Group Theory

Dietrich Burde

Lecture Notes 2017

Contents

Introduction

Group theory is a broad subject which arises in many areas of mathematics and physics, and has several different roots. One foundational root of group theory was the quest of solutions of polynomial equations of degree higher than 4. Lagrange introduced permutation groups for the theory of equations, and Galois the groups named after him for the solvability of the equation with radicals. A second root was the study of symmetry groups in geometry. The systematic use of groups in geometry was initiated by Klein's 1872 Erlangen program. Finally, a third root of group theory was number theory. Certain abelian group structures had been implicitly used in number-theoretical work by Gauss, and more explicitly by Kronecker.
Modern group theory nowadays is not just a part of abstract algebra. It has several branches, such as combinatorial group theory, geometric group theory, the theory of finite groups, the theory of discrete groups, transformation groups, Lie groups and algebraic groups, and many more. These lecture notes cover the topics stated in the curriculum for master mathematics at the university of Vienna.

CHAPTER 1

Review of basic notions

1.1. Group axioms

An axiomatic description of groups is given as follows.

DEFINITION 1.1.1. A group G is a non-empty set together with a binary operation $(a, b) \mapsto ab$ from $G \times G \to G$ satisfying the following conditions:

(1) *Associativity.* For all $g, h, k \in G$ we have
$$(gh)k = g(hk).$$
(2) *Existence of a neutral element.* There exists an element $e \in G$ such that
$$eg = g = ge$$
for all $g \in G$.
(3) *Existence of inverses.* For every $g \in G$ there exists an element $g^{-1} \in G$ such that
$$gg^{-1} = e = g^{-1}g.$$

Note that the neutral element is uniquely determined. Indeed, if e' is a second such element, then $e' = ee' = e$. Moreover, by (3), e is the unique element of G such that $ee = e$. Also the inverse element g^{-1} of g is uniquely determined.

REMARK 1.1.2. One can replace the axioms (2) and (3) by weaker ones, namely by (2′) there exists an e such that $ea = a$ for all $a \in G$, and (3′) for each $a \in G$ there exists an $a' \in G$ such that $a'a = e$.

LEMMA 1.1.3. *Let G be a group and $a, b \in G$. Then $(a^{-1})^{-1} = a$ and $(ab)^{-1} = b^{-1}a^{-1}$.*

PROOF. Exercise. □

LEMMA 1.1.4. *In every group the cancellation laws are satisfied,i.e., $gh = gk$ implies that $h = k$, and $hg = kg$ implies that $h = k$. If the group is finite, then the cancellation laws are equivalent with axiom* (3).

PROOF. Suppose that $gh = gk$ for $g, h, k \in G$. Using (3) we have
$$h = g^{-1}gh = g^{-1}gk = k.$$
In the same way, $hg = kg$ implies that $h = k$. Suppose that G is finite. As we have just shown, axiom (3) implies the cancellation laws in general. Assume now that the cancellation laws hold. Then each left multiplication map $L_g \colon x \mapsto gx$ is injective. Since G is finite, it follows that each L_g is also surjective. In particular, e is in the image. This shows axiom (3). □

EXAMPLE 1.1.5. *We start with* 5 *basic examples of groups.*

1. *The group $(\mathbb{Z}, +)$. Usually one writes $g + h$ instead of gh, and $-g$ for g^{-1}. However the group can also be written multiplicatively, and then is denoted by C_∞.*

2. *The group* $(\mathbb{Z}/n\mathbb{Z}, +)$. *It is given by the residue classes* $\{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$ *modulo* n. *Written multiplicatively, it is denoted by* $C_n = \{e, g, g^2, \ldots, g^{n-1}\}$, *where the letter* C *stands for "cyclic".*

3. *The group* $GL_n(F)$ *consists of the invertible* $n \times n$*-matrices with coefficients in* F. *It is called the general linear group of degree* n.

4. *The group* D_n *for* $n \geq 3$ *of rigid motions of the plane preserving a regular* n*-gon, with the operation being composition. It turns out that* D_n *has size* $2n$ *and is given by*

$$D_n = \{e, r, r^2, \ldots, r^{n-1}, s, rs, r^2s, \ldots r^{n-1}s\},$$

where r *is a rotation through* $\frac{2\pi}{n}$, *and* s *a reflection such that* $srs^{-1} = r^{-1}$. *We have* $s^2 = e$, *and* $s, rs, r^2s, \ldots r^{n-1}s$ *are the reflections, and* $e, r, \ldots, r^{n-1}$ *the rotations of the* n*-gon with* $r^n = e$.

5. *The "free" group* F_2 *consisting of all possible words in two distinct letters* a *and* b *and its inverses. Here we consider two words different unless their equality follows from the group axioms.*

Definition 1.1.6. A group G is called *abelian*, if it satisfies the commutativity law, e.g.,

$$gh = hg$$

for all $g, h \in G$.

Note that the groups of 1. and 2. are abelian, but the last three ones are non-abelian. For the dihedral group D_n the elements r and s satisfy $rs = sr^{-1}$. Since $n \geq 3$ we have $r \neq r^{-1}$, because of $r^n = e$. In F_2 the words ab and ba are different.

Lemma 1.1.7. *Let* S *be a non-empty subset of a group* G. *Suppose that the following two properties hold:*

(S1) *For all* $a, b \in S$ *we have* $ab \in S$.
(S2) *For all* $a \in S$ *we have* $a^{-1} \in S$.

Then the composition of G *makes* S *into a group.*

Proof. By (S1) the binary operation on G defines a binary operation on S, which inherits associativity. By assumption S contains at least one element a, its inverse a^{-1}, and the product $e = aa^{-1}$. By (S2) the inverses of elements in S lie in S. □

Definition 1.1.8. A non-empty subset S of a group G satisfying (S1) and (S2) is called a *subgroup* of G.

Example 1.1.9. 1. *The center of a group* G, *defined by*

$$Z(G) = \{g \in G \mid gx = xg \; \forall \, x \in G\},$$

is a subgroup of G.

2. *The intersection of arbitrary many subgroups of* G *is a subgroup of* G.

3. *The subset* $n\mathbb{Z}$ *of* $\mathbb{Z}$ *for an integer* n *is a subgroup of* $\mathbb{Z}$.

Lemma 1.1.10. *For any subset* X *of a group* G, *there is a smallest subgroup of* G *containing* X.

Proof. The intersection S of all subgroups of G containing X is again a subgroup of G containing X, and it is evidently the smallest such group. S contains with X also all finite products of elements of X and their inverses. But the set of such products satisfies (S1) and (S2) and hence is a subgroup containing X. Clearly it equals S. □

DEFINITION 1.1.11. The smallest subgroup of G containing X is denoted by $\langle X\rangle$, and is called the *subgroup generated by* X. We say that X *generates* G if $G = \langle X\rangle$, i.e., if every element of G can be written as a finite product of elements of X and their inverses.

We have $\langle\emptyset\rangle = \{e\}$, which is the *trivial group*. The group generated by a rotation r through $\frac{2\pi}{n}$ is given by $C_n = \langle r\rangle = \{e, r, r^2, \dots, r^{n-1}\}$.

DEFINITION 1.1.12. A group G is said to be *cyclic* if it is generated by a single element.

Note that cyclic groups are abelian, since elements r^k and r^ℓ commute. The groups C_n and C_∞ are cyclic, whereas $GL_n(F)$ for $n > 1$ is not cyclic, because it is not abelian.

1.2. Group homomorphisms

Having introduced our main "objects", we need "morphisms" to relate the objects to each other. As usual morphisms should preserve the structure, and two objects should be considered the same if they have the same structure:

DEFINITION 1.2.1. A map $\varphi\colon G \to H$ is called a *group homomorphism* if it satisfies

$$\varphi(gh) = \varphi(g) \cdot \varphi(h)$$

for all $g, h \in G$. A group homomorphism that is bijective is called a *group isomorphism*. Its inverse is also a group isomorphism. In this case, the groups G and H are called *isomorphic*. We denote this by $G \cong H$.

Note that $\varphi(e_G) = e_H$ for such a group homomorphism and the neutral elements of the two groups, and $\varphi(g^{-1}) = \varphi(g)^{-1}$.

EXAMPLE 1.2.2. *Here are three examples of group homomorphisms.*

1. *Let H be a subgroup of G. Then the inclusion map $H \hookrightarrow G$ is a group homomorphism.*
2. *The map $\varphi\colon \mathbb{Z} \to \mathbb{Z}$, $x \mapsto nx$, for a fixed integer n is a group homomorphism.*
3. *The map $\exp\colon (\mathbb{R}, +) \to (R_{>0}, \cdot)$ is a group isomorphism, its inverse given by the logarithm.*

Recall that the *kernel* of a group homomorphism $\varphi\colon G \to H$ is given by

$$\ker(\varphi) = \{g \in G \mid \varphi(g) = e\},$$

and the *image* of φ is given by

$$\operatorname{im}(\varphi) = \{\varphi(g) \mid g \in G\}.$$

Both are subgroups of G. It is easy to see that a group homomorphism is injective if and only if its kernel is trivial.

DEFINITION 1.2.3. Let X be a set. Then the set of all bijections $X \to X$ forms a group with respect to composition. It is denoted by $\operatorname{Sym}(X)$.

For $X = \{1, 2, \dots, n\}$ the group $\operatorname{Sym}(X)$ is the symmetric group S_n. It is a non-abelian group for $n > 2$.

THEOREM 1.2.4 (Cayley). *For any group G there is a canonical embedding $L\colon G \hookrightarrow \operatorname{Sym}(G)$. In particular, any finite group of order n can be realized as a subgroup of S_n.*

PROOF. Consider the map $L\colon G \to \mathrm{Sym}(G)$ given by $g \mapsto L_g$. We have

$$(L_a \circ L_b)(x) = L_{ab}(x)$$

for all $a, b, x \in G$, and $L_a \in \mathrm{Sym}(G)$ for all $a \in G$, because every L_a is bijective. Indeed, we have $L_e = \mathrm{id}$ and

$$L_a \circ L_{a^{-1}} = \mathrm{id} = L_{a^{-1}} \circ L_a.$$

It follows that L is a group homomorphism. It is injective because the cancellation laws hold. Hence it is an embedding. □

REMARK 1.2.5. The symmetric group S_n has order $n!$. Every finite group G of order n can be embedded in S_n, but often one can embed G in a permutation group of much smaller order. We may define the *degree* of a group G of order n, denoted $d(G)$, to be the least integer d such that G can be embedded in S_d. There is a large literature on the study of $d(G)$. Johnson classified all G of order n such that $d(G) = n$. Except for a family of 2-groups, these groups are precisely the cyclic p-groups. Here a group G is called a *p-group*, if its order is a power of p for a prime p.

An *automorphism* of a group G is a group isomorphism $G \to G$. For example, the conjugation map

$$i_g\colon G \to G, x \mapsto gxg^{-1}$$

is an automorphism of G. We have

$$(gh)x(gh)^{-1} = g(hxh^{-1})g^{-1},$$

for all $g, h \in G$, which says that $i_{gh}(x) = (i_g \circ i_h)(x)$, so that i_g is a bijective group homomorphism, and hence an automorphism.

DEFINITION 1.2.6. Denote by $\mathrm{Aut}(G)$ the set of automorphisms of G. It becomes a group under composition, and it is called the *automorphism group* of G. The subgroup $\mathrm{Inn}(G) = \{i_g \mid g \in G\}$ is called the group of *inner automorphisms*.

Note that $\mathrm{Inn}(G)$ is trivial if and only if G is abelian.

EXAMPLE 1.2.7. *We have* $\mathrm{Aut}(S_3) = \mathrm{Inn}(S_3) \cong S_3$ *and* $\mathrm{Aut}(\mathbb{F}_p^n) = GL_n(\mathbb{F}_p)$*, where the automorphisms of* $G = \mathbb{F}_p^n$ *as a commutative group are just the automorphisms of* G *as a vector space over the finite field* $\mathbb{F}_p$*. For* $n = p = 2$ *we have* $\mathrm{Aut}(\mathbb{F}_2^2) = GL_2(\mathbb{F}_2) \cong S_3$*.*

REMARK 1.2.8. Different groups may have an isomorphic automorphism group, e.g.,

$$\mathrm{Aut}(S_3) \cong S_3 \cong \mathrm{Aut}(C_2 \times C_2),$$

where $C_2 \times C_2$ is the direct product, with componentwise product.

We want to mention a few more groups consisting of bijective transformations.

DEFINITION 1.2.9. Let X be a metric space. The set of all isometries from $X \to X$ forms a group under composition, and is denoted by $\mathrm{Isom}(X)$. It is called the *isometry group* of X.

EXAMPLE 1.2.10. *The isometry group of the Euclidean space* $\mathbb{R}^n$ *is given by*

$$\mathrm{Isom}(\mathbb{R}^n) \cong O_n(\mathbb{R}) \rtimes \mathbb{R}^n,$$

where $O_n(\mathbb{R})$ *denotes the orthogonal group, which is the subgroup of* $GL_n(\mathbb{R})$ *given by all matrices* A *satisfying* $AA^t = I$*.*

Let M be a subset of X. A *symmetry* of M is an isometry of X fixing M. If we embed the n-gon M in $X = \mathbb{R}^2$, then the symmetry group of M is the dihedral group D_n.

DEFINITION 1.2.11. Let $L \mid K$ be a Galois extension of fields. Then the set

$$Gal(L, K) = \{\sigma \in \mathrm{Aut}(L) \mid \sigma_{|K} = \mathrm{id}_K\}$$

of field automorphisms of L fixing K is a group with respect to composition, and is called the *Galois group* of the extension $L \mid K$.

EXAMPLE 1.2.12. *Let $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ and $K = \mathbb{Q}$. Then the extension $L \mid K$ is Galois with Galois group*

$$Gal(L \mid K) \cong C_2 \times C_2.$$

DEFINITION 1.2.13. Let $\pi\colon X \to Y$ be a covering map of topological spaces. Then the set of homeomorphisms $f\colon X \to X$ satisfying $\pi \circ f = \pi$ form a group with respect to composition, the *Deck transformation group.*

EXAMPLE 1.2.14. 1. *The deck transformations for the universal covering $\mathbb{C} \to \mathbb{C}^*$ given by the exponential map is the set of translations of the form $z \mapsto z + 2\pi i k$ for $k \in \mathbb{Z}$. Thus, the group of deck transformations is isomorphic to $\mathbb{Z}$.*

2. *The deck transformations for the covering map $\mathbb{C}^* \to \mathbb{C}^*$ given by the power map $z \mapsto z^n$ are the maps of the form $z \mapsto \omega z$, where ω is any n-th root of unity. As an abstract group, this deck transformation group is isomorphic to $\mathbb{Z}/n\mathbb{Z}$.*

1.3. Cosets and normal subgroups

For a subset S of a group G we let

$$aS = \{as \mid s \in S\},\ Sa = \{sa \mid s \in S\}.$$

DEFINITION 1.3.1. For a subgroup H of a group G the sets of the form aH are called *left cosets* of H, and the sets of the form Ha are called *right cosets* of H.

Because $e \in H$ we have $aH = H$ if and only if $a \in H$.

PROPOSITION 1.3.2. *Let H be a subgroup of G.*

(*a*) *An element $a \in G$ lies in a left coset C of H if and only if $C = aH$.*
(*b*) *Two left cosets are either disjoint or equal.*
(*c*) *We have $aH = bH$ if and only if $a^{-1}b \in H$.*
(*d*) *Any two left cosets have the same number of elements, possibly infinite.*

PROOF. (*a*): If $C = aH$ then of course $a \in aH$. Conversely, if a lies in the left coset bH, then $a = bh$ for some $h \in H$, so that

$$aH = bhH = bH.$$

(*b*): Suppose that the cosets C and C' are not disjoint. Then there is an a in both C and C', so that $C = aH = C'$ by (*a*).

(*c*): If $a^{-1}b \in H$, then $H = a^{-1}bH$, and so $aH = aa^{-1}bH = bH$. Conversely, if $aH = bH$, then $H = a^{-1}bH$, and so $a^{-1}b \in H$.

