant G^p = Z(G)$. By the fundamental theorem of homomorphisms we even have equality everywhere. $\square$

4.11 Notation For a p-group G and $n \in \mathbb{N}_0$ we set

$$\Omega_n(G) := \langle x \in G \mid x^{p^n} = 1 \rangle .$$

Obviously, this is a characteristic subgroup of G.

4.12 Lemma *Let G be a p-group for an odd prime p and let $N \trianglelefteq G$. If N is not cyclic then N contains an elementary abelian subgroup of rank 2 which is normal in G.*

Proof Induction on $|G|$. The base case is $|G| = p^2$. The hypothesis implies that $N = G$ and that N is elementary abelian. Therefore, we can choose N as the desired subgroup.

Now let $|G| \geqslant p^3$. Since $N \neq 1$ it follows from a homework problem that N has a subgroup M of order p with is normal in G. By [P, 5.10] applied to M and N, $M \leqslant Z(N)$. We first consider the case that N/M is cyclic. Then N is abelian. Since N is not cyclic, it is a direct product of two non-trivial cyclic subgroups. This implies that the characteristic subgroup $\Omega_1(N)$ of N is elementary abelian of rank 2. Thus, $\Omega_1(N)$ is a subgroup as desired. From now on we can assume that N/M is not cyclic. By induction, applied to $N/M \trianglelefteq G/M$ there exists $N < U \leqslant M$ with $U \trianglelefteq G$ and U/N elementary abelian of rank 2. Since U is not cyclic, U can be elementary abelian, the direct product of two non-trivial cyclic subgroups, isomorphic to E_{p^3} or isomorphic to the group in Example 4.8(b). In the first and third case, choose any subgroup of U of order p^2 which is normal in G (see homework problem for the existence). This subgroup has the desired property. In the second and fourth case consider $\Omega_1(U)$. This group again has the desired property, cf. Theorem 4.10. $\square$

4.13 Corollary *Let G be a p-group for an odd prime p and assume that G has precisely one subgroup of order p. Then G is cyclic.*

Proof Assume that G is not cyclic. Then Lemma 4.12 with $N = G$ implies that G has a normal subgroup which is elementary abelian of rank 2. But then G has at least $p+1$ subgroups of order p. This is a contradiction. $\square$

4.14 Definition (a) For every integer $n \geqslant 3$ we define the *generalized quaternion group* Q_{2^n} of order 2^n as

$$Q_{2^n} := \langle x, y \mid x^{2^{n-1}} = 1, x^{2^{n-2}} = y^2, yxy^{-1} = x^{-1} \rangle .$$

(b) For every integer $n \geqslant 4$ we define the *semidihedral group* SD_{2^n} by

$$SD_{2^n} := \langle x, y \mid x^{2^{n-1}} = 1, y^2 = 1, yxy^{-1} = x^{2^{n-2}-1} \rangle \, .$$

4.15 Remark (a) The group Q_{2^n} has actually order 2^n, $\langle x \rangle$ is a subgroup of index 2 in Q_{2^n}, Q_{2^n} has only one element of order 2 namely $z := y^2 = x^{2^{n-2}}$ and $< z >= Z(Q_{2^n})$, cf. homework.

(b) It follows from (a) and Theorem 4.10 that the generalized quaternion group of order 8 is equal to the quaternion group of order 8.

(c) The group SD_{2^n} has order 2^n, the subgroup $\langle x \rangle$ has index 2. It is the semidirect product of the cyclic group $\langle x \rangle$ with the group $\langle y \rangle$ of order 2.

(d) Without proof we state: If G is a 2-group with precisely one subgroup of order 2 then G is cyclic or isomorphic to a generalized quaternion group.

(e) Again without proof we state the following result: Let G be a non-abelian 2-group of order 2^n, and assume that G has a cyclic subgroup of order 2^{n-1}. Then $n \geqslant 3$ and exactly one of the four statements holds:

(i) G is isomorphic to the dihedral group D_{2^n}.

(ii) G is isomorphic to the generalized quaternion group Q_{2^n}.

(iii) $n \geqslant 4$ and G is isomorphic to the semidihedral group SD_{2^n}.

(iv) $n \geqslant 4$ and G is isomorphic to the group $\langle x, y \mid x^{2^{n-1}} = 1, y^2 = 1, yxy^{-1} = x^{2^{n-2}+1} \rangle$.

The groups in (i),(iii),(iv) are semidirect products of the cyclic subgroup of order 2^{n-1} with a subgroup of order 2. The group in (ii) is not a semidirect product. They are pairwise non-isomorphic, because the numbers of elements of order 2 they contain are different.

5 Group Cohomology

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

5.1 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 $(fg)(x_1, \dots, x_n) = f(x_1, \dots, x_n)g(x_1, \dots, x_n)$, for $f, g \in F(G^n, A)$ and $x_1, \dots, x_n \in G$. If $n = 0$ we set $G^n := \{1\}$. For each $n \in \mathbb{N}_0$ there is a group homomorphism

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

given by

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

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

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

and

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

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 $[f] \in H^n(G, A)$.

5.2 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 $x, y \in G$. We will see later that $H^2(G, A)$ describes the extensions $1 \to A \to X \to G \to 1$ of G by A, up to a suitable equivalence.

(d) If A has finite exponent e then $f^e = 1$ for all $f \in F(G^n, A)$ and all $n \in \mathbb{N}_0$. In particular, each cocycle and each cohomology class has an order which divides e.

5.3 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

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

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

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

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

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

and $[f]^{|G|} = 1$ in $H^n(G, A)$. ∎

5.4 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 5.2(d) and Proposition 5.3 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 $[f] = [f]^1 = [f]^{rk+sl} = ([f]^k)^r([f]^l)^s = 1$. ∎

6 Group Extensions and Parameter Systems

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

6.1 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

$$\begin{tikzcd}
& H \arrow[dr, "\nu"] \arrow[dd, "\gamma"'] & \\
K \arrow[ur, "\varepsilon"] \arrow[dr, "\tilde{\varepsilon}"'] & & G \\
& \tilde{H} \arrow[ur, "\tilde{\nu}"'] &
\end{tikzcd} \tag{6.1.a}$$

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 $\mathrm{Ext}(G, K)$.

6.2 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

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

are already equivalent if there exists a *homomorphism* $\gamma\colon H \to \tilde{H}$ which makes Diagram (6.1.a) commutative. In fact, it is easy to see that in this case it follows that γ is an isomorphism.

6.3 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* $g\colon G \to K$ *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. ∎

6.4 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 $\mathrm{Par}(G,K)$.

6.5 Remark Every extension of G by K and every choice of elements h_x as in Proposition 6.3 leads to a parameter system (α, κ) of G and K. If h'_x is another choice of elements then, by Proposition 6.3(e), one obtains an equivalent parameter system (α', κ'). Thus, Proposition 6.3 defines a function

$$\varphi\colon \mathrm{ext}(G, K) \to \mathrm{Par}(G, K)\,.$$

6.6 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 6.4(b) defines a group action of $F(G, K)$ on $\mathrm{par}(G, K)$.

Proof (a) By Axiom (i) in Definition 6.4(a), 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 Axiom (ii) in Definition 6.4(a) 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 $x \in G$, Axiom (ii) in Definition 6.4(a) implies $\kappa(x, 1\cdot 1)\kappa(x\cdot 1, 1) = \alpha_x(\kappa(1,1))\kappa(x, 1\cdot 1)$. Thus, $\kappa(x,1) = \alpha_x(\kappa(1,1))$.

(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

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

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 $(\alpha',\kappa')\in\mathrm{par}(G,K)$. ∎

6.7 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. □

6.8 Theorem (Schreier) *The constructions in Proposition 6.3 and Proposition 6.7 induce mutually inverse bijections between* $\mathrm{Ext}(G,K)$ *and* $\mathrm{Par}(G,K)$.

Proof First assume that

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

are equivalent group extensions of G by K. Then there exists an isomorphism $\gamma\colon H \to \tilde H$ such that the diagram

$$\begin{tikzcd}
 & H \arrow[dr, "\nu"] \arrow[dd, "\gamma"] & \\
K \arrow[ur, "\varepsilon"] \arrow[dr, "\tilde{\varepsilon}"'] & & G \\
 & \tilde{H} \arrow[ur, "\tilde{\nu}"'] &
\end{tikzcd}$$

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 6.3, i.e.,

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

for all $x, y \in G$ and $a \in K$. We set $\tilde{h}_x := \gamma(h_x)$ for each $x \in G$. Then, $\tilde{\nu}(\tilde{h}_x) = \tilde{\nu}(\gamma(h_x)) = \nu(h_x) = x$ 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 γ 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 6.3 induces a map

$$\Phi\colon \mathrm{Ext}(G, K) \to \mathrm{Par}(G, K) .$$

Next let $(\alpha, \kappa) \in \mathrm{par}(G, K)$, $f \in F(G, K)$, 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 6.7. We want to show that they are equivalent. We define $\gamma\colon H \to \tilde{H}$ by

$$\gamma(a, x) := \Big(ea\alpha_x(e)^{-1} f(x)^{-1}, x\Big) \quad \text{with} \quad e := \kappa(1, 1)^{-1} f(1)^{-1} \kappa(1, 1) .$$

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

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

and

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

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

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

and

$$\tilde\nu(\gamma(a,x)) = \tilde\nu(ea\alpha_x(e)^{-1}f(x)^{-1},x) = x = \nu(a,x)\,.$$

Together with Remark 6.2(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 6.7 induces a map

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

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 6.3 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 6.7. We show that the two group extensions

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

are equivalent. In fact, let $\gamma\colon \tilde H\to H$ be defined by

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

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

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

and

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

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

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

by Proposition 6.3(c), and

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

Therefore, the two group extensions

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

are equivalent, and $\Psi \circ \Phi = \mathrm{id}$.

Now let $(\alpha,\kappa) \in \mathrm{par}(G,K)$ and let $1 \longrightarrow K \xrightarrow{\varepsilon} H \xrightarrow{\nu} G \longrightarrow 1$ be the group extension constructed in Proposition 6.7. 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

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

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. $\square$

6.9 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 $\delta\colon C \to H/\varepsilon(K)$, $c \mapsto c\varepsilon(K)$ 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

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

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

6.10 Remark (a) If the conditions in Proposition 6.9 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 splits and is represented by the semidirect product of G with K under the action defined by α.

6.11 Definition Even if K is not abelian, one can still define the so-called *non-commutative* cohomology $H^0(G, K)$ and $H^1(G, K)$ of G with values in K as follows:

(a) $H^0(G, K) := K^G$, the set of G-fixed points of K. This is a subgroup of K.

(b) $Z^1(G, K)$ is defined as the set of all functions $\mu\colon G \to K$ satisfying

$$\mu(xy) = {}^x\mu(y)\mu(x)\,.$$

It's elements are called *1-cocycles* or crossed homomorphisms from G to K. Two functions $\lambda, \mu \in Z^1(G, K)$ are called *equivalent* if there exists $a \in K$ such that

$$\lambda = {}^x a \cdot \mu(x) \cdot a^{-1}$$

for all $x \in G$. This defines an equivalence relation (see Homework problem). The equivalence class of $\mu \in Z^1(G, K)$ is denoted by $[\mu]$. The set of equivalence classes of $Z^1(G, K)$ is denoted by $H^1(G, K)$. It is not a group, but it has the structure of a *pointed set*, a set with a distinguished element, namely the class $[1]$ of the constant function $1\colon G \to K$.