(*d*): The map $L_{ba^{-1}}\colon aH \to bH$ given by $ah \mapsto bh$ is a bijection. □

DEFINITION 1.3.3. Let H be a subgroup of G. The *index* $(G : H)$ of H in G is the cardinality of the set $\{aH \mid a \in G\}$, i.e., the number of left cosets of H in G.

For the trivial subgroup $H = 1$ we have $(G : 1) = |G|$. We have

$$G = \bigcup_{a \in G} aH,$$

and because two cosets are either equal or disjoint, they form a partition of G.

THEOREM 1.3.4 (Lagrange). *Let G be a finite group. Then*

$$(G : 1) = (G : H)(H : 1).$$

In particular, the order of every subgroup H of G divides the order of G.

PROOF. The left cosets of H in G form a partition of G, and there are $(G : H)$ of them. Each left coset has $(H : 1)$ elements. □

Recall that the order of $g \in G$ is given by $\mathrm{ord}(g) = |\langle g \rangle|$.

COROLLARY 1.3.5. *For each $g \in G$, the order of g divides $|G|$.*

PROOF. Apply Lagrange for the subgroup $H = \langle g \rangle$, and use that $(H : 1) = \mathrm{ord}(g)$. □

COROLLARY 1.3.6. *Every group of prime order p is isomorphic to the cyclic group C_p.*

PROOF. Let G be a group of order p. Then every element has order 1 or p, since these two numbers are the only positive divisors of p. Since G is non-trivial there is an element $g \in G$ of order p. Let $H = \langle g \rangle \subseteq G$ be the cyclic subgroup of G generated by g. Then $|H| = p$ and $H = G = \{e, g, g^2, \ldots g^{p-1}\}$. □

EXAMPLE 1.3.7. *Up to isomorphism there is only one group of order $10^9 + 7$.*

Indeed, $10^9 + 7$ is prime.

PROPOSITION 1.3.8. *For each $n \leq \infty$ there is exactly one cyclic group of order n, up to isomorphism.*

PROOF. Exercise. □

A cyclic group of order n has an element of order n. Note that $C_2 \times C_2$ is not cyclic, since it does not have an element of order 4.

PROPOSITION 1.3.9. *Every subgroup of a cyclic group is cyclic.*

PROOF. Let G be a cyclic group, with generator g. For a subgroup $H \subseteq G$ we will show $H = \langle g^n \rangle$ for some $n \in \mathbb{N}$, so H is cyclic. The trivial subgroup is obviously of this form. So we may suppose H is non-trivial. Let n be the smallest positive integer such that $g^n \in H$. Such an n must exist since H contains some power of g. We claim that every $h \in H$ is a power of g^n. We know that $h = g^m$ for some $m \in \mathbb{Z}$. By the division theorem in $\mathbb{Z}$ we have $m = qn + r$ for some integers q and r such that $0 \leq r < n$. Therefore

$$h = g^m = (g^n)^q g^r,$$

and $g^r = (g^n)^{-q} h$. Since $g^n \in H$ this shows that $g^r \in H$. However, n was minimal, so that $0 \leq r < n$ now implies $r = 0$. Thus $n \mid m$ and $h = g^m \in \langle g^n \rangle$. This proves $H = \langle g^n \rangle$. □

PROPOSITION 1.3.10. *Let $H \supseteq K$ be two subgroups of G. Then we have*

$$(G : K) = (G : H)(H : K).$$

PROOF. Exercise. □

DEFINITION 1.3.11. A subgroup N of G is called *normal*, if $gNg^{-1} = N$ for all $g \in G$. We denote this by $N \triangleleft G$.

EXAMPLE 1.3.12. *Let $G = GL_2(\mathbb{Z}) = \{A \in M_2(\mathbb{Z}) \mid \det(A) = \pm 1\}$ and $N = \{\left(\begin{smallmatrix} 1 & n \\ 0 & 1 \end{smallmatrix}\right) \mid n \in \mathbb{Z}\}$. Then N is a subgroup which is not normal. On the other hand, $SL_2(\mathbb{Z}) = \{A \in M_2(\mathbb{Z}) \mid \det(A) = 1\}$ is a normal subgroup of G.*

For $g = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right) \in G$ we have

$$g \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} g^{-1} = \begin{pmatrix} 1 & 0 \\ n & 1 \end{pmatrix} \notin N.$$

Clearly a subgroup N of G is normal, if and only if $gN = Ng$ for all $g \in G$.

LEMMA 1.3.13. *Every subgroup H of G with $(G : H) = 2$ is normal.*

PROOF. If $(G : H) = 2$, then $G = H \cup gH$ as disjoint union. Hence gH is the complement of H in G. The same argument shows that Hg is the complement of H in G. Thus we have $gH = G \setminus H = Hg$ for all $g \in G$. □

EXAMPLE 1.3.14. *The subgroup $C_n = \{e, r, r^2, \ldots, r^{n-1}\}$ in D_n has index 2, and hence is normal.*

EXAMPLE 1.3.15. *Every subgroup of an abelian group is normal. The converse is not true: every subgroup of the quaternion group Q_8 is normal, but Q_8 is not abelian.*

The quaternion group is given by $Q_8 = \{1, -1, i, -i, j, -j, k, -k\}$ and composition defined by $i^2 = j^2 = k^2 = -1$ and $ij = k$, $ji = -k$, $jk = i$, $kj = -i$ and $ki = j$, $ik = -j$. This comes from the quaternion algebra $\mathbb{R} \cdot 1 \oplus \mathbb{R} \cdot i \oplus \mathbb{R} \cdot j \oplus \mathbb{R} \cdot k$. Its proper subgroups are given by

$$\langle 1, -1 \rangle,\ \langle 1, -1, i, -i \rangle,\ \langle 1, -1, j, -j \rangle,\ \langle 1, -1, k, -k \rangle.$$

They are all normal. Of course, Q_8 is not abelian, as $ij = -ji$. We may represent Q_8 as the following subgroup of $GL_2(\mathbb{C})$:

$$\begin{aligned} e &= \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right),\ a = \left(\begin{smallmatrix} 0 & i \\ i & 0 \end{smallmatrix}\right),\ a^2 = \left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right),\ a^3 = \left(\begin{smallmatrix} 0 & -i \\ -i & 0 \end{smallmatrix}\right), \\ b &= \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right),\ ab = \left(\begin{smallmatrix} -i & 0 \\ 0 & i \end{smallmatrix}\right),\ a^2b = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right),\ a^3b = \left(\begin{smallmatrix} i & 0 \\ 0 & -i \end{smallmatrix}\right). \end{aligned}$$

Note that i here is not the group element in Q_8, but $i^2 = -1$ in $\mathbb{C}$. For the group elements we have made the relabeling

$$\{1, -1, i, -i, j, -j, k, -k\} \leftrightarrow \{e, a^2, a^3b, ab, b, a^2b, a, a^3\}.$$

We recall the following result.

PROPOSITION 1.3.16. *The kernel of a group homomorphism $\varphi\colon G \to H$ is a normal subgroup of G, and every normal subgroup occurs as the kernel of a homomorphism.*

In particular, $SL_n(K)$ is the kernel of the group homomorphism

$$\det\colon GL_n(K) \to K^\times,$$

and hence a normal subgroup of $GL_n(K)$. Also, the alternating group A_n is the kernel of the signature group homomorphism $\text{sign} : S_n \to \{1, 1\}$. Hence $(S_n : A_n) = 2$ and A_n is a normal subgroup of S_n.

Also recall that if N is a normal subgroup of G, there is a unique group structure on the set G/N of cosets of N in G for which $\pi\colon G \to G/N$, $a \mapsto aN$ is a homomorphism.

1.4. Permutation groups

We already have defined the symmetric group S_n by $\text{Sym}(X)$, where X has n elements. Consider a permutation $\pi \in S_n$ given by

$$\pi = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ \pi(1) & \pi(2) & \pi(3) & \cdots & \pi(n) \end{pmatrix}.$$

The pairs (i, j) with $i < j$ and $\pi(i) > \pi(j)$ are called the *inversions* of π, and π is said *even* or *odd* according as the number of inversions is even or odd.

Definition 1.4.1. The *sign* of $\pi \in S_n$ is defined by

$$\text{sign}(\pi) = \prod_{i<j} \frac{\pi(i) - \pi(j)}{i - j}.$$

We have $\text{sign}(\sigma\circ\tau) = \text{sign}(\sigma)\text{sign}(\tau)$ for all $\sigma, \tau \in S_n$, so that $\text{sign}\colon S_n \to \{\pm 1\}$, $\pi \mapsto \text{sign}(\pi)$ is a group homomorphism. For $n \geq 2$ it is surjective so that its kernel is a normal subgroup of order $|S_n|/2 = n!/2$, i.e., the *alternating group* A_n.

Recall that we can write every permutation in S_n as a disjoint product of cycles. For example,

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 7 & 4 & 2 & 1 & 3 & 6 & 8 \end{pmatrix} = (15)(27634)(8).$$

Its order is the lcm of the cycle orders, which are $2, 5$ and 1, hence $\text{lcm}(2, 5) = 10$. Furthermore, each permutation can be written as a product of transpositions, because

$$(i_1 i_2 \cdots i_r) = (i_1 i_2)(i_2 i_3) \cdots (i_{r-1} i_r)$$

for cycles of length r. Because sign is a homomorphism and the sign of a transposition (ij) is -1 we have

$$\text{sign}(\pi) = (-1)^{t(\pi)},$$

where $t(\pi)$ is the number of transpositions in the decomposition of π.

Lemma 1.4.2. *In S_n the conjugate of a cycle $\alpha = (i_1 \cdots i_k)$ is given by*

$$\tau\alpha\tau^{-1} = (\tau(i_1) \cdots \tau(i_k)).$$

Proof. Because of $(\tau^{-1}\tau)(i_r) = i_r$ and $\alpha(i_r) = i_{r+1 \bmod k}$ we have

$$\tau\alpha\tau^{-1}(\tau(i_r)) = \tau(i_{r+1 \bmod k})$$

for all $1 \leq r \leq k$. Let $1 \leq j \leq n$ such that $j \neq i_r$ for any r. Then $\alpha(j) = j$ since j is not in the k-cycle α. Hence $\tau\alpha\tau^{-1}(\tau(j)) = \tau(j)$, and $\tau\alpha\tau^{-1}$ fixes any number which is not of the form $\tau(i_r)$ for some i, and we have

$$\tau\alpha\tau^{-1} = (\tau(i_1) \cdots \tau(i_k)).$$

□

Now the orbits of any element α in S_n form a partition

$$\{1, 2, \ldots, n\} = O_1 \cup \cdots \cup O_k,$$

which determine a partition of n by

$$n = n_1 + n_2 + \ldots + n_k$$

with $n_i = |O_i|$. For example, the element $\alpha = (15)(27634)(8)$ in S_8 defines the partition

$$2 + 5 + 1 = 8.$$

Note that there are $p(8) = 22$ partitions of 8.

PROPOSITION 1.4.3. *Two elements α and β in S_n are conjugate if and only if they have the same cycle type, i.e., if and only if they define the same partition of n. In particular, the number of conjugacy classes in S_n is the number of partitions of n, i.e., we have $k(S_n) = p(n)$.*

EXAMPLE 1.4.4. *The following table lists the $p(4) = 5$ conjugacy classes in S_4.*

Partition	*Cycle type*	*Elements*
$1+1+1+1$	1	(1)
$1+1+2$	(ab)	$(12), (13), (14), (23), (24), (34)$
$1+3$	(abc)	$(123), (132), (124), (142), (134), (143), (234), (243)$
$2+2$	$(ab)(cd)$	$(12)(34), (13)(24), (14)(23)$
4	$(abcd)$	$(1234), (1432), (1324), (1423), (1243), (1342)$

The normal subgroup A_4 consists of all elements of even parity, which are given by the cycle types $(1), (abc), (ab)(cd)$. Since this is a union of conjugacy classes, including (1), A_4 is a normal subgroup of S_4. The same is true for the Kleinian 4-group

$$V_4 = \{(1), (12)(34), (13)(24), (14)(23)\},$$

which is of course isomorphic to $C_2 \times C_2$.

LEMMA 1.4.5. *The alternating group A_n is generated by cycles of length three.*

PROOF. Any $\pi \in A_n$ is the product (possibly empty) of an even number of transpositions, but the product of each two transpositions can always be written as a product of 3-cycles, namely $(ij)(jl) = (ijl)$ and

$$(ij)(kl) = (ij)(jk)(jk)(kl) = (ijk)(jkl)$$

for i, j, k, l distinct. □

DEFINITION 1.4.6. A group G is called *simple*, if it does not have a proper normal subgroup.

THEOREM 1.4.7 (Galois). *The group A_n is simple for all $n \geq 5$.*

PROOF. One can show that every non-trivial normal subgroup N of A_n for $n \geq 5$ contains a 3-cycle, and then must contain all 3-cycles. Hence, by Lemma 1.4.5, $N = A_n$.
Another proof uses induction and shows it for A_5 as follows: the conjugacy class sizes are $1, 12, 12, 20, 15$. A non-trivial normal subgroup must contain the conjugacy class of size 1, and one or more other conjugacy classes. Thus, the order of any normal subgroup must be a sum of some of these numbers, including the 1. By Lagrange's theorem, the order must also divide 60. But no such sum among these numbers divides 60, other than 1 and 60 themselves. □

Note that A_2 is trivial, $A_3 \cong C_3$ and A_4 has a proper normal subgroup isomorphic to $C_2 \times C_2$.

COROLLARY 1.4.8. *The only normal subgroups of S_n for $n \geq 5$ are $1, A_n$ and S_n.*

PROOF. If N is normal in S_n, then $N \cap A_n$ is normal in A_n. Hence either $N \cap A_n = A_n$ or $N \cap A_n = 1$. In the first case $N \supseteq A_n$. Since A_n has index 2 in S_n it follows that $N = A_n$ or $N = S_n$. In the second case, the map $n \mapsto nA_n$ from N to $S_n/A_n \cong C_2$ is injective, and so N has order 1 or 2. But it cannot have order 2 because no conjugacy class in S_n other than $\{1\}$ consists of a single element (and N is the union of conjugacy classes including the trivial conjugacy class). □

We have seen that the conjugacy classes for S_n are determined by the cycle type. This is different in the alternating groups. For example, (123) and (132) are not conjugate in A_3 although they have the same cycle type, and therefore are conjugate in S_3. The 3-cycles form two different conjugacy classes in A_3 and A_4, but only one single class in all $A_n, n \geq 5$. A conjugacy class in S_n splits into two distinct conjugacy classes under the action of A_n if and only if its cycle type consists of distinct odd integers. Otherwise, it remains a single conjugacy class in A_n. Erdös, Dénes and Turán proved in 1969 the following result [**5**]:

PROPOSITION 1.4.9. *The number of conjugacy classes in A_n is given as follows:*

$$\begin{aligned} k(A_n) &= \frac{p(n) + 3q(n)}{2} \\ &= 2p(n) + 3\sum_{r \geq 1} (-1)^r p(n - 2r^2). \end{aligned}$$

Here $q(n)$ is the number of partitions of n into distinct, odd parts.

Let us check it for A_4. Of course, $p(4) = 5$, and only $4 = 1 + 3$ is a partition into distinct, odd parts, i.e., $q(4) = 1$. Hence $k(A_4) = 4$. The other formula yields $k(A_4) = 2p(4) - 3p(2) = 10 - 6 = 4$. Indeed, the conjugacy classes of A_4 are given by

$$\begin{aligned} \mathcal{C}_1 &= \{(1)\} \\ \mathcal{C}_2 &= \{(123), (142), (134), (243)\} \\ \mathcal{C}_3 &= \{(132), (124), (143), (234)\} \\ \mathcal{C}_4 &= \{(12)(34), (13)(24), (14)(23)\} \end{aligned}$$

1.5. Groups of small order

How many different groups of a given order n are there ? This is a difficult question in general, but we can answer it for "small" n. Let $f(n)$ denote the number of different groups of order n. We already know that $f(p) = 1$ for all primes p. The following table shows the result up to $n \leq 16$.

n	$f(n)$	Groups
1	1	1
2	1	C_2
3	1	C_3
4	2	$C_4, C_2 \times C_2$
5	1	C_5
6	2	C_6, S_3
7	1	C_7
8	5	$C_8, C_2 \times C_4, C_2 \times C_2 \times C_2, Q_8, D_4$
9	2	$C_9, C_3 \times C_3$
10	2	C_{10}, D_5
11	1	C_{11}
12	5	$C_{12}, C_2 \times C_6, C_2 \times S_3, A_4, C_3 \rtimes C_4$
13	1	C_{13}
14	2	C_{14}, D_7
15	1	C_{15}
16	14	$C_{16}, C_2 \times C_8, C_4 \times C_4, C_4 \times C_2 \times C_2, C_2 \times C_2 \times C_2 \times C_2,$ $C_2 \times D_4, D_8, C_2 \times Q_8, C_4 \rtimes C_4, G_{16}^1, G_{16}^2, G_{16}^3, G_{16}^4, G_{16}^5$

We have $f(p^2) = 2$, since there are only two groups of order p^2 for a prime p, namely $C_p \times C_p$ and C_{p^2}. For a proof see Proposition 2.2.10. For larger powers of p however, the number is growing rapidly. We have the following result, see [**8**] for the lower bound and unpublished work by Mike Newman and Craig Seeley for the upper bound.

THEOREM 1.5.1 (Higman, Newman). *The number of groups of prime power order p^n is bounded by*

$$p^{\frac{2}{27}n^2(n-6)} \leq f(p^n) \leq p^{\frac{2}{27}n^3+O(n^{5/2})}$$

There is the *Millennium project* by Besche, Eick and O'Brian [**2**] of classifying all groups of order $n \leq 2000$, which was published in 2002.

THEOREM 1.5.2. *There are exactly* 49.910.529.484 *different groups of order $n \leq 2000$. More than* 99% *of them have order 2^{10}. More precisely, $f(2^{10}) = 49.487.365.422$.*

In fact, $f(2^k)$, for $k = 1, \ldots 10$ is given by

$$1,\ 2,\ 5,\ 14,\ 51,\ 267,\ 2328,\ 56092,\ 10494213,\ 49487365422.$$

Pyber showd in 1993 the following estimate [**10**].

PROPOSITION 1.5.3 (Pyber). *The number of groups of order n is bounded by*

$$f(n) \leq n^{\left(\frac{2}{27}+o(1)\right)e(n)^2},$$

where $e(n) \leq \log_2(n)$ denotes the highest power of any prime dividing n.

For very small n we can easily do the classification now. The first non-trivial case is $n = 4$.

PROPOSITION 1.5.4. *Every group of order* 4 *is isomorphic to C_4 or $C_2 \times C_2$.*

PROOF. Let G be a group of order 4. If G has an element of order 4, then $G \cong C_4$. Otherwise we have $G = \{e, a, b, c\}$ and the order of a, b, c must be a proper divisor of 4, which is 2. So we have $a^2 = b^2 = c^2 = e$. Also, $ab = c$, because all other choices for ab are not

possible, i.e., $ab = e$ would give $a = b^{-1}$ contradicting $b = b^{-1}$, and $ab = a$ would imply $b = e$. Similarly, $ab = b$ would imply $a = e$, a contradiction. The same argument shows that $ba = c = ab, ca = b = ac$ and $cb = a = bc$. Using these relations, it is easy to check that the map $f\colon G \to C_2 \times C_2$ is an isomorphism, where

$$f(e) = (1,1),\ f(a) = (-1,1),\ f(b) = (1,-1),\ f(c) = (-1,-1).$$

□

For $n = 6$ we can prove a more general result.

PROPOSITION 1.5.5. *Every group of order $2p$ for a prime $p > 2$ is isomorphic to C_{2p} or D_p. In particular, every group of order 6 is isomorphic to C_6 or $D_3 \cong S_3$.*

PROOF. By Cauchy's theorem 2.2.5, for every prime divisor p of $|G|$ there is an element of order p in G. We can apply this for $p > 2$ and 2. Denote by s the element of order 2, and by r the element of order p. Then $C_p = \langle r\rangle$ is a normal subgroup of G because of $(G : C_p) = 2$, see Lemma 1.3.13. Obviously $s \notin C_p$, so that $G = C_p \cup C_p s$. This means $G = \{1, r, \dots, r^{p-1}, s, rs, \dots, r^{p-1}s\}$. As C_p is normal, $srs^{-1} = r^i$ for some $i \in \mathbb{Z}$. Because of $s^2 = e$ we have

$$r = s^2 r s^{-2} = s(srs^{-1})s^{-1} = r^{i^2}.$$

This implies $i^2 \equiv 1 \mod p$, or $i^2 = 1$ in the finite field $\mathbb{Z}/p\mathbb{Z}$. This quadratic equation has exactly two solutions, namely $i = \pm 1$, i.e., $i \equiv 1 \mod p$ or $i \equiv -1 \mod p$. In the first case G is commutative (any group generated by a set of commuting elements is commutative), i.e., $G = \langle r, s \mid r^p = s^2 = e, rs = sr\rangle \cong C_{2p}$. In the second case we have $srs^{-1} = r^{-1}$, so that $G \cong D_p$. □

PROPOSITION 1.5.6. *Every group of order 8 is isomorphic to $C_8, C_2 \times C_4, C_2 \times C_2 \times C_2$, or isomorphic to D_4, Q_8.*

PROOF. If G is abelian, we know by the theory of modules over a PID that G is isomorphic to one of the groups $C_8, C_2 \times C_4, C_2 \times C_2 \times C_2$. Hence suppose that G is non-abelian. The non-identity elements in G have order 2 or 4. If $g^2 = e$ for all $g \in G$ then G is abelian, so some element $x \in G$ must have order 4. Let $y \in G \setminus \langle x\rangle$. The subgroup $\langle x, y\rangle$ properly contains $\langle x\rangle$, so $\langle x, y\rangle = G$. Since G is non-abelian, x and y do not commute. Since $\langle x\rangle$ has index 2 in G, it is a normal subgroup. Therefore

$$yxy^{-1} \in \langle x\rangle = \{e, x, x^2, x^3\}.$$

Since yxy^{-1} has order 4, $yxy^{-1} = x$ or $yxy^{-1} = x^3 = x^{-1}$. The first case is impossible, since x and y do not commute. Therefore $yxy^{-1} = x^{-1}$. The group $G/\langle x\rangle$ has order 2, so

$$y^2 \in \langle x\rangle = \{e, x, x^2, x^3\}.$$

Since y has order 2 or 4, y^2 has order 1 or 2. Thus $y^2 = 1$ or $y^2 = x^2$. Putting this together, $G = \langle x, y\rangle$ where either

$$x^4 = e, y^2 = e, yxy^{-1} = x^{-1},$$

or

$$x^4 = e, y^2 = x^2, yxy^{-1} = x^{-1}.$$

In the first case $G \cong D_4$, and in the second case $G \cong Q_8$. □

CHAPTER 2

Groups acting on sets

2.1. Definitions and examples

DEFINITION 2.1.1. Let G be a group and X be a set. A *(left) group action* of G on X is a mapping $(g, x) \mapsto gx$, $G \times X \to X$ such that

(1) $g(hx) = (gh)x$ for all $g, h \in G$ and all $x \in X$,
(2) $ex = x$ for the neutral element $e \in G$ and all $x \in X$.

The conditions imply that all left multiplications maps L_g belong to $\mathrm{Sym}(X)$. Axiom (1) then just says that $L\colon G \to \mathrm{Sym}(X)$, $g \mapsto L(g) = L_g$ is a homomorphism. The action is said to be *faithful*, or *effective*, if the homomorphism L is injective, i.e., if

$$gx = x \text{ for all } x \in X \text{ implies } g = e.$$

EXAMPLE 2.1.2. 1. *The group $GL_n(K)$ acts on K^n by matrix multiplication $(A, x) \mapsto Ax$.*

2. *Every group G acts on every set X by the trivial action, i.e., by $gx = x$ for all $g \in G$ and all $x \in X$.*

3. *The symmetric group S_n acts by permutations on the set $X = \{1, 2, \ldots, n\}$.*

4. *Every group G acts on itself by conjugation: with $X = G$ the action is given by $(g, x) \mapsto gxg^{-1}$.*

5. *For any group G the automorphism group $\mathrm{Aut}(G)$ acts on G.*

6. *The group $SL_2(\mathbb{C})$ of complex 2×2 matrices $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ with $\det(A) = 1$ acts on the Riemann sphere $\overline{\mathbb{C}} = \mathbb{C} \cup \{\infty\}$ by Moebius transformations*

$$(A, z) \mapsto A \cdot z = \frac{az + b}{cz + d},$$

with $A \cdot \infty = a/c$ and $A \cdot (-d/c) = \infty$.

Let us verify the axioms for the last example. The identity matrix I acts by $Iz = \frac{1z+0}{0z+1} = z$. For two matrices $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$, $B = \left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right)$ we compute

$$\begin{aligned} A \cdot (B \cdot z) = A \cdot \left(\frac{\alpha z + \beta}{\gamma z + \delta} \right) &= \frac{a\left(\frac{\alpha z+\beta}{\gamma z+\delta}\right) + b}{c\left(\frac{\alpha z+\beta}{\gamma z+\delta}\right) + d} \\ &= \frac{(a\alpha + b\gamma)z + (a\beta + b\delta)}{(c\alpha + d\gamma)z + (c\beta + d\delta)} \\ &= \begin{pmatrix} a\alpha + b\gamma & a\beta + b\delta \\ c\alpha + d\gamma & c\beta + d\delta \end{pmatrix} \cdot z \\ &= (AB) \cdot z. \end{aligned}$$

DEFINITION 2.1.3. Let G be a group acting on a set X. For $x \in X$ the set

$$Gx = \{gx \mid g \in G\} \subseteq X$$

is called the *orbit* of x.

EXAMPLE 2.1.4. *Let G act on itself by conjugation. Then the G-orbits are just the conjugacy classes. For $x \in X = G$ the conjugacy class of x is the set*

$$\{gxg^{-1} \mid g \in G\}.$$

The G-orbits of an action partition G. A subset of X is stable under the action if and only if is a union of orbits. For example, a subgroup H of G is normal if and only if it is a union of conjugacy classes (H is stable under the conjugation action).

DEFINITION 2.1.5. An action of G on X is called *transitive*, if there is only one orbit, i.e., if for any two $x, y \in X$ there exists a $g \in G$ such that $gx = y$. The set X is then called a homogeneous G-set.

For example, S_n acts transitively on $X = \{1, 2, \ldots, n\}$, since there is a permutation sending 1 to any number, but a non-trivial group G acts never transitively on itself by conjugation, because $\{e\}$ is always its own conjugacy class. Hence there are at least two orbits.

DEFINITION 2.1.6. Let G be a group acting on a set X. For $x \in X$ the set

$$G_x = \{g \in G \mid gx = x\} \subseteq G$$

is called the *stabilizer* of x, or the isotropy group of x.

It is a subgroup of G, but need not be a normal subgroup. In fact we have the following result.

LEMMA 2.1.7. *For $g \in G$ and $x \in X$ we have*

$$gG_xg^{-1} = G_{gx}.$$

PROOF. Let $h \in G_x$, i.e., $hx = x$. Then $(ghg^{-1})gx = ghx = gx$, hence $ghg^{-1} \in G_{gx}$. This implies $gG_xg^{-1} \subseteq G_{gx}$. Conversely, if $h(gx) = gx$, then

$$(g^{-1}hg)x = g^{-1}(h(gx)) = g^{-1}gx = x.$$

This means $g^{-1}hg \in G_x$, or $h \in gG_xg^{-1}$. □

EXAMPLE 2.1.8. *Let G act on itself by conjugation. Then the stabilizer of an element $x \in X$ is the so-called centralizer of x in G,*

$$C_G(x) = \{g \in G \mid gx = xg\}.$$

The center $Z(G)$ of G is the intersection over all centralizers,

$$Z(G) = \bigcap_{x \in G} C_G(x) = \{g \in G \mid gx = xg \ \forall\, x \in G\}.$$

For a subset $S \subseteq X$ we define the stabilizer of S by

$$\mathrm{Stab}(S) = \{g \in G \mid gS = S\}.$$

Again $\mathrm{Stab}(S)$ is a subgroup of G, and $\mathrm{Stab}(x) = G_x$ for an element $x \in X$. The same argument as in the proof of Lemma 2.1.7 shows that

$$\mathrm{Stab}(gS) = g \cdot \mathrm{Stab}(S) \cdot g^{-1}.$$

EXAMPLE 2.1.9. *Let G act on itself by conjugation, and let H be a subgroup of G. Then the stabilizer of H is called the* normalizer $N_G(H)$ *of H in G:*

$$N_G(H) = \{g \in G \mid gHg^{-1} = H\}.$$

Note that $N_G(H)$ is the largest subgroup of G containing H as a normal subgroup.

PROPOSITION 2.1.10. *Let G act on a set X. Then the map*

$$G/G_x \to Gx,\ gG_x \mapsto gx$$

is an isomorphism of G-sets, i.e., it is bijective and G-invariant. We have $|Gx| = (G : G_x)$.

PROOF. The map is well-defined because, if $h \in G_x$, then $ghx = gx$. It is injective because $gx = g'x$ implies that $g^{-1}g'x = x$, so that g and g' lie in the same left coset of G_x. It is surjective by construction, and obviously G-invariant. □

The result is sometimes called the *Orbit Stabilizer Theorem*, and is written

$$|G| = |Gx| \cdot |\mathrm{Stab}(x)|.$$

COROLLARY 2.1.11. *The number of conjugates gHg^{-1} of a subgroup H of G is given by $(G : N_G(H))$.*

2.2. The class equation

When X is finite, it is a union of a finite number of orbits, i.e.,

$$X = \bigcup_{i=1}^{m} O_i.$$

This implies the following result.

PROPOSITION 2.2.1. *Let G act on X. Then, for $x_i \in O_i$,*

$$|X| = \sum_{i=1}^{m} |O_i| = \sum_{i=1}^{m} (G : G_{x_i}).$$

When G acts on itself by conjugation, this formula becomes:

PROPOSITION 2.2.2 (Class equation).

$$\begin{aligned}|G| &= \sum_{x\in\mathcal{C}}(G : C_G(x)) \\ &= |Z(G)| + \sum_{y\in\mathcal{C}'}(G : C_G(x)),\end{aligned}$$

where x runs over a set $\mathcal{C}$ of representatives for the conjugacy classes, and y runs over a set $\mathcal{C}'$ of representatives for the conjugacy classes containing more than one element.

Note that each summand is a divisor of $|G|$. So each conjugacy class has size dividing $|G|$. This does not follow from Lagrange since conjugacy classes need not be subgroups.

EXAMPLE 2.2.3. *The class equation for S_4 is given by*

$$|S_4| = 24 = 1 + 6 + 8 + 3 + 6,$$

see Example 1.4.4. *We have $Z(S_4) = 1$.*

Often the class equation completely characterizes the group, but there are some groups that share the same class equation:

EXAMPLE 2.2.4. *Both non-abelian groups of order 8, D_4 and Q_8 have the class equation*

$$8 = 1 + 1 + 2 + 2 + 2.$$

For the dihedral group D_4, the elements e and r^2 have a trivial conjugacy class, i.e., $Z(D_4) = \{e, r^2\}$, whereas $C_G(r) = \{e, r, r^2, r^3\}$ so that the conjugacy class of r has $(G : C_G(r)) = \frac{8}{4} = 2$ elements, namely $\{r, r^3\}$. Similarly the conjugacy classes of s and sr are given by $\{s, sr^2\}$ resp. $\{sr^3, sr\}$. So the class equation is

$$8 = 1 + 1 + \frac{8}{4} + \frac{8}{4} + \frac{8}{4} = 1 + 1 + 2 + 2 + 2.$$

The central elements $1, -1$ in Q_8 have trivial conjugacy classes, so that $Z(Q_8) = \{\pm 1\}$, and the conjugacy classes $\{i, -i\}$, $\{j, -j\}$, $\{k, -k\}$ have size 2 each.

The class equation has some important consequences.