6.12 Remark (a) There are no non-commutative versions of $H^n(G, K)$ for $n \geqslant 2$.

(b) If $K = A$ is abelian then the definitions in 6.11 coincide with the usual cohomology groups.

(c) If G acts on K and $\mu \in Z^1(G, K)$ then the equation $\mu(xy) = {}^x\mu(y)\mu(x)$ implies that $\mu(1) = 1$ by setting $x = y = 1$. Moreover, by setting $y = x^{-1}$ we obtain ${}^x\mu(x^{-1}) = \mu(x)^{-1}$ and $x^{-1}\mu(x) = \mu(x^{-1})^{-1}x^{-1}$.

6.13 Theorem *Let $\alpha\colon G \to \mathrm{Aut}(K)$ be a group homomorphism and let $H := K \rtimes G$ be the corresponding semidirect product. To simplify notation we assume that $K \trianglelefteq H$ and $G \leqslant H$ with $K \cap G = 1$ and $KG = H$. Let $\mathcal{C}$ denote the set of all complements of K in H, i.e., subgroups $C \leqslant H$, satisfying $K \cap C = 1$ and $KC = H$.*

(a) H acts by conjugation on $\mathcal{C}$ and the H-orbits of $\mathcal{C}$ are equal to the K-orbits of $\mathcal{C}$. The K-conjugacy classes of $\mathcal{C}$ will be denoted by $\overline{\mathcal{C}}$.

(b) For each $C \in \mathcal{C}$ there exists a unique function $\mu_C\colon G \to K$ such that

$$\mu_C(x) \in xC \quad \text{for all } x \in G.$$

Moreover, $\mu_C \in Z^1(G, K)$. Conversely, for every $\mu \in Z^1(G, K)$, the set

$$C_\mu := \{\mu(x)^{-1}x \mid x \in G\}$$

is a subgroup and a complement of K in H. These two constructions define mutual inverse bijections

$$\mathcal{C} \leftrightarrow Z^1(G, K)\,.$$

Moreover, these bijections induce mutually inverse bijections

$$\overline{\mathcal{C}} \leftrightarrow H^1(G, K)\,.$$

Proof Both statements of (a) are easy to verify.

(b) Let $C \in \mathcal{C}$. For every $x \in G$ there exist unique elements $\mu(x) \in K$ and $c \in C$ such that

$$x = \mu(x)c\,.$$

This implies the first statement. Next we show that the function $\mu\colon G \to K$ is a 1-cocycle. Let $x, y \in G$ and let $c, d \in C$ with $x = \mu(x)c$ and $y = \mu(y)d$. Then

$$xy = x\mu(y)d = {}^x\mu(y)xd = {}^x\mu(y)\mu(x)cd$$

with ${}^x\mu(y)\mu(x) \in K$ and $cd \in C$.

Next let $\mu \in Z^1(G, K)$ and let C_μ be defined as in the theorem. First we show that C_μ is a subgroup: For $x, y \in G$ we have

$$\mu(x)^{-1}x\mu(y)^{-1}y = \mu(x)^{-1}\,{}^x\mu(y)^{-1}xy = \mu(xy)^{-1}xy$$

which shows that the product of two elements in C_μ is again in C_μ. Moreover, if for $x \in G$ we have

$$x^{-1}\mu(x) = \mu(x^{-1})^{-1}x^{-1}$$

by Remark 6.12(c). If x is an element in G such that $\mu(x)^{-1}x \in K$, then also x is in K and therefore, $x = 1$ and $\mu(x)^{-1}x = 1$. Therefore, $K \cap C_\mu = 1$. Finally, every element in H can be written as ax with $a \in K$ and $x \in G$ and $ax = a\mu(x)\mu(x)^{-1}x \in KC_\mu$. This completes the proof that $C_\mu \in \mathcal{C}$.

It is easy to see that the two constructions are inverse to each other so that we obtain a bijection $\mathcal{C} \leftrightarrow Z^1(G, K)$.

Next assume that $C, D \in \mathcal{C}$ and that $D = {}^a C$ with $a \in K$. Let $x \in G$ and let $c \in C$ such that $x = \mu_C(x)c$. Then,

$$x = \mu_C(x)c = \mu(x) \cdot {}^c a \cdot a^{-1} \cdot {}^a c$$

with $\mu_C(x) \cdot {}^c a \cdot a^{-1} \in K$ and ${}^a c \in D$. Therefore,

$$\mu_D = \mu(x) \cdot {}^c a \cdot a^{-1} = \mu_C(x) \cdot {}^{\mu_C(x)^{-1}x} a \cdot a^{-1} = {}^x a \cdot \mu(x) \cdot a^{-1} .$$

Therefore, $[\mu_C] = [\mu_D] \in H^1(G, K)$. Conversely, let $\lambda, \mu \in Z^1(G, K)$ and let $a \in K$ such that $\lambda(x) = {}^x a \cdot \mu(x) \cdot a^{-1}$ for all $x \in G$. Then C_λ consists of all elements of the form $\lambda(x)^{-1}x = a \cdot \mu(x)^{-1} \cdot {}^x a^{-1} \cdot x = a\mu(x)^{-1}xa^{-1}$ with $x \in G$. But this is just $aC_\mu a^{-1}$. This completes the proof of the Theorem. $\square$

7 Group Extensions with Abelian Kernel

Throughout this section let A be an abelian group and let G be an arbitrary group.

7.1 Remark 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 6.3. 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, $c_{\kappa(x,y)} = \mathrm{id}_K$ and 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 can partition $\mathrm{Ext}(G, A)$ and $\mathrm{Par}(G, A)$ into disjoint unions indexed by $\alpha \in \mathrm{Hom}(G, \mathrm{Aut}(A))$, i.e., by the possible actions of G on A:

$$\mathrm{Par}(G, A) = \dot{\bigcup_\alpha} H^2_\alpha(G, A)$$

and

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

where $\mathrm{Ext}_\alpha(G, A)$ denotes those extensions which induce the automorphism system α. For given action $\alpha \colon G \to \mathrm{Aut}(A)$, we have the bijections from Schreier's Theorem 6.8:

$$\mathrm{Ext}_\alpha(G, A) \leftrightarrow H^2_\alpha(G, A)\,.$$

Recall that $H^2_\alpha(G, A)$ is an abelian group. Its identity element $[1]$ corresponds to the semidirect product extension of G by A under the action α. The multiplication in the group $H^2_\alpha(G, A)$ corresponds to the so-called *Baer product* which can be defined purely in terms of extensions.

Finally, if the above extension splits then the A-conjugacy classes (recall that they are the same as the H-conjugacy classes) of complements of A in H are parametrized by $H^1(G, A)$, by Theorem 6.13

7.2 Corollary *Assume that* $\gcd(|G|, |A|) = 1$.

(a) *Every extensions of* G *by* A *splits. In particular, for every action* $\alpha \in \mathrm{Hom}(G, \mathrm{Aut}(A))$, *there exist precisely one extension of* G *by* A *(up to equivalence) with automorphism system* α, *namely the semidirect product* $A \rtimes_\alpha G$.

(b) *Let* $\alpha \in \mathrm{Hom}(G, \mathrm{Aut}(A))$ *and let* $H := A \rtimes_\alpha G$ *be the corresponding semidirect product. Then any two complements of* A *in* H *are conjugate under* A.

Proof (a) We have $\mathrm{Ext}_\alpha(G, A) \cong H^2_\alpha(G, A)$ by the above remark. But the latter group is trivial by Corollary 5.4. Thus, the only extension of G by A, up to equivalence, that has automorphism system α, is the semidirect product.

(b) This follows immediately from Theorem 6.13. $\square$

8 Group Extensions with Non-Abelian Kernel

Throughout this section let K and G be arbitrary groups.

8.1 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 fundamental theorem of homomorsphisms, we obtain a homomorphism $\mathrm{Out}(K) \to \mathrm{Aut}(Z(K))$, $f\mathrm{Inn}(K) \mapsto f|_{Z(K)}$, 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 $\zeta := \mathrm{res}^K_{Z(K)} \circ \omega\colon G \to \mathrm{Aut}(Z(K))$. The next theorem will show that, if $\mathrm{Par}_\omega(G, K)$ is non-empty then it is in bijection with $H^2_\zeta(G, Z(K))$.

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

8.2 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

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

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. ∎

8.3 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 8.2, $\mathrm{Par}_\omega(G, K)$ 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 $H^2_\zeta(G, Z(K)) = 1$.
□

8.4 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

$$
\begin{aligned}
&c_{\vartheta(x,y,z)} \\
&= c_{\alpha_x(\chi(y,z))} \circ c_{\chi(x,yz)} \circ c_{\chi(xy,z)}^{-1} \circ c_{\chi(x,y)}^{-1} \\
&= \alpha_x \circ c_{\chi(y,z)} \circ \alpha_x^{-1} \circ \alpha_x \circ \alpha_{yz} \circ \alpha_{xyz}^{-1} \circ \alpha_{xyz} \circ \alpha_z^{-1} \circ \alpha_{xy}^{-1} \circ \alpha_{xy} \circ \alpha_y^{-1} \circ \alpha_x^{-1} \\
&= \alpha_x \circ \alpha_y \circ \alpha_z \circ \alpha_{yz}^{-1} \circ \alpha_{yz} \circ \alpha_z^{-1} \circ \alpha_y^{-1} \circ \alpha_x^{-1} \\
&= \mathrm{id}_K \,,
\end{aligned}
$$