THEOREM 2.2.5 (Cauchy). *Let p be a prime which divides $|G|$. Then G contains an element of order p.*

PROOF. We use induction on $|G|$. Suppose that there is an element $y \in G \setminus Z(G)$ such that $p \nmid (G : C_G(y))$, then $p \mid |C_G(y)|$ because of

$$(G : 1) = (G : C_G(y)) \cdot (C_G(y) : 1).$$

By induction hypothesis, there is an element of order p in $C_G(y)$, and hence in G. Hence we may suppose that p divides *all* of the terms $(G : C_G(y))$ in the class equation for non-central elements y. But then we also have $p \mid |Z(G)|$. Since $Z(G)$ is abelian it follows from the structure theorem that it contains an element of order p. □

PROPOSITION 2.2.6. *A finite group G is a p-group, i.e., has p^m elements if and only if every element has order a power of p.*

PROOF. If $|G| = p^m$ then Lagrange's theorem shows that the order of every element is a divisor of p^m and hence a p-power. Conversely, if $q \mid |G|$ for a prime $q \neq p$, then there is an element $g \in G$ with $\operatorname{ord}(g) = q \neq p^k$ by Cauchy's theorem. This is a contradiction to the assumption, so that we obtain $|G| = p^m$ for some m. □

PROPOSITION 2.2.7. *Let G be a non-trivial finite p-group. Then its center is non-trivial.*

PROOF. By assumption $(G : 1)$ is a power of p, so that all terms over $y \in \mathcal{C}'$ in the class equation are divisible by p. This implies $p \mid |Z(G)|$. □

PROPOSITION 2.2.8. *A group of order p^n has normal subgroups of every possible order $1, p, \ldots, p^n$.*

PROOF. We use induction on n. Since $Z(G)$ contains an element g of order p by Proposition 2.2.7, $N = \langle g \rangle$ is a normal subgroup of order p. Then $|G/N| = p^{n-1}$, and we may apply the induction hypothesis. But the normal subgroups of G/N correspond to normal subgroups of G containing N, so the claim follows for G. □

LEMMA 2.2.9. *Suppose G contains a subgroup H with $H \subseteq Z(G)$ such that G/H is cyclic. Then G is abelian.*

PROOF. Let a be an element in G whose image in G/H generates it. Then every element of G can be written $g = a^j h$ with $h \in H$ and $j \in \mathbb{Z}$. Because of $H \subseteq Z(G)$ we have

$$\begin{aligned} a^i h \cdot a^j h' &= a^i a^j h h' \\ &= a^j a^i h' h \\ &= a^j h' \cdot a^i h. \end{aligned}$$

□

PROPOSITION 2.2.10. *Every group of order p^2 for a prime p is commutative, and hence isomorphic to $C_p \times C_p$ or C_{p^2}.*

PROOF. By Lagrange we have $|Z(G)| \in \{1, p, p^2\}$, and because of Proposition 2.2.7 we can exclude order 1, which means that $|G/Z(G)| \in \{1, p\}$. In either case, $G/Z(G)$ is cyclic so that G is abelian by Lemma 2.2.9. □

How many groups of order p^3 are there? For $p = 2$ we have answered this in Proposition 1.5.6. For any prime p we consider the group

$$\mathrm{Aff}(\mathbb{Z}/(p^2)) = \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \mid a, b \in \mathbb{Z}/(p^2), a \neq 0 \right\} \subseteq GL_2(\mathbb{Z}/(p^2))$$

of order $p^2\varphi(p^2) = p^3(p-1)$, which is called the *affine group* over the ring $\mathbb{Z}/(p^2)$. It has a unique "Sylow p-subgroup" $\Gamma(p)$, i.e., a normal subgroup of order p^3 given by

$$\Gamma(p) = \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \mid a, b \in \mathbb{Z}/(p^2), a^p = 1 \text{ in } (\mathbb{Z}/(p^2))^\times \right\}.$$

It is the kernel of the homomorphism $\mathrm{Aff}(\mathbb{Z}/(p^2)) \to (\mathbb{Z}/(p^2))^\times$ given by $\left(\begin{smallmatrix} a & b \\ 0 & 1 \end{smallmatrix}\right) \mapsto a^p$, and it has an element of order p^2, namely $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$.

The *Heisenberg group* over $\mathbb{Z}/(p)$ is defined by

$$\mathrm{Heis}(\mathbb{Z}/(p)) = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \mid a, b, c \in \mathbb{Z}/(p) \right\}.$$

For $p = 2$ the groups $\Gamma(2)$ and $\mathrm{Heis}(\mathbb{Z}/(2))$ are both isomorphic to D_4. For $p > 2$ we obtain two non-isomorphic groups which are both non-abelian. In fact, all non-trivial elements in $\mathrm{Heis}(\mathbb{Z}/(p))$ for $p > 2$ have order p, since

$$\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}^p = \begin{pmatrix} 1 & 0 & \frac{p(p-1)}{2}ac \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = I,$$

because $\frac{p(p-1)}{2} \equiv 0 \bmod p$ for all $p > 2$. This is not the case in the group $\Gamma(p)$, as we have seen.

THEOREM 2.2.11. *Every group of order p^3 for a prime $p > 2$ is isomorphic to one of the groups $C_p \times C_p \times C_p$, $C_p \times C_{p^2}$, C_{p^3}, $\mathrm{Heis}(\mathbb{Z}/p)$ or $\Gamma(p)$.*

The proof is due to Hölder (1893).

2.3. The Sylow theorems

DEFINITION 2.3.1. Let G be a group and let p be a prime dividing $|G|$. A subgroup of G is called a *Sylow p-subgroup* of G if its order is the highest p-power dividing $|G|$.

EXAMPLE 2.3.2. *$P = \{(1), (123), (132)\}$ is a Sylow 3-subgroup of S_4, and*

$$Q = \{(1), (1234), (13)(24), (1432), (24), (14)(23), (13), (12)(34)\}$$

is a Sylow 2-subgroup of S_4 which is isomorphic to D_4.

Here we have $|S_4| = 24 = 2^3 \cdot 3$, and $r = (1234)$, $s = (24)$.

LEMMA 2.3.3. *Let H be a p-group acting on a finite set X, and let X^H be the set of points fixed by H, then*

$$|X| \equiv |X^H| \bmod p.$$

In particular we have

$$|H| \equiv |Z(H)| \bmod p.$$

PROOF. By the orbit-stabilizer theorem we have $(H : \mathrm{Stab}(x_0)) = |Hx_0|$. Because H is a p-group this is a power of p, and either Hx_0 consists of a single element, or $|Hx_0|$ is divisible by p. Since X is the disjoint union of the orbits, the first claim follows. When we apply this to the action by conjugation, the second claim follows. □

THEOREM 2.3.4 (Sylow I). *Let G be a finite group and p be a prime. If $p^r \mid |G|$ for some $r \geq 1$, then G has a subgroup of order p^r.*

PROOF. By Proposition 2.2.8 it suffices to prove the statement where $p^r \mid\mid |G|$ is the highest power of p dividing the order of G, because if G has a subgroup of order p^r, then it also has subgroups of all possible lower orders $1, p, p^2, \ldots, p^r$. So we may assume that $|G| = p^r m$ with $p \nmid m$. Let

$$X = \{S \subseteq G \mid |S| = p^r\}.$$

Define a G-action on X by

$$(g, A) \mapsto gA = \{ga \mid a \in A\}.$$

Let $A \in X$, i.e., $A = \{g_1, \ldots, g_{p^r}\}$, and let

$$H = \mathrm{Stab}(A) = \{g \in G \mid gA = A\}.$$

For any $g_i \in A$ the map $h \mapsto hg_i$, $H \to A$ is injective because of the cancellation law, and so

$$(H : 1) \leq |A| = p^r.$$

So in the equation

$$(G:1) = (G:H)(H:1)$$

we know that $(G:1) = p^r m$ with $p \nmid m$, and $(H:1) = p^k$ with $k \leq r$, and that $(G:H)$ is the number of elements in the orbit of A. Hence it is enough to find *one* set A such that p doesn't divide the number of elements in its orbit, because then we can conclude (for this particular A) that the subgroup $H = \mathrm{Stab}(A)$ has order p^r, and we are done. The number of elements in X is

$$|X| = \binom{p^r m}{p^r} = \frac{(p^r m)(p^r m - 1)\cdots(p^r m - i)\cdots(p^r m - p^r + 1)}{p^r(p^r - 1)\cdots(p^r - i)\cdots(p^r - p^r + 1)}.$$

Because of $i < p^r$ the power of p dividing $p^r m - i$ equals the power of p dividing i. The same is true for $p^r - i$. Therefore the corresponding terms on top and bottom are divisible by the same powers of p, and so p *does not divide* $|X|$. Because the orbits form a partition of X, at least one orbit (for a set A) is not divisible by p. This finishes the proof. □

COROLLARY 2.3.5. *The converse of Lagrange's theorem is true for p-groups.*

The converse of Lagrange's theorem is false in general: if G is a finite group and $d \mid |G|$, then there may not be a subgroup of G with order d. The simplest example of this is the group A_4, of order 12, which has no subgroup of order 6. For an elegant proof see section 3.4, which has more results on the converse of Lagrange's theorem. Of course, we also can just list all subgroups of A_4 by hand:

EXAMPLE 2.3.6. *The subgroups of A_4 are given as follows:*

Order	#	*Subgroups*
1	1	$\{(1)\}$
2	3	$\{(1),(12)(34)\}$, $\{(1),(13)(24)\}$, $\{(1),(14)(23)\}$
3	4	$\{(1),(123),(132)\}$, $\{(1),(243),(234)\}$, $\{(1),(142),(124)\}$, $\{(1),(134),(143)\}$
4	1	$\{(1),(12)(34),(13)(24),(14)(23)\}$
12	1	$\{1,(12)(34),(13)(24),(14)(23),(123),(243),(142),(134),$ $(132),(143),(234),(124)\}$

This also shows that there is no subgroup of order 6 in A_4, although $6 \mid 12 = |A_4|$. According to Sylow I there is a subgroup of order 2, 2^2, and 3. The group of order 4 is the unique Sylow 2-subgroup, and the four groups of order 3 the Sylow 3-subgroups.

EXAMPLE 2.3.7. *The subgroup U of upper unitriangular matrices in the group $G = GL_n(\mathbb{F}_p)$ forms a Sylow p-subgroup of G.*

A triangular matrix is called *unitriangular*, if all diagonal elements are 1. It is clear that

$$|U| = p^{\frac{n(n-1)}{2}},$$

and a simple counting argument shows that

$$\begin{aligned} |G| &= (p^n - 1)(p^n - p)(p^n - p^2)\cdots(p^n - p^{n-1}) \\ &= p^{\frac{n(n-1)}{2}} \cdot m, \end{aligned}$$

where $p \nmid m$. Hence U is a Sylow p-subgroup of G.

Sylow I gives another proof of Cauchy's Theorem 2.2.5:

COROLLARY 2.3.8 (Cauchy). *If p divides $|G|$, then G contains an element of order p.*

PROOF. By Sylow I, G has a subgroup of order p. Hence any $g \neq e$ is an element of order p in G. □

LEMMA 2.3.9. *Let P be a Sylow p-subgroup of G, and let H be a p-subgroup. If H normalizes P, i.e., if $H \subseteq N_G(P)$, then $H \subseteq P$. In particular, no Sylow p-subgroup of G other than P normalizes P.*

PROOF. Because H and P are subgroups of $N_G(P)$ with P normal in $N_G(P)$, HP is a subgroup. The second isomorphism theorem yields

$$H/H \cap P \cong HP/P.$$

Therefore $(HP : P)$ is a power of p, because $(H : 1)$ is a power of p by assumption. But we have

$$(HP : 1) = (HP : P)(P : 1),$$

and $(P : 1)$ is the largest power of p dividing $(G : 1)$, hence also the largest power of p dividing $(HP : 1)$. Thus $(HP : P) = p^0 = 1$, and $H \subseteq P$. □

THEOREM 2.3.10 (Sylow II). *Any two Sylow p-subgroups are conjugate.*

PROOF. Let X be the set of Sylow p-subgroups in G, and let G act on X by conjugation, i.e., by

$$(g, P) \mapsto gPg^{-1}.$$

Let O be one of the G-orbits. We have to show that $O = X$. Let $P \in O$, and let P act through the action of G. This single G-orbit O may break up into several P-orbits, and one of them will be P. In fact this is the *only* one-point orbit because $\{Q\}$ is a P-orbit if and only if P normalizes Q, which happens only for $Q = P$, by Lemma 2.3.9. Hence the number of elements in every P-orbit other than $\{P\}$ is divisible by p, and we have

$$|O| \equiv 1 \bmod p.$$

Suppose that there exists a $P \notin O$. Then the previous argument gives that the number of elements in every P-orbit is divisible by p, because there are no one-point orbits in this case. So we obtain $|O| \equiv 0 \bmod p$, a contradiction. Hence there is no P with $P \notin O$, so that $O = X$. □

THEOREM 2.3.11 (Sylow III). *Let s_p be the number of Sylow p-subgroups in G and let $|G| = p^r m$ with $p \nmid m$. Then $s_p \mid m$, and $s_p = (G : N_G(P))$ for any Sylow p-subgroup P of G. We have*

$$s_p \equiv 1 \bmod p.$$

PROOF. In the proof of Sylow II we already showed that $s_p = |O| \equiv 1 \bmod p$. Let P be a Sylow p-subgroup of G. In Corollary 2.1.11 we showed that the number of conjugates of P is $(G : N_G(H))$. But this is just s_p. We have

$$\begin{aligned}(G : N_G(P)) &= \frac{(G : 1)}{(N_G(P) : 1)} \\ &= \frac{(G : 1)}{(N_G(P) : P)(P : 1)} \\ &= \frac{m}{(N_G(P) : P)},\end{aligned}$$

which is a factor of m. Hence $s_p \mid m$. □

COROLLARY 2.3.12. *Every p-subgroup of G is contained in a Sylow p-subgroup.*

PROOF. Let H be a p-subgroup of G, and let H act on the set X of Sylow p-subgroups by conjugation. Because $|X| = s_p$ is not divisible by p by Sylow III, X^H must be nonempty by Lemma 2.3.3. This means that at least one H-orbit consists of a single Sylow p-subgroup. But then H normalizes P and Lemma 2.3.9 implies that $H \subseteq P$. □

COROLLARY 2.3.13. *A Sylow p-subgroup P of G is normal if and only if it is the only Sylow p-subgroup.*

PROOF. Suppose that P is normal. Then, by Sylow II, P is the only Sylow p-subgroup: another Sylow p-subgroup Q satisfies $Q = gPg^{-1} = P$. Conversely, suppose that $s_p = 1$. Then $gPg^{-1} = P$, so that P is normal. □

COROLLARY 2.3.14. *Suppose that G has only one Sylow p-subgroup for each prime p dividing $|G|$. Then G is a direct product of its Sylow p-subgroups.*

PROOF. Let $P_1, \ldots, P_k$ be the Sylow-subgroups of G, and let $|P_i| = p_i^{r_i}$ with the different primes p_i which divide $|G|$. By Corollary 2.3.13 each P_i is normal in G, so that the product $P_1 \cdots P_k$ is also normal in G. We shall prove by induction on k that $|P_1 \cdots P_k| = p_1^{r_1} \cdots p_k^{r_k}$. For $k = 1$ there is nothing to prove, so that we may assume that $k \geq 2$ and $|P_1 \cdots P_{k-1}| = p_1^{r_1} \cdots p_{k-1}^{r_{k-1}}$. Then $P_1 \cdots P_{k-1} \cap P_k = 1$, so that $(P_1 \cdots P_{k-1})P_k$ is the direct product of $P_1 \cdots P_{k-1}$ and P_k, and thus has order $p_1^{r_1} \cdots p_k^{r_k}$. Finally, G is the direct product of its Sylow p-subgroups, because G is the product of them, each one is normal in G, and all intersections $P_j \cap (P_1 \cdots P_{j-1} P_{j+1} \cdots P_k)$ are trivial. □

EXAMPLE 2.3.15. *Every group G of order 99 is commutative.*

We have $99 = 3^2 \cdot 11$ and $s_{11} \mid 9$, $s_{11} \equiv 1 \bmod 11$. This implies $s_{11} = 1$. Hence there is exactly one Sylow 11-subgroup H, which is normal in G. Similarly, $s_3 \mid 11$ and $s_3 \equiv 1 \bmod 3$, so that $s_3 = 1$. Hence there is exactly one Sylow 3-subgroup K, which is normal in G. By Corollary 2.3.14, $G = H \times K$, and both H and K are commutative. Hence G is commutative.

REMARK 2.3.16. The same argument shows that every group of order p^2q with primes $p < q$ and $q \not\equiv 1 \bmod p$ is commutative.

LEMMA 2.3.17. *Let G be a finite group and p be the smallest prime dividing $|G|$. Then any subgroup H of index p is normal in G.*

PROOF. Let H be a subgroup of G such that $(G : H) = p$. Let G act on the set of left cosets G/H by left multiplication. This action is non-trivial, so that it gives rise to a non-trivial group homomorphism

$$\theta : G \to \mathrm{Sym}(G/H) = S_p.$$

Since the action is transitive, $\ker(\theta)$ is the largest normal subgroup N of G contained in H. Suppose that $N \neq H$. We have

$$(G : N) = (G : H)(H : N) = p(H : N).$$

Since we assume that $(H : N) > 1$, there exists a prime q dividing it. Since p is the smallest prime dividing $|G|$ we have $p \leq q$. Hence

$$pq \mid (G : N) = \frac{|G|}{|N|} = |\mathrm{im}(\theta)| \mid p! = |S_p|.$$

But $pq \mid p!$ is impossible for $q \geq p$, and we obtain a contradiction. Hence $N = H$ is a normal subgroup of G. □

We can apply this Lemma together with the Sylow Theorems to show that groups of a certain order always have a non-trivial proper normal subgroup. Hence they cannot be simple.

PROPOSITION 2.3.18. *Let G be a group of order pq^r for primes $p < q$ and $r \geq 1$. Then G is not simple.*

PROOF. Let H be a Sylow q-subgroup of G. Then Lemma 2.3.17 shows that H is normal. Since $|H| = q^r$, this is a proper normal subgroup. □

We mention the following result of Burnside.

THEOREM 2.3.19 (Burnside 1901). *Let G be a group of order $p^r q^s$ for primes $p < q$ and $r, s \geq 1$. Then G is not simple.*

This result cannot be generalized to groups of order $p_1^{r_1} p_2^{r_2} p_3^{r_3}$, because $|A_5| = 60 = 2^2 \cdot 3 \cdot 5$, and A_5 is simple. It turns out that the smallest non-abelian simple group has order 60. The Sylow Theorems show that there is no other simple group of order 60 besides A_5.

PROPOSITION 2.3.20. *Every simple group of order 60 is isomorphic to A_5.*

PROOF. Suppose that G is simple, and $|G| = 60$. Then $s_5 \geq 2$, because otherwise the Sylow 5-subgroup would be a proper normal subgroup of G. We have $s_5 \mid 12$ and $s_5 \equiv 1 \bmod 5$, so that $s_5 = 6$.

Case 1: There exists a subgroup $U \neq G$ of index $n = (G : U) \leq 5$.
In this case the action of G on the cosets G/U yields a non-trivial homomorphism

$$\varphi \colon G \hookrightarrow \mathrm{Sym}(G/U) = S_n$$

for $n \leq 5$. Since G is simple, $\ker(\varphi)$ must be trivial, because φ is non-trivial. This implies $n = 5$. Then G is a normal subgroup of index 2 in S_5, so that $G \cong A_5$ by Corollary 1.4.8.

Case 2: For each proper subgroup $U \leq G$ we have $(G : U) \geq 6$.
We will show that this case cannot occur. Let P be a Sylow 2-subgroup of G. We have $s_2 \geq 2$ and $s_2 \mid 15$, $s_2 \equiv 1 \bmod 2$, so that $s_2 = 3, 5, 15$. Actually we have

$$s_2 = (G : N_G(P)) \geq 6$$

by assumption, so that $s_2 = 15$. We need a further case distinction.

Case 2a: For each two different Sylow 2-subgroups P and Q we have $P \cap Q = 1$.
In this case we have $15(4-1)$ elements of order 2 or 4 (the non-identity elements in the 15 Sylow 2-subgroups), and $6(5-1)$ elements of order 5, from the 6 Sylow 5-subgroups. Together we would have

$$(G : 1) \geq 15(4-1) + 6(5-1) + 1 = 70,$$

which is a contradiction to $(G : 1) = 60$.

Case 2b: There exist two different Sylow 2-subgroups P and Q of G with $P \cap Q \neq 1$.
Let $R = P \cap Q$. As $|R|$ divides $|P| = 4$, we have $|R| = 2, 4$. However, $|R| = 4$ would imply that $P = Q = P \cap Q$, a contradiction. Hence $|R| = 2$. Now $N_G(R) \neq G$, because otherwise R would be a proper normal subgroup of G, contradicting the assumption that G is simple. The Sylow 2-subgroups are of order 4, hence commutative. So P and Q are abelian, and thus $P, Q \leq N_G(R)$. Let $S = \langle P, Q \rangle$. We have $S \leq N_G(R)$, and hence $S \neq G$. Also, $4 \mid |S|$, $|S| \mid 60$

and $|S| > 4$, since otherwise $P = Q = S$, a contradiction. So $|S| = 12, 20$ and $(G : S) \leq \frac{60}{12} = 5$, which is a contradiction to the assumption of Case 2. □

LEMMA 2.3.21. *If p and q are different prime factors of $|G|$ with $s_p = s_q = 1$, then the elements of the p-Sylow subgroup commute with the elements of the q-Sylow subgroup.*

PROOF. Let P be the p-Sylow subgroup and Q be the q-Sylow subgroup. Since P and Q have relatively primes sizes, $P \cap Q = 1$ by Lagrange. The subgroups P and Q are normal in G by Corollary 2.3.13. For $a \in P$ and $b \in Q$ we have

$$aba^{-1}b^{-1} = (aba^{-1})b^{-1} = a(ba^{-1}b^{-1}) \in P \cap Q = 1,$$

so that $ab = ba$. □

PROPOSITION 2.3.22. *Let G be a group of order pq with primes $p < q$ and $q \not\equiv 1 \bmod p$. Then G is cyclic.*

PROOF. By Cauchy's Theorem, G has an element a of order p and an element b of order q. Let $P = \langle a \rangle$ and $Q = \langle b \rangle$. These subgroups have size p and q, and P is a Sylow p-subgroup, Q is a Sylow q-subgroup. By Sylow III we have $s_p \mid q$ and $s_p \equiv 1 \bmod p$. Since $q \not\equiv 1 \bmod p$ we must have $s_p = 1$, so that P is normal in G. Similarly we have $s_q \mid p$ and $s_q \equiv 1 \bmod q$. Since $1 < p < q$ and $q \not\equiv 1 \bmod p$ we must have $s_q = 1$ as well. Therefore Q is normal in G. Now we can apply Lemma 2.3.21 to show that the elements of P commute with the elements of Q. If we apply this to the generators a and b, we have $ab = ba$, and $\mathrm{ord}(a)$ and $\mathrm{ord}(b)$ are coprime. Hence $\mathrm{ord}(ab) = pq$, and ab generates G. □

EXAMPLE 2.3.23. *Every group of order 15 is cyclic.*

PROPOSITION 2.3.24. *Let G be the group $GL_2(\mathbb{F}_p)$ for p prime. Then any element of order p in G is conjugate to an upper unitriangular matrix $\left(\begin{smallmatrix} 1 & a \\ 0 & 1 \end{smallmatrix}\right)$. The number of Sylow p-subgroups is $p + 1$.*

PROOF. The order of G is $(p^2 - p)(p^2 - 1) = p(p+1)(p-1)^2$. Therefore a Sylow p-subgroup has size p. The matrix $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ has order p, hence it generates a Sylow p-subgroup P, which consists of all upper unitriangular matrices. Since all Sylow p-subgroups are conjugate, any matrix of order p in G is conjugate to some power of $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$.
By Sylow III, the number of Sylow p-subgroups is given by $(G : N_G(P))$. Let us compute $N_G(P)$. For a matrix $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ to lie in $N_G(P)$ means it conjugates $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ to some power $\left(\begin{smallmatrix} 1 & a \\ 0 & 1 \end{smallmatrix}\right)$. Since

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \frac{1}{ad - bc} \begin{pmatrix} ad - bc - ac & a^2 \\ -c^2 & ad - bc + ac \end{pmatrix},$$

we see that $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in N_G(P)$ precisely when $c = 0$. Therefore $N_G(P) = \{\left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right)\}$ in G, which has size $p(p-1)^2$. It follows that

$$s_p = (G : N_G(P)) = \frac{p(p+1)(p-1)^2}{p(p-1)^2} = p + 1.$$

□

COROLLARY 2.3.25. *The number of elements of order p in $GL_2(\mathbb{F}_p)$ is $p^2 - 1$.*

PROOF. Each Sylow p-subgroup has $p - 1$ elements of order p. Different Sylow p-subgroups only intersect trivially, so the number of elements of order p is $(p-1)s_p = p^2 - 1$. □

After Theorem 2.2.10 we had claimed that $\mathrm{Aff}(\mathbb{Z}/(p^2)$ has a unique Sylow p-subgroup, namely $\Gamma(p)$. We can now prove this.

PROPOSITION 2.3.26. *The group* $\mathrm{Aff}(\mathbb{Z}/(p^2))$ *for* p *prime has a unique Sylow* p*-subgroup.*

PROOF. The group has order $p^3(p-1)$, so a Sylow p-subgroup has order p^3. By Sylow III we have $s_p \mid (p-1)$ and $s_p \equiv 1 \bmod p$. Therefore $s_p = 1$. □

This unique Sylow p-subgroup $\Gamma(p)$ is a non-abelian group of order p^3. It has an element of order p^2, namely $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$. Therefore it is not isomorphic to $\mathrm{Heis}(\mathbb{Z}/(p))$ for $p > 2$, since in that case every non-identity element of $\mathrm{Heis}(\mathbb{Z}/(p))$ has order p, see the computation after Theorem 2.2.10. Hence we have the following result.

COROLLARY 2.3.27. *The groups* $\Gamma(p)$ *and* $\mathrm{Heis}(\mathbb{Z}/(p))$ *of order* p^3 *are non-isomorphic for* $p > 2$*, and isomorphic for* $p = 2$*.*

2.4. Semidirect products

A semidirect product of two groups is a generalization of the direct product, involving group automorphisms. We recall that inner automorphisms of G are of the form i_g, given by $i_g(x) = gxg^{-1}$.

LEMMA 2.4.1. *Let* G *be a group. Then* $G/Z(G) \cong \mathrm{Inn}(G)$*.*

PROOF. Consider the map $\varphi\colon G \to \mathrm{Aut}(G)$, $g \mapsto i_g$. It is a homomorphism with kernel $Z(G)$. By the isomorphism theorem, $G/\ker(\varphi) \cong \mathrm{im}(\varphi)$, which gives the claim. □

EXAMPLE 2.4.2. *The inner automorphism group of* Q_8 *is isomorphic to* $C_2 \times C_2$*.*

Since $Z(Q_8) = \{\pm 1\}$, $\mathrm{Inn}(Q_8) \cong Q_8/\{\pm 1\} \cong C_2 \times C_2$. In fact, $\mathrm{Aut}(Q_8) \cong S_4$.

LEMMA 2.4.3. $\mathrm{Inn}(G)$ *is a normal subgroup of* $\mathrm{Aut}(G)$*.*

PROOF. Clearly $\mathrm{Inn}(G)$ is a subgroup. Let $g \in G$ and $\alpha \in \mathrm{Aut}(G)$. Then we have

$$\begin{aligned}(\alpha \circ i_g \circ \alpha^{-1})(x) &= \alpha(g \cdot \alpha^{-1}(x) \cdot g^{-1}) \\ &= \alpha(g) \cdot x \cdot \alpha(g)^{-1} \\ &= i_{\alpha(g)}(x).\end{aligned}$$

□

DEFINITION 2.4.4. Let G be a group. The quotient group

$$\mathrm{Out}(G) = \mathrm{Aut}(G)/Inn(G)$$

is called the *outer automorphism group* of G. If $\mathrm{Out}(G)$ is trivial and G has a trivial center, then G is said to be *complete*.

A group G is complete if and only if the map $g \mapsto i_g$, $G \to \mathrm{Inn}(G)$ is an isomorphism. Hence a complete group is isomorphic to its automorphism group: $G \cong \mathrm{Aut}(G)$. The converse need not be true. In fact, $D_4 \cong \mathrm{Aut}(D_4)$, but D_4 is not complete, because it has a non-trivial center.
Clearly an abelian groups satisfies $\mathrm{Aut}(G) \cong \mathrm{Out}(G)$. We mention the following result.

PROPOSITION 2.4.5. *The group* S_n *is complete for* $n \neq 2, 6$*.*

We have $\mathrm{Out}(S_6) \cong C_2$, so that S_6 is not complete. Also $Z(S_2) = S_2$, and hence S_2 is not complete.

Let N be a normal subgroup of G. Each element $g \in G$ defines an automorphism of N by $n \mapsto gng^{-1}$, and this defines a homomorphism

$$\theta\colon G \to \mathrm{Aut}(N),\ g \mapsto i_{g|N}.$$

Suppose that there exists a subgroup Q of G such that the canonical homomorphism $\pi\colon G \to G/N$ maps Q isomorphically onto G/N. In this case we can reconstruct G from the triple $(N, Q, \theta_{|Q})$. Indeed, every $g \in G$ can be written uniquely in the form $g = nq$ with $n \in N$ and $q \in Q$, where q must be the unique element of Q mapping to $gN \in G/N$, and n must be gq^{-1}. Thus we have a one-to-one correspondence of sets

$$G \leftrightarrow N \times Q.$$

The product of two elements $g = nq$ and $g' = n'q'$ is given as follows

$$\begin{aligned} gg' &= (nq)(n'q') \\ &= n(qn'q^{-1})qq' \\ &= n \cdot \theta(q)(n') \cdot qq'. \end{aligned}$$

Definition 2.4.6. A group G is the *semidirect product* of its subgroups N and Q, if N is normal and $G \to G/N$ induces an isomorphism $Q \to G/N$. We write $G = N \rtimes Q$.

More precisely we write $G = N \rtimes_\theta Q$, where $\theta\colon Q \to \mathrm{Aut}(N)$ gives the action of Q on N by inner automorphisms. Note that Q need not be a normal subgroup of G.

Remark 2.4.7. Equivalently, G is a semidirect product of its subgroups N and Q if N is normal in G, $NQ = G$, and $N \cap Q = 1$.

Example 2.4.8. 1. *In D_n for $n \geq 2$ we have $N = \langle r \rangle = C_n$ and $Q = \langle s \rangle = C_2$ with*

$$D_n = N \rtimes_\theta Q = C_n \rtimes_\theta C_2,$$

where $\theta(s)(r^i) = r^{-i}$.

2. *$S_n = A_n \rtimes C_2$, because A_n is a normal subgroup of index 2 in S_n, so that $Q = \{(12)\}$ maps isomorphically onto S_n/A_n.*

3. *The group C_{p^2} for p prime is not a semidirect product of non-trivial subgroups, because it has only one subgroup of order p.*

4. *Also Q_8 cannot be written as a semidirect product of two non-trivial subgroups.*

We can construct the semidirect product $N \rtimes_\theta Q$ from two groups N and Q and a homomorphism $\theta\colon Q \to \mathrm{Aut}(N)$ as follows. As a set, let $G = N \times Q$, and define the composition in G by

$$(n, q)(n', q') = (n \cdot \theta(q)(n'), qq'). \tag{2.1}$$

Proposition 2.4.9. *The above composition law makes G into a group, which is the semidirect product $N \rtimes_\theta Q$.*

PROOF. Writing ${}^q n$ for $\theta(q)n$ we have

$$\begin{aligned}((n,q)(n',q'))(n'',q'') &= (n \cdot {}^q n' \cdot {}^{qq'} n'', qq'q'') \\ &= (n,q)((n',q')(n'',q'')).\end{aligned}$$

Hence the associative law holds. Because $\theta(1) = 1$ and ${}^q 1 = 1$,

$$(1,1)(n,q) = (n,q) = (n,q)(1,1).$$

Hence $(1,1)$ is an identity element. Also,

$$\begin{aligned}(n,q)({}^{q^{-1}} n, q^{-1}) &= (1,1) \\ &= ({}^{q^{-1}} n, q^{-1})(n,q),\end{aligned}$$

and so $({}^{q^{-1}} n, q^{-1})$ is an inverse for (n,q). Thus G is a group. It is not difficult to see that N is a normal subgroup with $QN = G$ and $N \cap Q = 1$, so that $G = N \rtimes Q$. Moreover, when N and Q are regarded as subgroups of G, the action of Q on N is that given by θ. □

REMARK 2.4.10. The direct product $N \times Q$ is isomorphic to the semidirect product $N \rtimes_\theta Q$ if and only if θ is the trivial homomorphism $Q \to \mathrm{Aut}(N)$ given by $\theta(q)(n) = n$ for all $q \in Q, n \in N$.