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

$$
\begin{aligned}
&\zeta_x(\vartheta(y,z,w))\vartheta(x,yz,w)\vartheta(x,y,z) \\
&= \alpha_x(\alpha_y(\chi(z,w)))\alpha_x(\chi(y,zw))\alpha_x(\chi(yz,w))^{-1}\alpha_x(\chi(y,z))^{-1}\vartheta(x,yz,w)\cdot \\
&\qquad\qquad \cdot \vartheta(x,y,z) \\
&= \alpha_x(\alpha_y(\chi(z,w)))\alpha_x(\chi(y,zw))\alpha_x(\chi(yz,w))^{-1}\vartheta(x,yz,w)\alpha_x(\chi(y,z))^{-1}\cdot \\
&\qquad\qquad \cdot \vartheta(x,y,z) \\
&= \alpha_x(\alpha_y(\chi(z,w)))\alpha_x(\chi(y,zw))\alpha_x(\chi(yz,w))^{-1}\cdot \\
&\qquad\qquad \cdot \alpha_x(\chi(yz,w))\chi(x,yzw)\chi(xyz,w)^{-1}\chi(x,yz)^{-1}\alpha_x(\chi(y,z))^{-1}\cdot \\
&\qquad\qquad \cdot \alpha_x(\chi(y,z))\chi(x,yz)\chi(xy,z)^{-1}\chi(x,y)^{-1} \\
&= \alpha_x(\alpha_y(\chi(z,w)))\alpha_x(\chi(y,zw))\chi(x,yzw)\chi(xyz,w)^{-1}\chi(xy,z)^{-1}\chi(x,y)^{-1} \\
&= \alpha_x(\alpha_y(\chi(y,w)))\alpha_x(\chi(y,zw))\chi(x,yzw)\chi(xy,zw)^{-1}\chi(x,y)^{-1}\cdot \\
&\qquad\qquad \cdot \chi(x,y)\chi(xy,zw)\chi(xyz,w)^{-1}\chi(xy,z)^{-1}\chi(x,y)^{-1} \\
&= \alpha_x(\alpha_y(\chi(z,w)))\vartheta(x,y,zw)\chi(x,y)\chi(xy,zw)\chi(xyz,w)^{-1}\chi(xy,z)^{-1}\chi(x,y)^{-1} \\
&= \chi(x,y)\alpha_{xy}(\chi(z,w))\chi(xy,zw)\chi(xyz,w)^{-1}\cdot \\
&\qquad\qquad \cdot \chi(xy,z)^{-1}\chi(x,y)^{-1}\vartheta(x,y,zw) \\
&= \chi(x,y)\vartheta(xy,z,w)\chi(x,y)^{-1}\vartheta(x,y,zw) \\
&= \vartheta(xy,z,w)\vartheta(x,y,zw)\,.
\end{aligned}
$$

(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

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

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

$$\begin{aligned}
&\vartheta'(x,y,z) \\
&= f(x)\alpha_x\Big(f(y)\alpha_y(f(z))\chi(y,z)f(yz)^{-1}g(y,z)\Big)f(x)^{-1}\cdot \\
&\qquad\qquad \cdot f(x)\alpha_x(f(yz))\chi(x,yz)f(xyz)^{-1}g(x,yz)\cdot \\
&\qquad\qquad \cdot g(xy,z)^{-1}f(xyz)\chi(xy,z)^{-1}\alpha_{xy}(f(z))^{-1}f(xy)^{-1}\cdot \\
&\qquad\qquad \cdot g(x,y)^{-1}f(xy)\chi(x,y)^{-1}\alpha_x(f(y))^{-1}f(x)^{-1} \\
&= f(x)\alpha_x(f(y))\alpha_x(\alpha_y(f(z)))\alpha_x(\chi(y,z))\cdot \\
&\qquad\qquad \cdot \chi(x,yz)\chi(xy,z)^{-1}\alpha_{xy}(f(z)^{-1})\chi(x,y)^{-1}\alpha_x(f(y)^{-1})f(x)^{-1}\cdot \\
&\qquad\qquad \cdot \alpha_x(g(y,z))g(x,yz)g(xy,z)^{-1}g(x,y)^{-1} \\
&= f(x)\alpha_x(f(y))\alpha_x(\alpha_y(f(z)))\vartheta(x,y,z)\chi(x,y)\alpha_{xy}(f(z)^{-1})\cdot \\
&\qquad\qquad \cdot \chi(x,y)^{-1}\alpha_x(f(y)^{-1})f(x)^{-1}(\partial^2_\zeta(g))(x,y,z) \\
&= f(x)\alpha_x(f(y))\alpha_x(\alpha_y(f(z)))\alpha_x(\alpha_y(f(z)^{-1}))\cdot \\
&\qquad\qquad \cdot \alpha_x(f(y)^{-1})f(x)^{-1}\vartheta(x,y,z)(\partial^2_\zeta(g))(x,y,z) \\
&= \vartheta(x,y,z)(\partial^2_\zeta(g))(x,y,z)\,,
\end{aligned}$$

which shows that the cohomology classes $[\vartheta]$ and $[\vartheta']$ coincide. $\square$

8.5 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 8.4 is called the *obstruction* of ω.

8.6 Theorem *Let $\omega\colon G \to \mathrm{Out}(K)$ be a group homomorphism and let $\zeta := \mathrm{res}^K_{Z(K)} \circ \omega \in \mathrm{Hom}(G, \mathrm{Aut}(Z(K)))$. 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

$$\begin{gathered}\omega(x) = \alpha_x \mathrm{Inn}(K)\,, \ \ \alpha_x \circ \alpha_y = c_{\kappa(x,y)} \circ \alpha_{xy} \text{ and} \\ \alpha_x(\kappa(y,z))\kappa(x,yz)\kappa(xy,z)^{-1}\kappa(x,y)^{-1} = 1\,,\end{gathered}$$

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 $\vartheta = d^2_\zeta(\varphi)$. 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. ∎

9 The Theorem of Schur-Zassenhaus

9.1 Definition Let π be a set of primes. We denote by π' 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 factorization of n then the *π-part* n_π of n is defined as $\prod_{p_i \in \pi} p_i^{\alpha_i}$. One has $n = n_\pi n_{\pi'}$.

(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 every 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 $g_\pi g_{\pi'} = g = g_{\pi'} g_\pi$. These elements are called the *π-part* and the *π'-part* of g. One has $g_\pi, g_{\pi'} \in \langle g \rangle$.

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

9.2 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 $\mathrm{Alt}(5)$ and $\pi = \{2,5\}$ or $\pi = \{3,5\}$ one sees that in general Hall π-subgroups do not exist.

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

(i) *G is solvable.*

(ii) *For every $N \lhd G$ 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. $\square$

9.4 Remark Let G be a finite group. 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.

9.5 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 In the case that H is abelian, Parts (a) and (b) are immediate from Corollary 7.2.

From now on we assume that H is not abelian. 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 $|H| > 1$. This will be done in 7 steps.

Claim 1: If $U < G$, then $U \cap H$ has a complement in U. *Proof:* $U \cap H$ is normal in U and a 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 $1 < N \triangleleft G$, 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:* (a) 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.

(b) 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. since H is not abelian, we have $1 < \Phi(H) < H$. Now Claim 3 applies and (a) and (b) hold.

Claim 5: If H is solvable, then (a) and (b) hold. *Proof:* This follows immediately from Theorem 9.3 and Claim 4.

Claim 6: Part (a) holds. *Proof:* 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.

Claim 7: Part (b) holds. *Proof:* By Claim 5 we may assume that G/H is solvable. By Theorem 9.3, 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, $1 \neq K \cap R$ 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. $\square$

9.6 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.

10 The π-Sylow Theorems

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

10.1 Definition (a) G is called π-*separable*, 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 each of whose factors is a solvable π-groups or an arbitrary π'-groups.

10.2 Remark (a) G is π-separable if and only if G is π'-separable.

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

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

(d) Subgroups and factor groups of π-separable (resp. π-solvable) groups are again π-separable (resp. π-solvable).

(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.

(f) One has: G is solvable $\iff$ G is π-solvable for all π. In fact, if G is solvable then, by Theorem 9.3 G has a normal series whose factors are p-groups. 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.

10.3 Theorem (π-Sylow Theorem, Ph. Hall 1928) (a) *If G is π-separable, 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-separable, 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 10.2(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 10.2(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 10.2(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 10.2(e). Therefore, by Schur-Zassenhaus, there exists $x \in UN$ such that $U = xVx^{-1} = x(UN\cap gHg^{-1})x^{-1} \leqslant (xg)H(xg)^{-1}$. □

10.4 Remark By the Odd-Order-Theorem of Feit-Thompson, it would be enough to require G to be π-separable in Theorem 10.3(b) and (c).

10.5 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 10.3 and Remark 10.2(f). □

10.6 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). $\square$

10.7 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 has a normal p-subgroup $N > 1$, for some prime p by Theorem 9.3. 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 10.6, we have $H_1 H_2 = G$ 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. □

10.8 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. We will use Burnside's Theorem in order to prove the following Theorem.

10.9 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 H_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 10.6(d), $[G : U_{ij}] = p_i^{e_i}p_j^{e_j}$ and $[H_i : U_{ij}] = p_j^{e_i}$. Therefore, each H_i satisfies the hypothesis of the theorem with $r-1$ prime divisors. By induction, each H_i is solvable. By Lemma 10.7, G is solvable. □

10.10 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) ⇒ (ii): This follows from the π-Sylow Theorem.
(ii) ⇒ (iii): This is trivial.
(iii) ⇒ (i): This follows from Theorem 10.9. □

10.11 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 The assertion is clear for $r = 0$ and $r = 1$. If $r = 2$, by Lemma 10.6(d) and (b) we have $P_1 P_2 = G = P_2 P_1$. From now on we assume that $r \geqslant 3$. For every $\pi \subseteq \{p_1, \ldots, p_r\}$, 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 10.6(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 $P_i P_j = G_{ij} = P_j P_i$. □

10.12 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.

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

Proof The equalities $P_i P_j = P_j P_i$ for $i, j \in \{1, \ldots, r\}$ imply by repeated use of Lemma 10.6(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 $\tilde{\pi} := \pi \smallsetminus \{p_{i_0}\}$. 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 10.6(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. □

10.14 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 10.11, (i) implies (ii). Moreover, by Proposition 10.13, (ii) implies (iii). Finally, by Corollary 10.10, (iii) implies (i). ∎

10.15 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

$$\mathcal{S} \underset{\psi}{\overset{\varphi}{\rightleftarrows}} \mathcal{K}$$
$$(P_1, \dots, P_r) \mapsto (\prod_{i \neq 1} P_i, \dots, \prod_{i \neq r} P_i)$$
$$(\bigcap_{i \neq 1} K_i, \dots, \bigcap_{i \neq r} K_i) \leftarrow\!\shortmid (K_1, \dots, K_r)$$

are well-defined inverse bijections. In fact, by Proposition 10.13, φ is well-defined, and by the arguments in the proof of Theorem 10.11, 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.

10.16 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 $i \in \{1, \dots, r\}$ 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 $[G : N_G(K_i)]$, $i = 1, \dots, r$, are pairwise coprime, repeated application of Lemma 10.6(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 10.15, since the maps φ and ψ are inverse isomorphisms of G-sets. $\square$

10.17 Theorem (Hall-Higman 1.2.3) *Let G be a π-separable group and assume that $\mathrm{O}_{\pi'}(G) = 1$. Then $C_G(\mathrm{O}_\pi(G)) \leqslant \mathrm{O}_\pi(G)$.*

Proof We set $C := C_G(\mathrm{O}_\pi(G))$ and $B := C \cap \mathrm{O}_\pi(G)$. It suffices to show that $B = C$. We assume that $B < C$ and will derive a contradiction. Note that B and C are normal in G and that B is a π-group. Since C/B is a non-trivial π-separable group, it has a non-trivial characteristic subgroup K/B which is a π-group or a π'-group. Therefore $K/B \trianglelefteq G/B$ and $K \trianglelefteq G$. First we consider the case that K/B is a π-group. Since B is a π-group, also K is a π-group. Since $K \trianglelefteq G$, we obtain $K \leqslant \mathrm{O}_\pi(G)$ and $K \leqslant \mathrm{O}_\pi(G) \cap C = B$, in contradiction to $K/B > 1$. Next consider the case that K/B is a π'-group. Then, by Schur-Zassenhaus, the normal Hall π-subgroup B of K has a complement H, and since $K/B > 1$, we have $H > 1$. We have $H \leqslant C = C_G(\mathrm{O}_\pi(G)) \leqslant C_G(B)$. Thus, B centralizes H. Since $K = BH$, this implies that $H \trianglelefteq K$. Thurs $1 < H \leqslant \mathrm{O}_{\pi'}(K) \trianglelefteq G$. This is a contradiction to the hypothesis $\mathrm{O}_{\pi'}(G) = 1$. $\square$

10.18 Definition For a π-separable group G we define its *π-length* as the minimum number of factors that are π-groups in any normal series of G in which each factor is either a π-group or a π'-group. For example G has π-length 0 if and only if G is a π'-group. And, G has π-length 1 if and only if G has a normal series $1 = G_0 \leqslant G_1 < G_2 \leqslant G_3 = G$ such that G_1 is a π'-group, G_2/G_1 is a non-trivial π-group and G_3/G_2 is a π'-group.