EXAMPLE 2.4.11. *Every group of order* 6 *is a semidirect product, namely* $C_6 \cong C_3 \times C_2$ *and* $S_3 \cong C_3 \rtimes_\theta C_2$.

Indeed, there are only two homomorphisms $\theta\colon C_2 \to \mathrm{Aut}(C_3) \cong C_2$. The trivial one gives rise the the direct product $C_3 \times C_2$, and the other one to $C_3 \rtimes_\theta C_2$. In fact, it coincides with the semidirect product $D_3 = C_3 \rtimes_\theta C_2$ from Example 2.4.8, and we have $D_3 \cong S_3$.

EXAMPLE 2.4.12. *We have* $\mathrm{Isom}(\mathbb{R}^n) \cong T(n) \rtimes_\theta O_n(\mathbb{R})$, *where* $T(n)$ *denotes the normal subgroup of translations, and* θ *is the natural inclusion*

$$\theta\colon O_n(\mathbb{R}) \to \mathrm{Aut}(T(n)).$$

EXAMPLE 2.4.13. *Every non-abelian group of order* p^3 *for* $p > 2$ *is a semidirect product.*

Such a group either has an element a of order p^2, or it doesn't. In the first case let $N = \langle a \rangle$, and $Q = \langle b \rangle$ for an element b of order p. Then $\mathrm{Aut}(N) \cong C_{p-1} \times C_p$, and the second factor is generated by the automorphism $\beta\colon a \mapsto a^{1+p}$. We have $\beta^k(a) = a^{1+kp}$. Define $\theta\colon Q \to \mathrm{Aut}(N)$ by $b \mapsto \beta$. The group $G := N \ltimes_\theta Q$ has generators a, b and defining relations

$$a^{p^2} = 1,\ b^p = 1,\ bab^{-1} = a^{1+p}.$$

It is isomorphic to the group $\Gamma(p)$.

In the second case, take two different elements a, b of order p, and let $N = \langle a, b \rangle$ be the product of the cyclic groups $\langle a \rangle$ and $\langle b \rangle$. Let $Q = \langle c \rangle$ with another element c of order p. Define $\theta\colon Q \to \mathrm{Aut}(N)$ to be the homomorphism such that

$$\theta(c^i)(a) = ab^i,\ \theta(c^i)(b) = b.$$

The group $G := N \ltimes_\theta Q$ is of order p^3, with generators a, b, c and defining relations

$$a^p = b^p = c^p = 1,\ ab = cac^{-1},\ [b,a] = [b,c] = 1,$$

where $[g,h] := ghg^{-1}h^{-1}$ denotes the commutator of two elements. This group is isomorphic to $\mathrm{Heis}(\mathbb{Z}/(p))$. For $p > 2$ it does not have an element of order p^2. When $p = 2$, then $G \cong D_4$,

which does have an element of order 2^2.

We can now extend Proposition 2.3.22.

PROPOSITION 2.4.14. *Let G be a group of order pq with primes $p < q$. If $q \not\equiv 1 \bmod p$, then $G \cong C_{pq}$. If $q \equiv 1 \bmod p$, then G is isomorphic to either C_{pq}, or to the non-abelian group*

$$\left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \mid a \in (\mathbb{Z}/(q))^\times, b \in \mathbb{Z}/(q), a^p \equiv 1 \bmod q \right\} \cong C_q \rtimes C_p.$$

PROOF. Let P be a Sylow p-subgroup of G, and Q be a Sylow q-subgroup of G. We have $P \cong C_p$, $Q \cong C_q$ and $(G : Q) = p$, which is the smallest prime dividing $(G : 1)$. By Lemma 2.3.17, Q is normal. Because P maps bijectively onto G/Q, we have that $G = Q \rtimes P$. Since $\mathrm{Aut}(Q) \cong C_{q-1}$ we obtain $G = Q \times P \cong C_q \times C_p \cong C_{pq}$, unless $p \mid (q-1)$, i.e., $q \equiv 1 \bmod p$. In that case the cyclic group $\mathrm{Aut}(Q)$ has a unique subgroup A of order p. In fact, A consists of the automorphisms $x \mapsto x^i$ for $i \in \mathbb{Z}/q\mathbb{Z}$ with $i^p = 1$. Let a and b be generators of P and Q respectively, and let the action of a on Q by conjugation be $x \mapsto x^j$ with $j \neq 1$ in $\mathbb{Z}/q\mathbb{Z}$. Then

$$G = \langle a, b \mid a^p = b^q = 1,\ aba^{-1} = b^j \rangle,$$

which is the semidirect product $Q \rtimes P$ with this action of P on Q by conjugation. Choosing a different j amounts to choosing a different generator a for P, and so gives a group isomorphic to G. By definition, this group is non-abelian. In fact it is isomorphic to the subgroup of $\mathrm{Aff}(\mathbb{Z}/(q))$ given above. □

The semidirect product of C_3 and C_4 given by the unique non-trivial homomorphism

$$\theta \colon C_4 \to \mathrm{Aut}(C_3) \cong C_2,$$

namely the one sending a generator of C_4 to the map $a \mapsto a^2$, gives a non-abelian group $C_3 \rtimes_\theta C_4$ of order 12. There are only two more non-abelian groups of order 12, namely the obvious direct product $C_2 \times S_3$, and the alternating group A_4.

PROPOSITION 2.4.15. *There are 5 different groups of order 12, namely C_{12} and $C_2 \times C_6$ and the three non-abelian groups $C_2 \times S_3, A_4$ and $C_3 \rtimes C_4$.*

PROOF. Let G be a group of order 12, and let P be a Sylow 3-subgroup. We may assume that G is non-abelian.

Case 1: Assume that P is not normal. Then P does not contain a non-trivial normal subgroup of G, and so the action on the left cosets

$$\varphi \colon G \to \mathrm{Sym}(G/P) \cong S_4$$

is injective, and its image is a subgroup of order 12 in S_4. By Sylow III, $s_3 = 4$, so that G has exactly 8 elements of order 3. But all elements of S_4 of order 3 are in A_4, and so $\varphi(G)$ intersects A_4 in a subgroup with at least 8 elements.. By Lagrange's Theorem $\varphi(G) = A_4$, and so $G \cong A_4$.

Case 2: Assume that P is normal. Then $G = P \rtimes Q$ with a Sylow 2-subgroup Q of order 4. Either $Q \cong C_4$ or $Q \cong C_2 \times C_2$. In the first case there is a unique non-trivial map $Q \cong C_4 \to \mathrm{Aut}(P) \cong C_2$, and hence we obtain the group $C_3 \rtimes_\theta C_4$ from above. In the second case there are exactly 3 non-trivial homomorphisms $\theta \colon Q \to \mathrm{Aut}(P)$, but the three groups resulting are all isomorphic to $S_3 \times C_2$ with $C_2 \cong \ker(\theta)$. □

REMARK 2.4.16. Note that

$$\mathrm{Aff}(\mathbb{Z}/(6)) \cong D_6 \cong D_3 \times C_2 \cong S_3 \times C_2,$$

and

$$PSL_2(\mathbb{F}_3) \cong A_4.$$

Indeed, $PSL_2(\mathbb{F}_3)$ has no normal Sylow 3-subgroup, and hence is isomorphic to A_4 by the above proof.

PROPOSITION 2.4.17. *Let G be a group of order $2p^n, 4p^n$, or $8p^n$ for an odd prime p. Then G is not simple.*

PROOF. Let $|G| = 2^m p^n$ with $1 \leq m \leq 3$, P be a Sylow p-subgroup of G, and $N = N_G(P)$, so that $s_p = (G : N)$. By Sylow III we have $s_p \mid 2^m$ and $s_p \equiv 1 \bmod p$. If $s_p = 1$, then P is normal and G is not simple. Hence $s_p = 4$ or $s_p = 8$.

Case 1: $s_p = 4$, $m \geq 2$ and $4 \equiv 1 \bmod p$, i.e., $p = 3$. The action by conjugation of G on the set of Sylow 3-subgroups defines a homomorphism $G \to S_4$, which must be injective, because G is simple. Therefore $2^m 3^n = |G| \mid 4!$, and hence $n = 1$. Now a Sylow 2-subgroup Q has index 3, and so we have a homomorphism $\varphi\colon G \to \mathrm{Sym}(G/Q) \cong S_3$. Then $\ker(\varphi)$ is a non-trivial normal subgroup of G, because $|G| = 2^m 3 \geq 12$, and G is not simple.

Case 2: $s_p = 8$, $m = 3$ and $8 \equiv 1 \bmod p$, i.e., $p = 7$. As before we obtain $8p^n = |G| \mid 8!$, hence $n = 1$ and $|G| = 56$, $s_7 = 8$. Therefore G has 48 elements of order 7, and so there can be only one Sylow 2-subgroup, which must be therefore normal. Hence G is not simple. □

CHAPTER 3

Solvable and nilpotent groups

3.1. Subnormal series

DEFINITION 3.1.1. Let G be a group. A chain of subgroups

$$G = G_0 \supseteq G_1 \supseteq \cdots \supseteq G_i \supseteq G_{i+1} \supseteq \cdots \supseteq G_n = 1$$

is called a *subnormal series* if G_i is normal in G_{i-1} for every i. If in addition G_i is normal in G for all i, then it is called a *normal series*.

The quotient groups G_i/G_{i+1} are called the *factors* of the series, and the *length* of the series is the number of strict inclusions. We also write

$$G = G_0 \rhd G_1 \rhd \cdots \rhd G_i \rhd G_{i+1} \rhd \cdots \rhd G_n = 1$$

for a subnormal series. Instead of a descending series, it can be also written as an ascending series

$$1 = G_0 \lhd G_1 \lhd \cdots \lhd G_j \lhd G_{j+1} \lhd \cdots \lhd G_n = G.$$

The only difference is the indexing.

DEFINITION 3.1.2. A subnormal series of a group G is called a *composition series*, if all quotient groups are non-trivial and simple.

In other words, a subnormal series is a composition series if it has no proper *refinement* that is also a subnormal series. Here refinement means that every subgroup in the first series appears as a term in the second (refined) series.

REMARK 3.1.3. Every finite group admits a composition series (usually many): choose G_1 to be a maximal proper normal subgroup of G; then choose G_2 to be a maximal proper normal subgroup of G_1; and continue this way. An infinite group may or may not have a finite composition series. Every simple infinite group S has a finite composition series, namely $S = S_0 \rhd S_1 = 1$. The infinite cyclic group C_∞ has no finite composition series. Any finite series must have cyclic factors, and at least one of the factors must be infinite cyclic, and therefore cannot be simple.

EXAMPLE 3.1.4. 1. *The symmetric group S_3 has a composition series*

$$S_3 \rhd A_3 \rhd 1$$

with factors C_2, C_3.

2. *The symmetric group S_4 has a composition series*

$$S_4 \rhd A_4 \rhd V_4 \rhd \langle (12)(34) \rangle \rhd 1,$$

where $V_4 \cong C_2 \times C_2$ consists of $\{(1), (12)(34), (13)(24), (14)(23)\}$. The factors are C_2, C_3, C_2, C_2.

3. *For $n \geq 5$ the symmetric group S_n has only one composition series, namely*

$$S_n \rhd A_n \rhd 1.$$

The only normal subgroups of S_n are S_n, A_n and 1, see Corollary 1.4.8, and A_n is simple for $n \geq 5$.

The following theorem is the analogue of unique prime factorization for composition series.

THEOREM 3.1.5 (Jordan-Hölder). *Let G be a non-trivial finite group. If*

$$G = G_0 \rhd G_1 \rhd \cdots \rhd G_s = 1,$$
$$G = H_0 \rhd H_1 \rhd \cdots \rhd H_t = 1,$$

are two composition series for G, then $s = t$ and there is a permutation π of $\{1, 2, \ldots, s\}$ such that

$$G_i/G_{i+1} \cong H_{\pi(i)}/H_{\pi(i)+1}$$

for $1 \leq i \leq s$.

PROOF. We use induction on $|G|$. In case that $H_1 = G_1$, we have two composition series for G_1, to which we can apply the induction hypothesis. So we may assume that $H_1 \neq G_1$. Because G_1 and H_1 are both normal in G, the product G_1H_1 is normal in G. It properly contains both G_1 and H_1, which are maximal normal subgroups of G, and so $G = G_1H_1$. Therefore we have

$$G/G_1 = G_1H_1/G_1 \cong H_1/(G_1 \cap H_1) = H_1/K_2, \tag{3.1}$$
$$G/H_1 = G_1H_1/H_1 \cong G_1/(G_1 \cap H_1) = G_1/K_2, \tag{3.2}$$

with $K_2 := G_1 \cap H_1$, which is a maximal normal subgroup in both G_1 and H_1. Choose a composition series

$$K_2 \rhd K_3 \rhd \cdots \rhd K_u = 1.$$

Denote by $Q(G_0 \rhd G_1 \rhd \cdots \rhd G_s)$ the set of factors G_i/G_{i+1}, and write $Q(S) \sim Q(S')$, if one set is a rearrangement of the other. On applying the induction hypothesis to G_1 and H_1 and the composition series

$$G \rhd G_1 \rhd G_2 \rhd G_3 \rhd \cdots \rhd G_s,$$
$$G \rhd G_1 \rhd K_2 \rhd K_3 \rhd \cdots \rhd K_u,$$
$$G \rhd H_1 \rhd H_2 \rhd H_3 \rhd \cdots \rhd G_t,$$

we find that

$$\begin{aligned}
Q(G \rhd G_1 \rhd \cdots \rhd G_s) &= \{G/G_1, G_1/G_2, G_2/G_3, \ldots, G_{s-1}\} \quad \text{(definition)} \\
&\sim \{G/G_1, G_1/K_2, K_2/K_3, \ldots, K_{u-1}\} \quad \text{(induction)} \\
&\sim \{H_1/K_2, G/H_1, K_2/K_3, \ldots, K_{u-1}\} \quad \text{((3.1),(3.2))} \\
&\sim \{G/H_1, H_1/K_2, K_2/K_3, \ldots, K_{u-1}\} \quad \text{(reorder)} \\
&\sim \{G/H_1, H_1/H_2, H_2/H_3, \ldots, H_{t-1}\} \quad \text{(induction)} \\
&= Q(G \rhd H_1 \rhd H_2 \rhd H_3 \rhd \cdots \rhd H_t) \qquad \text{(definition)}.
\end{aligned}$$

□

EXAMPLE 3.1.6. *Consider the following two decomposition series for D_6:*

$$D_6 \rhd \langle r \rangle \rhd \langle r^2 \rangle \rhd 1,$$
$$D_6 \rhd \langle r^3, s \rangle \rhd \langle r^3 \rangle \rhd 1.$$

With the notations of the Jordan-Hölder Theorem we have the isomorphisms

$$H_0/H_1 \cong G_2/G_3 \cong C_3,$$
$$H_1/H_2 \cong G_1/G_2 \cong C_2,$$
$$H_2/H_3 \cong G_0/G_1 \cong C_2.$$

Hence the Theorem applies with $\pi = (13)$.

REMARK 3.1.7. This theorem was proved by Jordan in 1873, in the weaker form that $(G_i : G_{i+1}) = (H_{\pi(i)} : H_{\pi(i)+1})$ for a suitable permutation π. That the quotient groups themselves are isomorphic was proved by Hölder 16 years later.
Roughly speaking, the Jordan-Hölder Theorem says that a group determines its composition series. The converse is not true in general. For example, the non-isomorphic groups D_p and C_{2p} for a prime p both have composition series of the same length with the same factors C_2 and C_p, i.e.,

$$D_p \triangleright \langle r \rangle \triangleright 1, \quad C_{2p} \triangleright C_p \triangleright 1.$$

3.2. Solvable groups

A subnormal series whose factors are all commutative is called a *solvable series*.

DEFINITION 3.2.1. A group G is called *solvable*, if it has a solvable series.

The term "solvable" comes from Galois theory, where it is shown that polynomials in $\mathbb{Q}[x]$ whose roots can be described in terms of nested radicals are precisely those whose Galois groups are solvable groups in the above sense. Speakers of British English use soluble instead of solvable.

EXAMPLE 3.2.2. *The group S_n is solvable for $n \leq 4$.*

This follows from Example 3.1.4.

Consider the subgroups

$$B = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \mid a, d \in K^\times, b \in K \right\}, \quad U = \left\{ \begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix} \mid t \in K \right\}$$

of $GL_2(K)$ for a field K. Then U is a normal subgroup of B, because we have

$$\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}^{-1} = \begin{pmatrix} 1 & \frac{at}{d} \\ 0 & 1 \end{pmatrix},$$

and both $B/U \cong K^\times \times K^\times$ and $U \cong (K, +)$ are abelian. So we have:

EXAMPLE 3.2.3. *The group B is solvable, with solvable series $B \triangleright U \triangleright 1$.*

PROPOSITION 3.2.4. *Every subgroup and every quotient group of a solvable group is solvable.*

PROOF. Let $G \triangleright G_1 \triangleright \cdots \triangleright G_n$ be a solvable series for G, and let H be a subgroup of G. The homomorphism $H \cap G_i \to G_i/G_{i+1}$ given by $x \mapsto xG_{i+1}$ has kernel

$$(H \cap G_i) \cap G_{i+1} = H \cap G_{i+1}.$$

Therefore $H \cap G_{i+1}$ is a normal subgroup of $H \cap G_i$, and the quotient $(H \cap G_i)/(H \cap G_{i+1})$ is abelian, because it injects to G_i/G_{i+1}, which is abelian. Altogether this shows that

$$H \triangleright (H \cap G_1) \triangleright \cdots \triangleright (H \cap G_n)$$

is a solvable series for H.

Let N be a normal subgroup of G. We will construct a solvable series for G/N from the solvable series of G. We have $NG_i \triangleright NG_{i+1}$, since N and G_{i+1} normalize NG_i inside G. We obtain the normal series

$$G = NG_0 \triangleright NG_1 \triangleright \cdots \triangleright NG_n = N.$$

We can reduce this series modulo N to obtain

$$\overline{G} = G/N \triangleright \overline{G}_1 \triangleright \cdots \triangleright \overline{G}_n = \{\overline{1}\},$$

where $\overline{G}_i = (NG_i)/N \cong G_i/(N \cap G_i)$. The natural map $G_i \to \overline{G}_i$ is onto, so the map $G_i \to \overline{G}_i/\overline{G}_{i+1}$ is onto and kills G_{i+1}, so $\overline{G}_i/\overline{G}_{i+1}$ is a quotient group of G_i/G_{i+1} for all i, hence abelian. We have shown that the above series is a solvable series for G/N. □

PROPOSITION 3.2.5. *Let N be a normal subgroup of G and assume that N and G/N are solvable. Then G is solvable.*

PROOF. Let $\overline{G} = G/N$ and

$$\overline{G} \triangleright \overline{G}_1 \triangleright \cdots \triangleright \overline{G}_n = 1,$$
$$N \triangleright N_1 \triangleright \cdots \triangleright N_m = 1$$

be solvable series for $\overline{G}$ and N. Let G_i be the inverse image of $\overline{G}_i$ in G, i.e., with $G_i \mapsto \overline{G}_i$ under the natural map $G \to G/N$. Then we have

$$G_i/G_{i+1} \cong \overline{G}_i/\overline{G}_{i+1},$$

and so

$$G \triangleright G_1 \triangleright \cdots \triangleright G_n = N \triangleright N_1 \triangleright \cdots \triangleright N_m$$

is a solvable series for G. □

COROLLARY 3.2.6. *A finite p-group is solvable.*

PROOF. Let G be a non-trivial p-group. We use induction on the order of G. Since $Z(G)$ is non-trivial by Proposition 2.2.7, the induction hypothesis gives that $G/Z(G)$ is solvable. Clearly $Z(G)$ is solvable, because it is abelian. Then G is solvable by Proposition 3.2.5. □

A solvable group G has a *canonical* solvable series, namely the *derived series*. It is in fact the shortest solvable series for G. Let us recall first that the commutator of two elements x, y in a group G is given by

$$[x, y] := xyx^{-1}y^{-1} = (xy)(yx)^{-1}.$$

Thus $[x, y] = 1$ says that x and y commute, i.e., $xy = yx$.

DEFINITION 3.2.7. Let G be a group. The *derived subgroup*, or *commutator subgroup* of G is the group generated by all commutators of G. It is denoted by G', or by $[G, G]$.

Note that G' need not consist only of commutators. It is only *generated* by commutators.

EXAMPLE 3.2.8. 1. *A group G is abelian if and only if $G' = 1$.*

2. *For $n \geq 3$ we have $D_n' = \langle r^2 \rangle$, where $[r, s] = r(sr^{-1}s^{-1}) = r^2$.*

3. *For $n \geq 5$ we have $A_n' = A_n$, since $[(abd), (ace)] = (abc)$ for distinct a, b, c, d, e, and A_n is generated by all 3-cycles.*

4. *We have $A_4' = V_4$, which is the normal Sylow 2-subgroup of A_4.*

5. *The derived group of Q_8 is $Q_8' = \{\pm 1\} = Z(Q_8)$.*

It turns out that G' is normal in G. Indeed, any automorphism $\varphi \in \mathrm{Aut}(G)$ maps the generating set for G' to G', because of

$$\begin{aligned}\varphi([x,y]) &= \varphi(xyx^{-1}y^{-1}) \\ &= \varphi(x)\varphi(y)\varphi(x)^{-1}\varphi(y)^{-1} \\ &= [\varphi(x),\varphi(y)].\end{aligned}$$

Hence $\varphi(G') \subseteq G'$, and G' is a "characteristic" subgroup. Taking φ inner shows that G' is normal in G.

We remark that a subgroup $H \leq G$ is called *characteristic*, if $\varphi(H) \subseteq H$ for all $\varphi \in \mathrm{Aut}(G)$.

PROPOSITION 3.2.9. *The commutator subgroup G' is the smallest normal subgroup N of G such that G/N is abelian.*

PROOF. We first show that G/G' is abelian. The canonical homomorphism $\pi\colon G \to G/G'$ maps g to $\overline{g} = gG'$. We have

$$[\overline{g},\overline{h}] = \overline{[g,h]} = \overline{1}$$

for all g, h, since $[g,h] \in G'$. Hence all $\overline{g}, \overline{h}$ in G/G' commute.
let N be another normal subgroup of G such that G/N is abelian. Then the image of $[g,h]$ in G/N is trivial again, and so $[g,h] \in N$. Since these elements generate G', we have $N \supseteq G'$. □

EXAMPLE 3.2.10. *For $n \geq 5$ we have $S_n' = A_n$, because A_n is the smallest normal subgroup of S_n with an abelian quotient.*

DEFINITION 3.2.11. The *derived series* of a group G is given by

$$G = G^{(0)} \triangleright G^{(1)} \triangleright G^{(2)} \triangleright \cdots$$

where $G^{(i+1)} = [G^{(i)}, G^{(i)}] = (G^{(i)})'$ for all i.

So we have $G = G^{(0)}$, $G' = G^{(1)}$, $G'' = G^{(2)}$, and so on. This normal series may not end with the trivial group. By Example 3.2.8 and Example 3.2.10 we know that the derived series of S_n is given by

$$S_n \triangleright A_n \trianglerighteq A_n \trianglerighteq \cdots$$

Indeed, it turns out that a group G is solvable if and only if its derived series ends with the trivial group.

PROPOSITION 3.2.12. *A group G is solvable if and only if $G^{(s)} = 1$ for some $s \geq 0$.*

PROOF. If $G^{(s)} = 1$, then the derived series clearly is a solvable series for G. Conversely, let

$$G = G_0 \triangleright G_1 \triangleright \cdots \triangleright G_s = 1$$

be a solvable series for G. Because G/G_1 is abelian, $G_1 \supseteq G'$ by Proposition 3.2.9. Now $G'G_2$ is a subgroup of G_1, and from

$$G'/(G' \cap G_2) \cong G'G_2/G_2 \subseteq G_1/G_2$$

we see that the commutativity of G_1/G_2 implies that $G'/(G' \cap G_2)$ is abelian, and hence that $G'' \subset G' \cap G_2 \subseteq G_2$. Continuing this way, we find that $G^{(i)} \subseteq G_i$ for all i, and hence $G^{(s)} = 1$. □

The second part of the proof shows that the derived series of a solvable group is its shortest normal abelian series.

DEFINITION 3.2.13. The least i such that $G^{(i)}$ is trivial, or equivalently the number of factors in the derived series, is called the *solvable length* (or derived length) of G.

The only group with solvable length 0 is the trivial group. Solvable length 1 means the group is non-trivial and abelian. Solvable length 2 means the group is non-abelian but its commutator subgroup is abelian.

EXAMPLE 3.2.14. 1. *For the Heisenberg group $G = \mathrm{Heis}(R)$ over a commutative ring R with unit, we have $G' = Z(G)$, which is abelian. Hence $G'' = 1$, and its derived series is*

$$G \triangleright G^{(1)} \triangleright G^{(2)} = 1.$$

It has length 2.

2. *For $n \geq 3$ the dihedral group D_n has solvable length* 2*, with derived series $D_n \triangleright \langle r^2 \rangle \triangleright 1$.*

3. *S_4 has solvable length* 3*, with $S_4 \triangleright A_4 \triangleright V_4 \triangleright 1$.*

We want to conclude this section with two famous Theorems on finite solvable groups.

THEOREM 3.2.15 (Burnside 1904). *If $|G| = p^a q^b$ for primes p and q, then G is solvable.*

Burnside's original proof used representation theory. A purely group-theoretic proof of the Theorem was found in the early 1970s. The next Theorem is the deepest result about solvability of finite groups and illustrates the special role of the prime 2 in finite group theory.

THEOREM 3.2.16 (Feit-Thompson 1963). *Every finite group of odd order is solvable.*

The proof is 255 pages long and occupies an entire volume of the Pacific Journal of Mathematics [**6**].

3.3. Nilpotent groups

DEFINITION 3.3.1. An ascending series

$$1 = G_0 \subseteq G_1 \subseteq G_2 \subseteq \cdots \subseteq G_n = G$$

is called an *ascending central series* for G if $G_i \trianglelefteq G$ and $G_{i+1}/G_i \subseteq Z(G/G_i)$ for all i. A descending series

$$G = G_0 \supseteq G_1 \supseteq G_2 \supseteq \cdots \supseteq G_n = 1$$

is called a *descending central series* for G if $G_i \trianglelefteq G$ and $G_i/G_{i+1} \subseteq Z(G/G_{i+1})$ for all i.

We need $G_i \trianglelefteq G$ to make sense of G/G_i as a group. Note that it implies that G_i is normal in G_{i+1} for all i.

DEFINITION 3.3.2. The ascending series

$$1 \subseteq Z_1(G) \subseteq Z_2(G) \subseteq \cdots$$

defined by $Z_1(G) = Z(G)$ and $Z_i(G)$ recursively defined by

$$Z_{i+1}(G)/Z_i(G) = Z(G/Z_i(G))$$

for all $i \geq 0$ is called the *upper central series* for G, if it terminates in G. The descending series

$$G^0 = G \supseteq G^1 \supseteq G^2 \supseteq \cdots$$

defined by $G^0 = G$ and $G^{i+1} = [G, G_i] = [G_i, G]$ for all $i \geq 0$, is called the *lower central series* for G if it terminates in 1.

Here $g \in Z_{i+1}(G)$ if and only if $[g, x] \in Z_i(G)$ for all $x \in G$.
One has to check that both series, if they terminate, are indeed central series. This is clear for the upper central series, because the center of a group is a normal subgroup, so that

$$Z_{i+1}(G)/Z_i(G) = Z(G/Z_i(G)) \trianglelefteq G/Z_i(G),$$

so that $Z_{i+1} \trianglelefteq G$ for all i. Furthermore the second requirement is satisfied by definition. For the lower central series it follows from the next Lemma.

LEMMA 3.3.3. *Let G be a group.*

(1) *If $H \leq G$ then $H^i \leq G^i$ for all $i \geq 0$.*
(2) *If $\varphi\colon G \to K$ is a surjective homomorphism, then $\varphi(G^i) = K^i$ for all $i \geq 0$.*
(3) *G^i is a characteristic subgroup of G for all $i \geq 0$, hence $G_i \trianglelefteq G$.*
(4) *We have $G^i/G^{i+1} \subseteq Z(G/G^{i+1})$ for all $i \geq 0$.*

PROOF. (1): we use induction on i. We have $H^0 = H \leq G = G^0$. If we assume $H^i \leq G^i$, then this together with $H \leq G$ gives

$$[H^i, H] = H^{i+1} \leq G^{i+1} = [G^i, G].$$

(2): we use induction on i. We have $\varphi(G^0) = \varphi(G) = K = K^0$. Suppose that $\varphi(G^i) = K^i$. If $x \in G^i$ and $y \in G$, then

$$\varphi([x, y]) = [\varphi(x), \varphi(y)] \in [\varphi(G^i), \varphi(G)] = [K^i, K] = K^{i+1},$$

so $\varphi(G^{i+1}) = \varphi([G^i, G]) = K^{i+1}$. On the other hand, if $a \in K^i$ and $b \in K$, then $a = \varphi(x)$ and $b = \varphi(y)$ for some $x \in G^i$ and $y \in G$. So

$$[a, b] = [\varphi(x), \varphi(y)] = \varphi([x, y]) \in \varphi([G^i, G]) = \varphi(G^{i+1}).$$

Thus $K^{i+1} = [K^i, K] \leq \varphi(G^{i+1})$. Together we have $\varphi(G^{i+1}) = K^{i+1}$.

(3): If $\varphi \in \mathrm{Aut}(G)$, then φ is surjective so that $\varphi(G^i) = G^i$ by (2).

(4): If $x \in G^i$ and $y \in G$, then $[x, y] \in G^{i+1}$, so $G^{i+1}x$ and $G^{i+1}y$ commute for all such x and y, thus $G^i/G^{i+1} \subseteq Z(G/G^{i+1})$ for all $i \geq 0$. □

LEMMA 3.3.4. *Let*

$$G = G_0 \supseteq G_1 \supseteq G_2 \supseteq \cdots \supseteq G_n = 1$$

be a central series for G. Then we have for all $i \geq 0$,

$$G^i \leq G_i, \quad Z_i(G) \geq G_{n-i}.$$

PROOF. This can be proved by induction on i. We will leave this to the reader. □

PROPOSITION 3.3.5. *The following conditions are equivalent for a group G:*

(1) *$G^c = 1$ for some $c \geq 0$.*
(2) *$Z_c(G) = G$ for some $c \geq 0$.*
(3) *G has a central series.*

PROOF. If G has a central series (G_i) of length n, then

$$G^n \leq G_n = 1, \quad Z_n(G) \geq G_0 = G.$$

Hence (3) implies both (1) and (2). If $Z_c(G) = G$, then the upper central series is a central series, so that (2) implies (3). If $G^c = 1$ for some $c \geq 0$, then the lower central series is a central series by Lemma 3.3.3, hence (1) implies (3). □

Note that we have $G^c = 1$ if and only if $Z_c(G) = G$.

DEFINITION 3.3.6. A group G is called *nilpotent*, if it satisfies one of the three properties of Proposition 3.3.5. The least integer c then is called the *nilpotency class* of G.