10.19 Theorem *Let G be a π-separable group and suppose that a Hall π-subgroup of G is abelian. Then the π-length of G is at most* 1.

Proof Set $\overline{G} := G/\mathrm{O}_{\pi'}(G)$. Then $\mathrm{O}_{\pi'}(\overline{G}) = 1$. Let H be an abelian Hall π-subgroup of G. Then $\overline{H} = H\mathrm{O}_{\pi'}(G)/\mathrm{O}_{\pi'}(G)$ is a Hall π-subgroup of $\overline{G}$, and it contains every normal π-subgroup of $\overline{G}$. In particular, it contains $\mathrm{O}_\pi(\overline{G})$. Since $\overline{H}$ is abelian, we have $\overline{H} \leqslant C_{\overline{G}}(\mathrm{O}_\pi(\overline{G})) \leqslant \mathrm{O}_\pi(\overline{G})$, where the last containment follows from Hall-Higman. This implies $\overline{H} = \mathrm{O}_\pi(\overline{G})$ and $\overline{H} \trianglelefteq \overline{G}$. This shows that $1 \leqslant \mathrm{O}_{\pi'}(G) \leqslant H\mathrm{O}_{\pi'}(G) \leqslant G$ is a normal sequence whose first and third factor is a π'-group and whose second factor is a π-group. $\square$

11 Coprime Action

Throughout this section let G and A be finite groups. We assume that A acts by group automorphisms on G. We denote this action by $(a,g) \mapsto {}^a g$. The resulting semi-direct product will be denoted by $\Gamma := G \rtimes A$. Recall that $(g,a)(h,b) = (g\,{}^a h, ab)$ for $g,h \in G$ and $a,b \in A$. We will view G and S as subgroups of Γ via the usual embeddings and then have $\Gamma = GA = AG$ with $A \cap G = 1$. Recall that

$$C_A(G) = \{a \in A \mid {}^a g = g \text{ for all } g \in G\} \trianglelefteq A$$

denotes the kernel of the action of A on G and

$$C_G(A) = \{g \in G \mid {}^a g = g \text{ for all } a \in A\} \leqslant G$$

denotes the A-fixed points of G, previously also denoted by G^A.

11.1 Remark (a) We will often consider a set X on which A and G acts. We will denote these actions by $(a,x) \mapsto a \cdot x$ and $(g,x) \mapsto g \cdot x$. It is easy to verify that the map

$$\Gamma \times X \to X\,, \quad (ga, x) \mapsto g \cdot (a \cdot x)\,,$$

defines an action of Γ on X if and only if the the actions of A and G on X are compatible in the following sense:

$$a \cdot (g \cdot x) = {}^a g \cdot (a \cdot x) \tag{11.1.a}$$

for $x \in X$, $a \in A$ and $g \in G$.

(b) Assume that the compatibility condition (11.1.a) is satisfied. We will denote the A-fixed points of X by

$$X^A := \{x \in X \mid {}^a x = x \text{ for all } a \in A\}\,.$$

It is easy to see that X^A is stable under the action of $C_G(A) = G^A$.

11.2 Lemma (Glauberman) *Assume that G and A act on a set X such that (11.1.a) is satisfied. Moreover assume that* $\gcd(|G|,|A|) = 1$, *that G acts transitively on X and that G or A is solvable. Then the following hold:*

(a) *The set of A-fixed points X^A is non-empty.*

(b) *The action of G^A on X^A is transitive.*

Proof (a) Let $x \in X$ and set $U = \Gamma_x$ denote the stabilizer of x in Γ. We claim that $GU = UG = \Gamma$. In fact, if $\gamma \in \Gamma$ then, by the transitivity of the action of G on X there exists $g \in G$ such that $\gamma \cdot x = g \cdot x$. Thus, $g^{-1}\gamma \in U$ and the claim is proved. Since

$$U/U \cap G \cong GU/G = \Gamma/G \cong A\,,$$

$U \cap G$ is a normal Hall subgroup of U. By Schur-Zassenhaus, $U \cap G$ has a complement H in U. Then $|H| = [U : U \cap G] = |A|$ and H is also a complement of G in Γ. Again by Schur-Zassenhaus, A is conjugate to H in Γ and there exists $\gamma \in \Gamma$ such that $A = {}^{\gamma}H$. Since H stabilizes x, A stabilizes $\gamma \cdot x$ and $\gamma \cdot x \in X^A$.

(b) Let x and y be arbitrary elements in X^A. Set $M := \{g \in G \mid g{\cdot}x = y\}$. Since G acts transitively on X, the subset M of G is non-empty. Moreover, set $H := G_y$, the stabilizer of y in G. Then H acts by left multiplication on M. Also, M is A-stable, since ${}^{a}m \cdot x = {}^{a}m \cdot (a \cdot x) = a \cdot (m \cdot x) = a \cdot y = y$. Therefore, M is a left A-set and a left H-set and $\gcd(|H|,|A|) = 1$. We want to apply Part (a) to this situation. The actions of A and H on M satisfy (11.1.a), since ${}^{a}(hm) = {}^{a}h\,{}^{a}m$ for all $a \in A$, $h \in H$ and $m \in M$ (because A acts on G by group automorphisms). Finally, H acts transitively on M, since for $m, n \in M$ we have $m \cdot x = y = n \cdot x$ and therefore, $mn^{-1} \in G_y = H$ which implies that $m = hn$ for some $h \in H$. Now Part (a) implies that there exists an A-fixed point on M, i.e., an element $m \in M$ which is also in G^A. □

Note that, since A acts on G via group automorphisms, A also acts on the set of subgroups of G, and also on the set of subgroups of G of a fixed order, by ${}^{a}H := \{\,{}^{a}h \mid h \in H\}$ for $a \in A$ and $H \leqslant G$. In particular, A acts on $\mathrm{Syl}_p(G)$ for every prime p of G. We say that H is A-invariant if ${}^{a}H = H$ for all $a \in A$.

11.3 Theorem *Assume that* $\gcd(G,A) = 1$ *and that G or A is solvable. Moreover, let p be a prime. Then the following hold:*

(a) *There exists an A-invariant Sylow p-subgroup of G.*

(b) *Any two A-invariant Sylow p-subgroups of G are conjugate by an element in G^A.*

(c) *Every A-invariant p-subgroup of G is contained in some A-invariant Sylow p-subgroup of G.*

Proof Parts (a) and (b) follow immediately from Lemma 11.2. In fact, A and G act on $X := \mathrm{Syl}_p(G)$, G acts transitively on X, and the compatibility condition (11.1.a) is satisfied: ${}^a g \cdot (a \cdot P) = {}^{{}^a g}({}^a P) = {}^a({}^g P) = a \cdot (g \cdot P)$, for all $a \in A$, $g \in G$ and $P \in \mathrm{Syl}_p(G)$.

(c) It suffices to show that every maximal A-invariant p-subgroup P of G is a Sylow p-subgroup of G. Set $N := N_G(P)$ and note that with P also N is A-invariant. By Part (a) (applied to N instead of G), we may choose an A-invariant Sylow p-subgroup S of N. Since P is normal in N, we have $P \leqslant S$. Since P was a maximal A-invariant p-subgroup of G, we have $P = S$ and P is a Sylow p-subgroup of N. But this implies that P is a Sylow p-subgroup of G. In fact assume this is not the case; then P is properly contained in some Sylow p-subgroup T of G and $Q := N_T(P) > P$, since T is nilpotent. Thus, $Q \leqslant N_G(P)$, contradicting the fact that P is a Sylow p-subgroup of N. ◻

Since A acts on G by automorphisms, we have for every $a \in A$ and $g, h \in G$: g and h are conjugate in G if and only if ${}^a g$ and ${}^a h$ are conjugate in G. This implies that for every conjugacy class K of G the subset ${}^a K := \{ {}^a g \mid g \in K\}$ is again a conjugacy class of G. Thus, A acts on the set $\mathrm{cl}(G)$ of conjugacy classes of G. If $K \in \mathrm{cl}(G)^A$, we also say that K is A-invariant.

11.4 Theorem *Assume that* $\gcd(|G|, |A|) = 1$ *and that A or G is solvable. Then the map*

$$\mathrm{cl}(G)^A \to \mathrm{cl}(G^A)\,, \quad K \mapsto K \cap G^A\,,$$

is a well-defined bijection.

Proof Let $K \in \mathrm{cl}(G)^A$. We first show that $K \cap G^A$ is a conjugacy class of G^A. We will apply Glauberman's Lemma 11.2 to the set $X = K$ on which G acts transitively by conjugation and on which A acts, since K is A-invariant. It is straightforward to verify that the compatibility condition (11.1.a) holds: For $a \in A$, $g \in G$ and $x \in K$, the left hand side equals ${}^a(gxg^{-1}) = {}^a g\, {}^a x ({}^a g)^{-1}$ and the last expression equals the right hand side in (11.1.a). By Glauberman's Lemma, $K^A = K \cap G^A$ is not empty and it is a single orbit under the G^A-conjugation action. Therefore, $K \cap G^A \in \mathrm{cl}(G^A)$.

Next we show that the map in the theorem is surjective. Let $L \in \mathrm{cl}(G^A)$ and let $x \in L$. Let $K \in \mathrm{cl}(G)$ denote the conjugacy class of x. Then K is A-invariant, since it contains the A-fixed point x. By the previous paragraph, $K \cap G^A$ is a single conjugacy class of G^A. But since it contains x, it is equal to L.

Finally, we show that the map in the theorem is injective. Assume that K_1 and K_2 are A-invariant conjugacy classes of G with $K_1 \cap G^A = K_2 \cap G^A$. By the first part of the proof, this latter is a non-epmty set. This implies that K_1 and K_2 have non-empty intersection. Therefore, $K_1 = K_2$. $\square$

Since A acts on G, it acts on the set of subsets of G via ${}^aY = \{ {}^ay \mid y \in Y\}$ for $a \in A$ and $Y \subseteq G$. Since A acts on G via group automorphisms, it also acts on the set of subgroups. We say that a subset Y of G is *A-invariant* it it is a fixed point under this action, i.e., if ${}^ay \in Y$ for all $a \in A$ and $y \in Y$. In this case, A also acts on Y, and if Y is a subgroup of G then A acts on Y via group automorphisms. If the subgroup Y of G is A-stable then A also acts on the set G/Y of left cosets of Y and on the set $Y\backslash G$ of right cosets of Y.

11.5 Theorem *Assume that $H \leqslant G$ is an A-invariant subgroup of G, that $\gcd(|A|, |H|) = 1$ and that A or H is solvable. Then, the A-invariant left (or right) cosets of H are precisely those that contain an A-fixed point.*

Proof Clearly, if a coset contains an A-fixed point g then it is equal to gH (or Hg) and it is A-invariant. Conversely, assume that the coset gH is A-invariant (right cosets can be treated similarly). We can consider $X := gH$ as a left A-set and also as a left H-set via $h \cdot (gh') := gh'h^{-1}$, for $h, h' \in H$. Note that H acts transitively on X. We verify that the compatibility condition (11.1.a) is satisfied. For $h' \in H$, $a \in A$ and $x \in X$, its left hand side equals $a \cdot (h \cdot gh') = {}^a gh'h^{-1} = {}^a gh'({}^ah)^{-1}$ and the last expression is equal to ${}^ah \cdot (a \cdot gh')$. By Glauberman's Lemma 11.2 X has an A-fixed point. This completes the proof. $\square$

If N is an A invariant normal subgroup of G then A acts on G/N via group automorphisms by ${}^a gN = {}^ag\,{}^aN = {}^agN$, for $a \in A$ and $g \in G$.

11.6 Corollary *Let N be an A-invariant normal subgroup of G and assume that $\gcd(|A|, |N|) = 1$ and that A or N is solvable. Then $(G/N)^A = G^AN/N$.*

Proof This follows immediately from Theorem11.5, since $(G/N)^A$ is the set of A-invariant cosets of N and $G^A N/N$ is the set of cosets of N which contain an A-fixed point. ∎

Since the Frattini subgroup $\Phi(G)$ is characteristic in G, it is an A-stable normal subgroup of G and the action of A on G induces an action of A on $G/\Phi(G)$ via group automorphisms.

11.7 Corollary *Assume that* $\gcd(|A|, |\Phi(G)|) = 1$ *and that A acts trivially on $G/\Phi(G)$. Then A acts trivially on G.*

Proof It suffices to show that for every element $a \in A$ the cyclic subgroup $B := \langle a \rangle$ of A acts trivially on G. Note that with A also B acts trivially on $G/\Phi(G)$ and since B is solvable, we can apply Corollary 11.6 to G, $\Phi(G)$ and B to obtain $G^B\Phi(G)/\Phi(G) = (G/\Phi(G))^B = G/\Phi(G)$. The correspondence theorem implies $G^B\Phi(G) = G$ and Lemma 2.3 implies that $G^B = G$. Therefore, B acts trivially on G. ∎

11.8 Corollary *Assume that* $\gcd(|A|, |\Phi(G)|) = 1$ *and that the action of A on G is faithful. Then the action of A on $G/\Phi(G)$ is faithful.*

Proof Let B denote the kernel of the action of A on $G/\Phi(G)$. Then Corollary 11.7 implies that B acts trivailly on G. But since A acts faithfully on G we obtain $B = 1$. But this means that A acts faithfully on $G/\Phi(G)$. ∎

12 Commutators

Throughout this section we fix a group G.

12.1 Definition (a) For $x, y \in G$ we define their *commutator* by $[x, y] := xyx^{-1}y^{-1}$. For $n \geqslant 3$ and elements $x_1, \ldots, x_n$ in G we define their commutator recursively by

$$[x_1, \ldots, x_n] := [x_1, [x_2, \ldots, x_n]]\,.$$

(b) For subgroups X and Y of G we define their commutator $[X, Y]$ as the subgroup generated by all commutators $[x, y]$ for $x \in X$ and $y \in Y$. For $n \geqslant 3$ and subgroups $X_1, \ldots, X_n$ of G we define their commutator recursively by

$$[X_1, \ldots, X_n] := [X_1, [X_2, \ldots, X_n]]\,.$$

Warning: In general, $[X_1, \ldots, X_n]$ is not generated by the elements $[x_1, \ldots, x_n]$ with $x_i \in X_i$ for $i = 1, \ldots, n$.

12.2 Proposition *Let x, y and z be elements of G, let X and Y be subgroups of G and let N be a normal subgroup of G.*

(a) *One has $[y, x] = [x, y]^{-1}$ and $[X, Y] = [Y, X]$.*

(b) *One has $[x, yz] = [x, y] \cdot {}^{y}[x, z]$.*

(c) *One has $[X, Y] \trianglelefteq \langle X, Y\rangle$.*

(d) *If $f\colon G \to H$ is a group homomorphism then $f([x, y]) = [f(x), f(y)]$ and $f([X, Y]) = [f(X), f(Y)]$.*

(e) *One has $[xN, yN] = [x, y]N$ and $[X, Y]N/N = [XN/N, YN/N]$ in G/N.*

(f) *One has $[X, Y] \leqslant Y$ if and only if $X \leqslant N_G(Y)$.*

Proof (a) $[x, y][y, x] = xyx^{-1}y^{-1}yxy^{-1}x^{-1} = 1$. By definition, $[X, Y]$ is generated by the elements $[x, y]$ with $x \in X$ and $y \in Y$, and $[Y, X]$ is generated by their inverses. Therefore, $[X, Y] = [Y, X]$.

(b) We have $[x, y]\cdot {}^{y}[x, z] = (xyx^{-1}y^{-1})(yxzx^{-1}z^{-1}y^{-1}) = xyzx^{-1}z^{-1}y^{-1} = [x, yz]$.

(c) For $x \in X$ and $y, y' \in Y$, Part (a) yields $[x, yy'] = [x, y] \cdot {}^{y}[x, y']$, and therefore ${}^{y}[x, y'] = [x, y]^{-1} \cdot [x, yy'] \in [X, Y]$. This shows that Y normalizes $[X, Y]$. For the same reason, X normalizes $[Y, X]$. But $[Y, X] = [X, Y]$, by Part (a). Therefore, the group $\langle X, Y\rangle$ normalizes $[X, Y]$. Obviously, $[X, Y] \leqslant \langle X, Y\rangle$.

(d) We have $f([x,y]) = f(xyx^{-1}y^{-1}) = f(x)f(y)f(x)^{-1}f(y)^{-1} = [f(x), f(y)]$. Since $[X,Y]$ is generated by the elements $[x,y]$ with $x \in X$ and $y \in Y$, the group $f([X,Y])$ is generated by the elements $f([x,y]) = [f(x), f(y)]$ with $x \in X$ and $y \in Y$. Thus, $f([X,Y]) = [f(X), f(Y)]$.

(e) This follows immediately from part (e) applied to the natural epimorphism $f\colon G \to G/N$, $g \mapsto gN$.

(f) For $x \in X$ and $y \in Y$ one has $[x,y] = {}^{x}y \cdot y^{-1}$ and therefore ${}^{x}y = [x,y] \cdot y$. This shows that $[x,y] \in Y$ if and only if ${}^{x}y \in Y$ and the result follows. $\square$

12.3 Lemma *Let A be an abelian normal subgroup of G and suppose that G/A is cyclic. Then $G' = [G,A] \leqslant A$ and*

$$G' \cong A/(A \cap Z(G))\,.$$

In particular, if A is finite then G' is finite and $|A| = |G'| \cdot |A \cap Z(G)|$.

Proof Let $g \in G$ be such that $G/A = \langle gA \rangle$. Since A is normal in G, we have $[G,A] \leqslant A$ and we can define the function $\theta\colon A \to A$, $a \mapsto [g,a]$. By Proposition 12.2(b), and since A is abelian, we have $[g,ab] = [g,a][g,b]$ for all $a,b \in A$. Thus, θ is a homomorphism. Moreover, $\ker(\theta) = C_A(g) = C_A(G) = A \cap Z(G)$, and $\theta(A) \leqslant [G,A] \leqslant G'$. We will show that $G' \leqslant \theta(A)$ and all statements in the lemma will follow. To that end it suffices to show that $\theta(A)$ is normal in G and that $G/\theta(A)$ is abelian. Since $\theta(A) \leqslant A$ and A is abelian, $\theta(A)$ is normalized by A. Moreover, for $a \in A$ we have ${}^{g}\theta(a) = {}^{g}[g,a] = [{}^{g}g, {}^{g}a] = [g, {}^{g}a] = \theta({}^{g}a) \in \theta(A)$. Therefore, $\theta(A)$ is normal in G. Finally, set $\overline{G} := G/\theta(A)$. Note that $\overline{G}$ is generated by $\overline{g}$ and the elements $\overline{a}$ for $a \in A$. In order to show that $\overline{G}$ is abelian it suffices to show that $[\overline{g}, \overline{a}] = \overline{1}$. But $[\overline{g}, \overline{a}] = \overline{[g,a]} = \overline{\theta(a)} = \overline{1}$. $\square$

12.4 Lemma *For $x,y,z \in G$ one has the* Hall-Witt identity

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

Proof Straightforward computation. $\square$

12.5 Lemma (3 subgroup lemma) *Let X, Y and Z be subgroups of G. If $[X,Y,Z] = 1$ and $[Y,Z,X] = 1$ then $[Z,X,Y] = 1$.*

Proof It suffices to show that $[X, Y] \in C_G(Z)$. Since $C_G(Z)$ is a subgroup of G, it suffices to show that $[x, y] \in C_G(Z)$ for all $x \in X$ and $y \in Y$. For this it suffices to show that $[z, x, y] = 1$ for all $x \in X$, $y \in Y$ and $z \in Z$. This follows now from the hypothesis and the Hall-Witt identity. □

12.6 Corollary (3 subgroup corollary) *Let N be a normal subgroup of G and let X, Y, Z be subgroups of G. If $[X, Y, Z] \leqslant N$ and $[Y, Z, X] \in N$ then $[Z, X, Y] \in N$.*

Proof This follows immediately from Proposition 12.2(e) and the 3 subgroup lemma applied to G/N. □

12.7 Definition We recalibrate the lower central series of a group by setting $G^1 := G$, $G^2 := [G, G]$ and $G^n := [G, G, \ldots, G]$ with n entries G. Note that with the conventions in [P] we have $G^n = Z_{n-1}(G)$. Recall that G^n is characteristic in G for all $n \in \mathbb{N}$. We call any subgroup of n-fold commutators of copies of G a *weight n commutator subgroup* of G. For instance, $[[[G, G], G], [[G, G], [[G, G], G]]]$ is a weight 8 commutator subgroup of G.

12.8 Theorem *For any $i, j \in \mathbb{N}$ one has $[G^i, G^j] \leqslant G^{i+j}$.*

Proof We proceed by induction on i. If $i = 1$ then $[G^i, G^j] = [G, G^j] = G^{j+1}$ by definition. Now assume that $i > 1$. Then we can write $G^i = [G, G^{i-1}]$ and have $[G^i, G^j] = [G^j, G^i] = [G^j, G, G^{i-1}]$. By the 3 subgroup corollary it suffices to show that $[G, G^{i-1}], G^j] \leqslant G^{i+j}$ and $[G^{i-1}, G^j, G] \leqslant G^{i+j}$. But, by induction, we have

$$[G, G^{i-1}, G^j] = [G, [G^{i-1}, G^j]] \leqslant [G, G^{i+j-1}]] = G^{i+j}$$

and

$$[G^{i-1}, G^j, G] = [G^{i-1}, [G^j, G]] = [G^{i-1}, [G, G^j]] = [G^{i-1}, G^{j+1}] \leqslant G^{i+j}$$

and the proof is complete. □

12.9 Corollary *Let $n \in \mathbb{N}$. Any weight n commutator subgroup of G is contained in G^n.*

Proof We proceed by induction on n. For $n = 1$ and $n = 2$ the statement is obviously true. For $n > 2$ every weight n commutator subgroup of G is of the form $[X, Y]$ where X is a weight i commutator subgroup of G and Y is a weight j commutator subgroup of G for positive integers i and j with $i+j = n$. By induction and by Theorem 12.8, we obtain $[X, Y] \leqslant [G^i, G^j] \leqslant G^{i+j} = G^n$ and the proof is complete. □

12.10 Corollary *For any $n \in \mathbb{N}_0$ one has $G^{(n)} \leqslant G^{2^n}$.*

Proof We proceed by induction on n. For $n = 0$ we have $G^{(0)} = G = G^1 = G^{2^0}$. For $n > 0$ we have $G^{(n)} = [G^{(n-1)}, G^{(n-1)}] \leqslant [G^{2^{n-1}}, G^{2^{n-1}}] \leqslant G^{2^{n-1}+2^{n-1}} = G^{2^n}$ by induction and Corollary 12.9. □

For the rest of this section let A denote a group and assume that A acts on G via automorphisms. As before we view A and G as subgroups of the resulting semidirect product Γ and note that inside Γ the conjugation action of A on G coincides with the original action of A on G.

12.11 Remark (a) A subgroup H of G is A-invariant and normal in G if and only if it is normal in Γ. In this case $[A, H] \leqslant H$, since A normalizes H, and moreover, $[A, H]$ is again normal in AH. In fact, for $a, b \in A$ and $h, k \in H$ we have ${}^a[b, h] = [{}^ab, {}^ah] \in [A, H]$ (showing that A normalizes $[A, H]$) and $[a, hk] = [a, h] \cdot {}^h[a, k]$ (showing that ${}^h[a, k] \in [A, H]$ and therefore that also H normalizes $[A, H]$). In particular, $[A, G]$ is an A-invariant normal subgroup of G. Iterating this process, one obtains a sequence

$$G \trianglerighteq [A, G] \trianglerighteq [A, A, G] \trianglerighteq [A, A, A, G] \trianglerighteq \cdots$$

of A invariant subgroups of G. In general the subgroups in this sequence are not normal in G. The next lemma will show that the induced A-action on each of the factor groups is trivial.

(b) If H is an A-invariant subgroup of G then the action of A on G induces an action of A on the set of left cosets, G/H, and also on the set of right cosets, $H\backslash G$, as already explained in the paragraph preceding Theorem 11.5. Moreover, if H is an A-invariant and normal subgroup of G, then the action of A on G induces an action of A on the group G/H via automorphisms.

12.12 Lemma *The subgroup $[A, G]$ of G is A-invariant and normal in G and the induced action of A on $G/[A, G]$ is trivial. Conversely, assume that*

N is a normal A-invariant normal subgroup of G such that the induced action of A on G/N is trivial. Then $[A, G] \leqslant N$.

Proof By Remark 12.11(a), we already know that $[A, G]$ is an A-invariant and normal subgroup of G. Moreover, if N is any A-invariant normal subgroup of G then one has:

$$\begin{aligned} A \text{ acts trivially on } G/N &\iff {}^{a}(Ng) = Ng \text{ for all } g \in G \text{ and all } a \in A \\ &\iff N \cdot {}^{a}g = Ng \text{ for all } g \in G \text{ and all } a \in A \\ &\iff {}^{a}gg^{-1} \in N \text{ for all } g \in G \text{ and all } a \in A \\ &\iff [a, g] \in N \text{ for all } g \in G \text{ and all } a \in A \\ &\iff [A, G] \leqslant N. \end{aligned}$$

This completes the proof. □

12.13 Corollary *For any subgroup $H \leqslant G$ the following are equivalent:*
(i) *Every left coset of H in G is A-invariant.*
(ii) *Every right coset of H in G is A-invariant.*
(iii) $[A, G] \leqslant H$.

Proof (i) $\iff$ (ii): If X is an A-stable subset of G then also $X^{-1} := \{x^{-1} \mid x \in X\}$ is A-stable. But $(gH)^{-1} = Hg^{-1}$ for all $g \in G$.

(ii)$\Rightarrow$(iii): The hypothesis implies in particular that H is A-invariant. Further, for every $a \in A$ and $g \in G$, we have $Hg = {}^{a}(Hg) = {}^{a}H\,{}^{a}g = H\,{}^{a}g$. This implies $[a, g] = {}^{a}gg^{-1} \in H$. Since a and g were arbitrary, we obtain $[A, G] \leqslant H$.

(iii)$\Rightarrow$(i): Every left coset of H in G is a union of left cosets of $[A, G]$ in G. By Lemma 12.12, each coset of $[A, G]$ in G is A-invariant (since A acts trivially on $G/[A, G]$). Thus, every left coset of H is A-invariant. □

For $n \in \mathbb{N}$ we set $[A, \ldots, A, G]_n := [A, \ldots, A, G]$ where the last expression contains n copies of A.

12.14 Theorem *Let $n \in \mathbb{N}$ and assume that $[A, \ldots, A, G]_n = 1$. Then $A^{(n-1)} \leqslant C_A(G)$. In particular, if A acts faithfully on G and $[A, \ldots, A, G]_n = 1$ then $A^{(n-1)} = 1$ and A is solvable.*

Proof It suffices to show the first statement. The second statement follows immediately, since $C_A(G) = 1$ if A acts faithfully on G. We show the first statement by induction on n. If $n = 1$ then $[A, G] = 1$ and A acts trivially on G. Thus $A^{(0)} = A = C_A(G)$. Next we assume that $n > 1$ and that the statement holds for values smaller than n. We want to show that $A^{(n-1)} \leqslant C_A(G)$, or equivalently that $[G, A^{(n-1)}] = 1$. First note that the hypothesis yields $1 = [A, \ldots, A, G]_n = [A, \ldots, A, N]_{n-1}$ for $N := [A, G]$. By induction we obtain $A^{(n-2)} \leqslant C_A(N)$, or equivalently $1 = [A^{(n-2)}, N] = [A^{(n-2)}, A, G]$. In particular, we have $[A^{(n-2)}, A^{(n-2)}, G] = 1$. But then also $[A^{(n-2)}, G, A^{(n-2)}] = [A^{(n-2)}, A^{(n-2)}, G] = 1$. Now the 3 subgroup lemma implies $[G, A^{(n-2)}, A^{(n-2)}] = 1$, and $[G, A^{(n-1)}] = 1$, as desired. $\square$

12.15 Corollary *Assume that A acts faithfully on G and that $[A, A, G] = 1$. Then A is abelian.*

Proof This is immediate from Theorem 12.14 with $n = 2$. $\square$

For any group A we set $A^\infty := \bigcap_{n \in \mathbb{N}} A^n$. If A is finite then the descending sequence A^n of subgroups of A terminates and A^∞ is the final subgroup in this sequence, i.e., $A^\infty = A^k = A^{k+1} = \cdots$ for some $k \in \mathbb{N}$.

12.16 Theorem *Assume that A and G are finite. If $[A, \ldots, A, G]_n = 1$ for some positive integer n then $A^\infty \leqslant C_A(G)$. In particular, if A acts faithfully on G and $[A, \ldots, A, G]_n = 1$ for some positive integer n then A is nilpotent.*

Proof We proceed by induction on $|G|$. If $|G| = 1$ then $C_A(G) = A$ and $A^\infty \leqslant A = C_A(G)$. Now we assume that $|G| > 1$. Then $N := [A, G] < G$, since otherwise $1 = [A, \ldots, A, G]_n = G$. Since $1 = [A, \ldots, A, G]_n = [A, \ldots, A, N]_{n-1}$, we obtain by induction that $C_A(N) \leqslant A^\infty$, or equivalently, $[A^\infty, A, G] = [A^\infty, N] = 1$. We need to show that $[G, A^\infty] = 1$, or equivalently that $[G, A^\infty, A] = 1$, since $A^\infty = A^k = A^{k+1} = [A, A^k] = [A, A^\infty] = [A^\infty, A]$ for some $k \in \mathbb{N}$. By the 3 subgroup lemma it suffices to show that $[A, G, A^\infty] = 1$.

We claim that it suffices to find a normal subgroup C of G with $1 < C \leqslant G^A$. In fact, then we know that A acts on $\overline{G} := G/C$ and $[A, \ldots, A, \overline{G}]_n = \overline{[A, \ldots, A, G]_n} = \overline{1}$ and by induction we obtain $1 = [A^\infty, \overline{G}] = \overline{[A^\infty, G]}$. This implies $[A^\infty, G] \leqslant C$, and since A acts trivially on C we obtain $1 = [A, A^\infty, G] = [A, G, A^\infty]$, and the claim is proved.

We may assume that $[A^\infty, G] > 1$, since otherwise $A^\infty \leqslant C_A(G)$ and we are done. We set $C := C_{[A^\infty,G]}(A)$. Then clearly, $C \leqslant G^A$. To see that $C > 1$, note that $[A, \ldots, A, [A^\infty, G]]_n \leqslant [A, \ldots, A, G] = 1$ but $[A^\infty, G] > 1$. Let $m \in \mathbb{N}_0$ be maximal with $[A, \ldots, A, [A^\infty, G]]_m > 1$, then this subgroup is centralized by A and it is contained in $[A^\infty, G]$. Therefore it is contained in C and $C > 1$.

Finally, we show that C is normal in G. First we claim that $[A^\infty, G]$ centralizes $[A, G]$. From the first paragraph we have $[A^\infty, A, G] = 1$ and therefore $[G, A^\infty, [A, G]] = [G, 1] = 1$. Moreover, $[A, G] \trianglelefteq G$ and therefore $[[A, G], G] = [G, [A, G]] \leqslant [A, G]$. This implies $[A^\infty, [A, G], G] \leqslant [A^\infty, [A, G]] = 1$. The 3 subgroup lemma now implies that $[[A, G], G, A^\infty] = 1$, proving our claim. In particular, since $C \leqslant [A^\infty, G]$, we have $[C, A, G] = 1$. Since A centralizes C, we also have $[G, C, A] = 1$. The 3 subgroup lemma implies $[A, G, C] = 1$ so that $[G, C]$ is centralized by A. Recall that $C \leqslant [A^\infty, G] \trianglelefteq G$ and therefore $[G, C] \leqslant [G, [A^\infty, G]] \leqslant [A^\infty, G]$. But we just saw that A centralizes $[C, G]$. Thus, $[C, G] \leqslant C_{[A^\infty,G]}(A) = C$. This implies that G normalizes C and the proof is complete. $\square$

12.17 Lemma *If $[A, A, G] = 1$ then $[A, G]$ is abelian.*

Proof We have $[G, A, [A, G]] = [G, 1] = 1$. Moreover, $[A, G] \trianglelefteq G$ implies $[A, [A, G], G] = [A, G, [A, G]] \leqslant [A, [A, G]] = 1$. By the 3 subgroup lemma we obtain $[[A, G], [A, G]] = [[A, G], G, A] = 1$ and $[A, G]$ is abelian. $\square$

12.18 Theorem *Assume that A and G are finite and that A is a p-group. If $[A, \ldots, A, G]_n = 1$ for some positive integer n then $[A, G]$ is a p-group.*

Proof We set $N := [A, G]$ and recall from Lemma 12.12 that N is an A-invariant normal subgroup of G and that A acts trivially on G/N. We prove the theorem by induction on $|G|$. If $|G| = 1$ then $N = 1$ and N is a p-group. Now we assume that $|G| > 1$. Since $[A, \ldots, A, G]_n = 1$, we have $N \triangleleft G$. Moreover, $[A, \ldots, A, N]_{n-1} = 1$ and, by induction, $[A, N]$ is a p-group. Again by Lemma 12.12, $[A, N]$ is a normal A-invariant subgroup of N and A acts trivially on $N/[A, N]$. Set $U := \mathrm{O}_p(N)$. Then $U \underset{\text{char}}{\trianglelefteq} N \triangleleft G$ implies that U is A-invariant and normal in G. We have $[A, N] \leqslant U \leqslant N$ and set $\overline{G} := G/U$. Then A acts trivially on $\overline{N}$ since it acts trivially on $N/[A, N]$. Moreover, A acts trivially on G/N and on $\overline{G}/\overline{N}$. We obtain $1 = [A, \overline{N}] =$

$[A, \overline{[A, G]}] = [A, A, \overline{G}]$ and by Lemma 12.17, $\overline{N} = [A, \overline{G}]$ is abelian. Since $\mathrm{O}_p(\overline{N}) = 1$, we can conclude that $\overline{N}$ is a p'-group. Now the hypotheses of Corollary 11.6 are satisfied for the subgroup $\overline{N}$ of $\overline{G}$. Thus, every coset of $\overline{N}$ in $\overline{G}$ contains an A-fixed point. But also $\overline{N}$ consists of A-fixed points. This implies that A acts trivially on $\overline{G}$. This implies $1 = [A, \overline{G}] = \overline{[A, G]} = \overline{N}$ and $N \leqslant U$. Thus, N is a p-group. □

12.19 Theorem *Assume that A and G are finite and that $[A, \ldots, A, G]_n = 1$ for some positive integer n. Then $[A, G]$ is nilpotent.*

Proof We prove the theorem by induction on $|A|$. If $|A| = 1$ then $[A, G] = 1$ is nilpotent. We assume from now on that $|A| > 1$. We claim that every proper subgroup B of A acts trivially on $G/F(G)$, where $F(G)$ is the Fitting subgroup of G. In fact, $[B, \ldots, B, G]_n \leqslant [A, \ldots, A, G]_n = 1$ and the induction hypothesis implies that $[B, G]$ is nilpotent. Since $[B, G] \trianglelefteq G$, we obtain $[B, G] \leqslant F(G)$. Since B acts trivially on $G/[B, G]$, it also acts trivially on $\overline{G} := G/F(G)$.

If A is generated by all its proper subgroups then A acts trivially on $\overline{G}$. This implies that $1 = [A, \overline{G}] = \overline{[A, G]}$ and $[A, G] \leqslant F(G)$. But then $[A, G]$ is nilpotent. Therefore we may assume that A is not generated by its proper subgroups. Since A is generated by its Sylow subgroups for all prime divisors of $|A|$, A must be equal to a Sylow subgroup of A. Thus, A is a p-group and Theorem 12.18 applies to show that $[A, G]$ is a p-group. This completes the proof. □

13 Thompson's $P \times Q$ Lemma

Throughout this section, G and A denote groups and we assume that A acts on G via automorphisms. We view G and A as subgroups in the semidirect product $\Gamma := G \rtimes A$.

13.1 Lemma *Assume that A and G are finite, that* $\gcd(|A|, [A,G]) = 1$, *and that A or $[A,G]$ is solvable. Then $G = A^G \cdot [A,G]$.*

Proof This follows immediately from Lemma 12.12 and Corollary 11.6, since every coset of $[A,G]$ in G is A-invariant and therefore contains an A-fixed point. $\square$

13.2 Lemma *Assume that A and G are finite and that* $\gcd(|A|, [A,G]) = 1$. *Then $[A,A,G] = [A,G]$.*

Proof Clearly $[A,A,G] \leqslant [A,G]$. To show the reverse inclusion it suffices to show that $[a,g] \in [A,A,G]$ for all $a \in A$ and $g \in G$. In a first step we assume that A is solvable. Then, by Lemma 13.1, we can write $g = xc$ with $c \in G^A$ and $x \in [A,G]$. We obtain $[a,g] = [a,xc] = [a,x] \cdot {}^x[a,c] = [a,x] \in [A,A,G]$, since $[a,c] = 1$. In the general case (A not necessarily solvable), we work with $\langle a \rangle$ instead of A and obtain $[a,g] \in [\langle a \rangle, \langle a \rangle, G] \subseteq [A,A,G]$. $\square$

13.3 Corollary *Assume that A and G are finite, that A acts faithfully on G and that $[A,\ldots,A,G]_n = 1$ for some $n \in \mathbb{N}$. Then every prime divisor of $|A|$ also divides $|G|$.*

Proof Let p be a prime divisor of $|A|$ and assume that p does not divide $|G|$. For $P \in \mathrm{Syl}_p(A)$, repeated application of Lemma 13.2 yields $1 = [P,\ldots,P,G]_n = [P,G]$. This implies that P acts trivially on G, in contradiction to A acting faithfully on G. $\square$

13.4 Lemma *Let p be a prime. Assume that A and G are p-groups and that $G > 1$. Then $[A,G] < G$ and $G^A > 1$.*

Proof Note that the semidirect product $\Gamma := G \rtimes A$ is again a p-group. Therefore, there exists $n \geqslant 2$ such that $\Gamma^n = 1$. This implies $[A,\ldots,A,G]_{n-1} \leqslant \Gamma^n = 1$ with $n-1 \geqslant 1$. Since $G > 1$ and $[A,\ldots,A,G]_{n-1} = 1$, we have

$[A,G] < G$ and there exists an integer $i > 0$ such that $C := [A, \ldots, A, G]_{i-1} > 1$ but $[A, \ldots, A, G]_i = 1$. This implies $1 < C \leqslant G^A$. ∎

13.5 Theorem (Thompson's $P \times Q$ Lemma) *Let p be a prime. Assume that $A = P \times Q$, where P is a p-group and Q is a p'-group, and that G is a p-group. If $G^P \leqslant G^Q$ then $G^Q = G$.*

Proof We prove the theorem by induction on $|G|$. If $|G| = 1$ then the clearly Q acts trivially on G. So assume that $|G| > 1$ and set $\Gamma := G \rtimes A$. By Lemma 13.4 we have $[P,G] < G$. Since A normalizes P and G, the subgroup $[P,G] < G$ is A-invariant. Moreover, $[P,G]^P = G^P \cap [P,G] \leqslant G^Q \cap [P,G] = [P,G]^Q$. By induction we obtain that Q acts trivially on $[P,G]$. In other words, $[Q,P,G] = 1$. But also $[G,Q,P] = 1$, since $[Q,P] = 1$. By the 3 subgroup lemma we obtain $[P,G,Q] = 1$ and P acts trivially on $[Q,G]$. But then $[Q,G] = [Q,G]^P = [Q,G] \cap G^P \leqslant [Q,G] \cap G^Q = [Q,G]^Q$, which implies that Q centralizes $[Q,G]$ and that $[Q,Q,G] = 1$. Now, Lemma 13.2 implies that $[Q,Q,G] = [Q,G]$ and the proof is complete. ∎

13.6 Theorem *Let p be a prime, let G be a p-solvable group, let P be a p-subgroup of G, and set $H := N_G(P)$. Then $\mathrm{O}_{p'}(H) \leqslant \mathrm{O}_{p'}(G)$.*

Proof We set $Q := \mathrm{O}_{p'}(H)$ and $N := \mathrm{O}_{p'}(G)$. We first assume that $N = 1$ and need to show that $Q = 1$. Note that both P and Q are normal subgroups of H and that $P \cap Q = 1$. Thus, $A := PQ = P \times Q$ is the internal direct product of P and Q. Moreover, A acts on the p-group $U := \mathrm{O}_p(G) > 1$ by conjugation. We want to show that $C_U(P) \leqslant C_U(Q)$. Note that $C_U(P) = U \cap C_G(P) \leqslant U \cap N_G(P) = U \cap H$ and that $U \cap H$ is a normal p-subgroup of H. Since Q is a normal p'-subgroup of H, $U \cap H$ and Q centralize each other. Therefore $C_U(P)$ and Q centralize each other. In other words, $C_U(P) \leqslant C_G(Q) \cap U = C_U(Q)$, and we can apply Thompson's $P \times Q$ lemma. This yields $[U,Q] = 1$ or $Q \leqslant C_G(U)$. By the Higman-Hall 1.2.3 lemma, we have $C_G(U) \leqslant U$ and therefore $Q \leqslant U$. Since U is a p-group and Q is a p'-group, this implies $Q = 1$ as desired.

Now assume that $N = \mathrm{O}_{p'}(G) > 1$. Then $\overline{G} := G/N$ is p-solvable with $\mathrm{O}_{p'}(\overline{G}) = 1$. We have $N_{\overline{G}}(\overline{P}) = \overline{N_G(P)} = \overline{H}$ (cf. Homework problem), since N is a normal p'-subgroup of G. By the first case applied to $\overline{G}$ we have $\mathrm{O}_{p'}(\overline{H}) = 1$. But $\overline{\mathrm{O}_{p'}(H)} \leqslant \mathrm{O}_{p'}(\overline{H})$ and therefore, $\mathrm{O}_{p'}(H) \leqslant N = \mathrm{O}_{p'}(G)$. This completes the proof. ∎

13.7 Theorem *Assume that A and G are finite, that* $\gcd(|A|, |G|) = 1$, *and that G is abelian. Then $G = G^A \times [A, G]$.*

Proof We already know that $G = G^A \cdot [A, G]$ by Lemma 13.1. Since G is abelian, it suffices to show that $G^A \cap [A, G] = 1$. Let $\theta \colon G \to G$ be defined as

$$\theta(g) := \prod_{a \in A} {}^a g \, .$$

Since G is abelian, this definition does not depend on the order of the product. Also, since G is abelian, θ is a group homomorphism. If $c \in G^A$ then $\theta(c) = c^| A|$. Moreover, for $a \in A$ and $g \in G$ we have $\theta({}^a g) = \prod b \in A \, {}^{ba} g = \theta(g)$ and therefore $\theta([a, g]) = \theta({}^a g)\theta(g^{-1} = \theta(g)\theta(g)^{-1} = 1$. This implies that $[A, G] \leqslant \ker(\theta)$. Now let $x \in G^A \cap [A, G]$. Then $1 = \theta(x) = x^{|A|}$. But since A and G have coprime orders, this implies $x = 1$ and the proof is complete. □

13.8 Corollary *Let p be a prime. Assume that G is an abelian p-group and A is a p'-group. If A fixes every element of order p in G then A acts trivially on G.*

Proof By Fitting's Theorem 13.7 we have $G = G^A \times [A, G]$ and every element of order p in G is already contained in G^A. Therefore, $[A, G]$ is a p-group with no elements of order p. This implies $[A, G] = 1$ and $G^A = 1$. □

Our goal is to show that we can drop the assumption that G is abelian in the previous corollary. The following trick, due to Reinhold Baer, will come in handy.

13.9 Lemma (Baer trick) *Let G be a finite nilpotent group of odd order with $G^3 = 1$ (i.e, $G' \leqslant Z(G)$). There exists a binary operation*

$$G \times G \to G \, , \quad (x, y) \mapsto x + y \, ,$$

with the following properties:

(i) *$(G, +)$ is an abelian group.*

(ii) *If $x, y \in G$ are commuting elements then $x + y = xy$.*

(iii) *The additive order of every element of G is equal to its multiplicative order.*

(iv) $\mathrm{Aut}(G) \leqslant \mathrm{Aut}(G, +)$.

Proof Since G has odd order, there exists $n \in \mathbb{Z}$ with $|G|+1 = 2n$. For $x, y \in G$, we define $x + y := [x,y]^n yx$.

We first show that $x+y = y+x$ for $x, y \in G$. We need to show that $[x,y]^n xy = [y,x]^n xy$, or equivalently that $[x,y]^n = xyx^{-1}y^{-1}$. But this holds, since $2n = |G|+1$.

Next, assume that $x, y \in G$ are commuting elements. Then $x + y = [x,y]^n yx = xy$, since $[x,y] = 1$. This shows (ii).

Since 1 commutes with every x we have $x + 1 = x \cdot 1 = x$. Thus, 1 is an identity element with respect to $+$. Moreover, since x and x^{-1} commute, we have $x + x^{-1} = xx^{-1} = 1$. Next we show associativity of $+$. Note that, since $G' \leqslant Z(G)$, every commutator is central in G, and every triple commutator is trivial. Moreover, for every $x \in G$, the function $G \to G$, $y \mapsto [x,y]$, is a homomorphism. In fact, $[x,yz] = [x,y] \cdot {}^{y}[x,z] = [x,y][x,z]$ for $x, y, z \in G$. Similarly, $[xy,z] = [x,z][y,z]$. We have

$$\begin{aligned} x + (y+z) &= x + [y,z]^n zy = \Big[x, [y,z]^n zy\Big]^n \cdot [y,z]^n zyx \\ &= \Big([x,[y,z]^n][x,z][x,y]\Big)^n [y,z]^n zyx \\ &= \Big([x,[y,z]]^n[x,z][x,y]\Big)^n [y,z]^n zyx \\ &= [x,y]^n[x,z]^n[y,z]^n zyx \end{aligned}$$

and similarly

$$\begin{aligned} (x+y)+z &= [x,y]^n yx + z = \Big[[x,y]^n yx, z\Big]^n \cdot z[x,y]^n yx \\ &= [x,y]^n[x,z]^n[y,z]^n zyx \end{aligned}$$

Thus, $+$ is associative and $(G,+)$ is an abelian group with identity element 1 and $-x = x^{-1}$. This shows (i).

To see (iii), note that (a) implies $n \cdot x = x^n$ for all positive integers n (by induction on n) and that additive and multiplicative identity coincide.

Finally, let $f \in \mathrm{Aut}(G)$. Then

$$\begin{aligned} f(x+y) &= f([x,y]^n yx) = f([x,y])^n f(y)f(x) = [f(x),f(y)]^n f(y)f(x) \\ &= f(x) + f(y) \end{aligned}$$

and (iv) follows. This completes the proof. $\square$

13.10 Theorem *Let p be an odd prime. Assume that G is a p-group and that A is a p'-group. If A fixes every element of order p in G then A acts trivially on G.*

Proof We prove the theorem by induction on $|G|$. If $|G| = 1$ then certainly A acts trivially on G. So assume from now on that $|G| > 1$. By induction, A acts trivially on every A-invariant proper subgroup H of G. In particular, if $[A, G] < G$ then A acts trivially on $[A, G]$ so that $[A, A, G] = 1$. But by Lemma 13.2 we have $[A, G] = [A, A, G] = 1$ and A acts trivially on G. Therefore, we can assume from now on that $[A, G] = G$. Since G is a non-trivial p-group we have $G' < G$. Moreover, since G' is characteristic in G, it is also A-invariant. We obtain, by induction, that $[A, G'] = 1$. In particular we have $[G, A, G'] = 1$. Moreover, since G' is normal in G, we have $[G, G'] \leqslant G'$, which implies $[A, G', G] = [A, G, G'] \leqslant [A, G'] = 1$. By the 3 subgroup lemma, we have $[G', G, A] = 1$. But since we assumed that $[A, G] = G$, we obtain $[G', G] = 1$. In other words, $G' \leqslant Z(G)$. By Lemma 13.9, G carries an abelian group structure $(G, +)$ satisfying conditions (i)–(iv) in the Lemma. By (iv), the action of A on G is also an action on $(G, +)$ via group automorphisms. By (iii), every element of $(G, +)$ of order p is fixed by A. Thus, by Corollary 13.8, A acts trivially on $(G, +)$ and on G. $\square$

13.11 Theorem *Let p be an odd prime. Assume that $A = PQ$, where P is a p-subgroup of A and Q is a normal p'-subgroup of A, and assume that G is a p-group. If $G^P \leqslant G^Q$ then $G^Q = G$.*

Proof First note that, since A normalizes G and Q, the subgroup $[Q, G]$ of G is A invariant.

Our next goal is to prove the theorem in the case that G is abelian. In this case, by Fitting's Theorem, we have $G = G^Q \times [Q, G]$. Assume that $[Q, G] > 1$. Lemma 13.4 implies that $[Q, G]^P > 1$. But then the hypothesis of the theorem implies $[Q, G]^Q \geqslant [Q, G]^P > 1$. This implies $[Q, G] \cap G^Q = 1$, in contradiction to $G = G^Q \times [Q, G]$.

Now we prove the theorem for general G by induction on $|G|$. We can assume that $|G| > 1$. Note that if H is a proper A-invariant subgroup of G then H satisfies the hypothesis of the theorem and, by induction, Q acts trivially on H. We apply this to $[Q, G]$. So, if $[Q, G] < G$ then $[A, Q, G] = 1$. In particular, $[Q, Q, G] = 1$ and by Lemma 13.2 we obtain $[Q, G] = [Q, Q, G] = 1$ and we are done. So we can assume from now on that $[Q, G] =$

G. Consider the proper A-invariant subgroup G' of G. By the above we obtain $[Q, G'] = 1$ and in particular $[G, Q, G'] = 1$ and $[Q, G', G] \leqslant [Q, G'] = 1$. The 3 subgroup lemma implies $[G', Q, G] = 1$ and since $[Q, G] = G$, we obtain $[G', G] = 1$. In other words, $G' \leqslant Z(G)$. Now we can again apply Baer's trick to see that Q acts trivially on G, since we have already proved the theorem in the case that G is abelian. $\square$

14 The Transfer Map

Throughout this section, G denotes a finite group.

14.1 Definition Let H and K be subgroups of G with $H' \leqslant K \trianglelefteq H \leqslant G$ (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 $g = \rho(g)\eta(g)$. The function

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

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

14.2 Proposition *Using the notation of Definition 14.1, 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. $\square$

14.3 Remark Let $H' \leqslant K \trianglelefteq H \leqslant G$ be as in Definition 14.1. 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 $r_1H, \ldots, r_sH$ 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 $i = 1, \ldots, s$. Then

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

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 $i = 1, \ldots, s$, 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 $i = 1, \ldots, s$ (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.

14.4 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.

14.5 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 14.3 we therefore have

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

for all $h \in H$.

14.6 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. □

14.7 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.

14.8 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 14.7. Then $H^{i+1} \leqslant H_i$ for all $i \in \mathbb{N}_0$, where $H^{i+1} = [H, H, \ldots, H]$ with $i+1$ entries equal to H. In fact, $H^1 = H = H_0$ and if $i > 0$, then by induction and Part (a) we have

$$\begin{aligned} H^{i+1} &= [H, H^i] = \langle \{[h,x] \mid h \in H, x \in H^i\} \rangle \\ &\leqslant \langle \{[g,x] \mid g \in G, x \in H^i \text{ such that } [g,x] \in H^i\} \rangle \\ &= \mathrm{Foc}_G(H^i) \leqslant \mathrm{Foc}_G(H_{i-1}) = H_i \,. \end{aligned}$$

In particular, if H is hyperfocal in G then H is nilpotent.

14.9 Theorem *If $H \leqslant G$ is a hyperfocal Hall subgroup of G, then H 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 14.6, 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 10.2(g)) and hyperfocal in N (by Remark 14.8). 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, $H \cap K = H \cap N \cap K = 1$, and finally, by Proposition 14.6, $HK = H(H \cap N)K = HN = G$. □

14.10 Theorem *Let H be a nilpotent Hall subgroup of G. Assume that 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 14.9, it suffices to show that $H_i = H^{i+1}$ 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 14.8(b), we have $H^{i+1} \leqslant H_i$. 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. $\square$

14.11 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 $nAn^{-1} = gy^{-1}Ayg^{-1} = gAg^{-1} = B$. $\square$

14.12 Theorem (Burnside) *Let P be a Sylow p-subgroup of G such that $N_G(P) = C_G(P)$ (in other words that $P \leqslant Z(N_G(P))$). 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 14.11, 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 14.10 implies the assertion. $\square$

14.13 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 14.12 completes the proof. $\square$

14.14 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 14.13 implies that every group of order $2n$, with n odd, has a normal subgroup of order n.

14.15 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 14.13. Again, every Sylow subgroup of K is cyclic, and by induction K is solvable. Therefore, with $G/K \cong P$, also G is solvable. □

14.16 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 14.15. □

14.17 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 14.12 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. □

15 p-Nilpotent Groups

15.1 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.

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

(a) We have

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

(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

$$G \to \prod_{p||G|} G/O_{p'}(G)\,, \quad g \mapsto \Big(gO_{p'}(G)\Big)_{p||G|}\,,$$

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 (Homework).

15.3 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 15.2(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 10.2(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 $N_G(Q) = C_G(Q)R = RC_G(Q)$ (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 14.10. $\square$

15.4 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) If G has an abelian Sylow p-subgroup P then $N_G(P)$ controls the fusion of p-subgroups of G. (Homework)

(c) 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.

References

[P] R. Boltje: Preliminaries; Class Notes Algebra I (Math200), Fall 2008, UCSC.