Only the trivial group 1 has class 0, and the groups of class 1 are exactly the abelian groups. A group G is nilpotent of class 2 if and only if $G/Z(G)$ is abelian and non-trivial.

REMARK 3.3.7. Let G be a non-trivial nilpotent group. Then $Z(G)$ is non-trivial, because otherwise there is no c such that $Z_c(G) = G$.

PROPOSITION 3.3.8. *Every nilpotent group is solvable.*

PROOF. A normal series that is central is abelian, so nilpotency implies solvability. Alternatively, $G^{(i)} \leq G^i$ for all $i \geq 0$, so that $G^c = 1$ implies $G^c = 1$. □

The converse of this result is not true.

EXAMPLE 3.3.9. *Let $n \geq 3$ be an* odd *integer. Then D_n is solvable, but not nilpotent.*

For odd $n \geq 3$ we have $D_n^i = \langle r \rangle$ for all $i \geq 3$. Hence there is no c such that $D_n^c = 1$. Actually it turns out that D_n is nilpotent if and only if n is a power of 2.

PROPOSITION 3.3.10. *Every group of order p^3 for a prime p is nilpotent of class $c \leq 2$.*

PROOF. If G is abelian, then $c = 1$. If G is non-abelian then $G' = Z(G)$ and $|Z(G)| = p$ by Proposition 3.2.9 and Proposition 2.2.10. Hence $G'' = 1$. □

In particular, $Q_8, D_4, \mathrm{Heis}(\mathbb{Z}/(p))$ and $\Gamma(p)$ are nilpotent of class 2.

PROPOSITION 3.3.11. *Every finite p-group is nilpotent.*

PROOF. Let $|G| = p^n$. We use induction on n. For $n = 0$, G is trivial, and hence nilpotent. Otherwise we have $Z(G) \neq 1$ by Remark 3.3.7. Hence $G/Z(G)$ is a p-group of smaller order, so that by induction it is nilpotent, say $(G/Z(G))^c = 1$. Denote by π the natural homomorphism $\pi\colon G \to G/Z(G)$. By Lemma 3.3.3, part (2), we have

$$\pi(G^c) = (G/Z(G))^c = 1.$$

Hence $G^c \leq \ker(\pi) = Z(G)$. Thus

$$G^{c+1} = [G^c, G] \leq [Z(G), G] = 1.$$

□

PROPOSITION 3.3.12. *Subgroups and homomorphic images (hence also quotients) of nilpotent groups are nilpotent.*

PROOF. Let G be nilpotent with $G^c = 1$, and $H \leq G$. Then $H^c \leq G^c = 1$ by Lemma 3.3.3, part (1). Hence $H^c = 1$ and H is nilpotent. Let $\varphi\colon G \to K$ be a surjective homomorphism. Then $K^c = \varphi(G^c) = \varphi(1) = 1$ by Lemma 3.3.3, part (2). □

REMARK 3.3.13. Note that if N and G/N are nilpotent, G need not be nilpotent. For $G = S_3$ and $N = A_3$ we have that A_3 and S_3/A_3 are abelian, hence nilpotent. But S_3 is not nilpotent, because $Z(S_3) = 1$. Another example is $G = D_n$ and $N = \langle r \rangle$ for $n \geq 3$ odd, see Example 3.3.9.

The next result gives a setting where nilpotency of N and G/N implies nilpotency of G.

PROPOSITION 3.3.14. *Let N be a normal subgroup of G such that $N \subseteq Z_i(G)$ for some $i \geq 0$. If G/N is nilpotent, then G is nilpotent.*

PROOF. Let $Z_i = Z_i(G)$. Now G/Z_i is nilpotent by Proposition 3.3.12, since it is a quotient of G/N. We see that

$$Z_i/Z_i \subseteq Z_{i+1}/Z_i \subseteq Z_{i+2}/Z_i \subseteq \cdots \subseteq G/Z_i$$

is the upper central series for G/Z_i. Because G/Z_i is nilpotent we must have $Z_j/Z_i = G/Z_i$ for some $j \geq i$, so $Z_j = G$ for some j. Thus G is nilpotent. □

Note that Z_i is nilpotent, so that $N \subseteq Z_i$ is also nilpotent. So the nilpotency of N is included in the assumptions as well.

LEMMA 3.3.15. *Let G be a finite group and P a Sylow p-subgroup. Let $H \leq G$ with $H \supseteq N_G(P)$. Then $N_G(H) = H$. In particular we have $N_G(N_G(P)) = N_G(P)$.*

PROOF. Let $g \in N_G(H)$. Then $gHg^{-1} = H$, and $H \supseteq gPg^{-1} = Q$. The group Q is a Sylow p-subgroup of H. By Sylow II we have $hQh^{-1} = P$ for some $h \in H$, and hence

$$(hg)P(hg)^{-1} = h(gPg^{-1})h^{-1} \subseteq P.$$

It follows that $hg \in N_G(P) \subseteq H$, so that $g \in H$. This shows $N_G(H) \subseteq H \subseteq N_G(H)$. □

We obtain another characterization of finite nilpotent groups.

PROPOSITION 3.3.16. *Let G be a finite group. The following conditions on G are equivalent.*

1. *G is nilpotent.*
2. *For every proper subgroup H of G we have $N_G(H) \neq H$.*
3. *Every Sylow subgroup of G is normal.*
4. *G is a direct product of its Sylow subgroups.*

PROOF. (1) $\Rightarrow$ (2) : Let H be a proper subgroup of G, and $n \geq 0$ the largest integer with $Z_n(G) \subseteq H$, and $Z_0(G) = 1$. Because G is nilpotent, there is an $a \in Z_{n+1}(G)$ with $a \notin H$. For each $h \in H$ the cosets $aZ_n(G)$ and $hZ_n(G)$ commute in $G/Z_n(G)$, so that

$$aha^{-1}h^{-1} \in Z_n(G) \subseteq H,$$

and hence $aha^{-1} \in H$. Thus $a \in N_G(H) \setminus H$ and $N_G(H) \neq H$.

(2) $\Rightarrow$ (3) : Let P be a Sylow p-subgroup of G. We have $N_g(N_G(P)) = N_G(P)$ by Lemma 3.3.15. Hence (2) implies that $N_G(P)$ is not a proper subgroup of G, i.e., we have $N_G(P) = G$ and P is normal.

(3) $\Rightarrow$ (4) : This has been shown in Corollary 2.3.14.

(4) $\Rightarrow$ (1) : Each Sylow subgroup is a p-group and hence nilpotent by Proposition 3.3.11. Then $G = P_1 \times \cdots \times P_n$ is the direct product of nilpotent groups, and hence nilpotent: it is easy to see that

$$Z_m(G) = Z_m(P_1) \times \cdots \times Z_m(P_n)$$

for all $m \geq 0$. Now choose m large enough such that $Z_m(P_i) = P_i$ for all i. Then $Z_m(G) = G$, and G is nilpotent. □

COROLLARY 3.3.17. *Let G be a nilpotent group of order n. Then G has a subgroup of order d for every positive divisor $d \mid n$.*

PROOF. Let $d = p_1^{e_1} \cdots p_k^{e_k}$ be the prime decomposition of the divisor d. For each factor $p_i^{e_i}$ there is a Sylow p-subgroup of order $p_i^{e_i}$. The product of these subgroups has order d, because G is the direct product of its Sylow subgroups. □

In other words, finite nilpotent groups satisfy the converse of Lagrange's Theorem. We finish this section by introducing the Frattini subgroup, which is of significance in many parts of group theory.

DEFINITION 3.3.18. The *Frattini subgroup* $\Phi(G)$ of a group G is the intersection of all of its maximal subgroups.

If G is an infinite group with no maximal subgroups, then $\Phi(G) = G$.

LEMMA 3.3.19 (Frattini's argument). *Let H be a normal subgroup of a finite group G, and let P be a Sylow p-subgroup of H. Then $G = H \cdot N_G(P)$.*

PROOF. Let $g \in G$. Then $gPg^{-1} \subseteq gHg^{-1} = H$, and both gPg^{-1} and P are Sylow p-subgroups of H. According to Sylow II, there is an $h \in H$ such that $gPg^{-1} = hPh^{-1}$, and it follows that $h^{-1}g \in N_G(P)$ amd so $g \in H \cdot N_G(P)$. □

We obtain the following result characterizing finite nilpotent groups.

PROPOSITION 3.3.20. *A finite group is nilpotent if and only if every maximal proper subgroup is normal.*

PROOF. Let G be nilpotent, and H be a proper subgroup of G. By Proposition 3.3.16, part (2) we have $H \subsetneqq N_G(H)$. If H is maximal, then this implies $N_G(H) = G$, so that H is normal in G.
Conversely, suppose every maximal proper subgroup of G is normal. We will show that all Sylow subgroups are normal, and hence G is nilpotent by Proposition 3.3.16, part (3). Assume that a Sylow subgroup P is not normal in G. Then there exists a maximal proper subgroup $H \subsetneqq G$ containing $N_G(P)$. Being maximal, H is normal, and so Frattini's argument shows that $G = H \cdot N_G(P) = H$, which is a contradiction. □

PROPOSITION 3.3.21. *Let G be a finite group. The Frattini subgroup $\Phi(G)$ is nilpotent.*

PROOF. Let P be a Sylow subgroup of $\Phi(G)$. We will show that P is normal, so that G is nilpotent by Proposition 3.3.16, part (3). Frattini's argument gives $G = \Phi(G) \cdot N_G(P)$. If $N_G(P) \neq G$ then there is a maximal proper subgroup M of G with $N_G(P) \subseteq M \subsetneqq G$. By definition $\Phi(G) \leq M$. Hence

$$\Phi(G) \cdot N_G(P) \subseteq M \subsetneqq G,$$

contrary to the above. Therefore $N_G(P) = G$ and P is normal in G, and hence also normal in $\Phi(G)$. □

REMARK 3.3.22. Let G be a finite group. One can show that the following conditions on G are equivalent.

(1) G is nilpotent.
(2) $G' \leq \Phi(G)$.
(3) $G/\Phi(G)$ is nilpotent.

3.4. Lagrangian groups

Since the converse of Lagrange's theorem is false in general, one might ask which finite groups satisfy the converse, and which groups do not. Let us say that a group G is Lagrangian if it does satisfy the converse Lagrange theorem.

DEFINITION 3.4.1. A finite group G is called *Lagrangian* if and only if for each positive divisor d of $|G|$ there exists at least one subgroup $H \leq G$ with $|H| = d$.

We have already seen that finite nilpotent groups are Lagrangian.

PROPOSITION 3.4.2. *Finite nilpotent groups are Lagrangian.*

Lagrangian groups are related to a special type of solvability.

DEFINITION 3.4.3. A group G is called *supersolvable* if it has a normal series with cyclic factors.

Clearly supersolvable groups are solvable, but the converse need not be true.

EXAMPLE 3.4.4. 1. *The group A_4 is solvable but not supersolvable.*

2. *All dihedral groups D_n are supersolvable.*

In fact, A_4 has no cyclic normal subgroup, so there is no way it can have a normal series where all successive quotients are cyclic. The factors of its derived series for D_n are C_2 and C_n, hence cyclic.

The class of Lagrangian groups lies between the class of supersolvable and solvable groups, see [**3**].

THEOREM 3.4.5. *Lagrangian groups have the following properties.*

(1) *Every Lagrangian group is solvable.*
(2) *Every supersolvable group is Lagrangian.*

The inclusions are strict. In fact, every group $G = A_4 \times H$ with a group H of odd order is solvable, but not Lagrangian; and for any Lagrangian group G, the group $(A_4 \times C_2) \times G$ is Lagrangian, but not supersolvable. Let us show that A_4 is not Lagrangian. This is the classical counterexample to Lagrange's Theorem.

LEMMA 3.4.6. *Let H be a subgroup of G with $(G : H) = 2$. Then $g^2 \in H$ for all $g \in G$.*

PROOF. We have $G = H \cup aH$ for all $a \in G \setminus H$. Thus a^2H has to be H or aH. The second case is impossible since $a^2H = aH$ would imply $aH = H$, and hence $a \in H$; a contradiction. Hence $a^2H = H$. Since $h^2H = H$ anyway for all $h \in H$, it follows that $g^2H = H$ for all $g \in G$. This is the claim. □

PROPOSITION 3.4.7. *The group A_4 of order 12 has no subgroup of order 6. Hence A_4 is not Lagrangian.*

PROOF. Assume that $H \leq A_4$ is a subgroup with $|H| = 6$. Let g be any 3-cycle in A_4. Then $g^2 \in H$ by the Lemma. Furthermore $g^3 = e$, so that $g = g^4 = (g^2)^2 \in H$. But there are eight 3-cycles in A_4, so that $|H| \geq 9$, a contradiction. □

PROPOSITION 3.4.8. *The group A_5 of order 60 has no subgroup of order 30. Hence A_5 is not Lagrangian.*

PROOF. Assume that $H \leq A_5$ is a subgroup with $|H| = 30$. Then there exists a 3-cycle g which is not in H, because otherwise H would contain all 3-cycles which generate A_5, so that $H = A_5$, a contradiction. But as before $g^2 \in H$ so that $g^4 = g \in H$, a contradiction. □

REMARK 3.4.9. In fact, no group S_n or A_n with $n \geq 5$ is Lagrangian. This follows from the fact that A_n and S_n are not solvable for $n \geq 5$.

Another condition for a group to be Lagrangian is the index of the center. We have the following result, see [**4**].

PROPOSITION 3.4.10. *If $(G : Z(G)) < 12$ then G is supersolvable, hence Lagrangian.*

The group A_4 shows that the above result is best possible. We have $(A_4 : Z(A_4)) = 12$.

PROPOSITION 3.4.11. *If $|G|$ is odd and $(G : Z(G)) < 75$ then G is supersolvable, hence Lagrangian.*

There is exactly one non-abelian group G_{75} of order $75 = 3 \cdot 5^2$. It has trivial center, and no subgroup of order 15. Hence it is not Lagrangian. This shows that the above result is best possible.

In [**4**] the following result is shown:

PROPOSITION 3.4.12. *If $|[G, G]| < 4$, then G is supersolvable, hence Lagrangian.*

Again A_4 shows that this result is best possible.

PROPOSITION 3.4.13. *If $|G|$ is odd and $|[G, G]| < 25$, then G is supersolvable, hence Lagrangian.*

In fact, $[G_{75}, G_{75}] \simeq C_5 \times C_5$ has order 25, so that this result is best possible.

Denote the number of different conjugacy classes of G by $k(G)$.

PROPOSITION 3.4.14. *If $\frac{k(G)}{|G|} > \frac{1}{3}$, then G is supersolvable, hence Lagrangian.*

Because of $\frac{k(A_4)}{|A_4|} = \frac{1}{3}$ the result is best possible. It means that if the average size of a conjugacy class of G is less than 3, then G is Lagrangian.

PROPOSITION 3.4.15. *If $|G|$ is odd and $\frac{k(G)}{|G|} > \frac{11}{75}$, then G is supersolvable, hence Lagrangian.*

In fact, $\frac{k(G_{75})}{|G_{75}|} = \frac{11}{75}$, so that the result is best possible.

Finally, let us mention a result of Pinnock (1998), which is related to Burnside's $p^a q^b$-theorem on the solvability of groups of such order.

PROPOSITION 3.4.16. *Let G be a group of order pq^b with primes p, q satisfying $q \equiv 1 \bmod p$. Then G is supersolvable, hence Lagrangian.*

CHAPTER 4

Free groups and presentations

In combinatorial group theory one describes groups by *generators* and *defining relations*, which give a *presentation*. If a group is given by a presentation, then there hold no other relations except the given ones and those implied by the group actions. For example, D_n has generators r and s, and defining relations $r^n = s^2 = e$ and $srs^{-1} = r^{-1}$. Hence a presentation of D_n would be

$$D_n = \langle r, s \mid r^n = s^2 = e, srs^{-1} = r^{-1} \rangle.$$

Presentations turn out to be very useful for describing many groups, but they also have disadvantages. In general it is impossible to analyze a group by a presentation. For example we cannot decide whether or not a group given by a presentation is finite, trivial or even abelian. It has been proven that there are no algorithms to decide this. In some cases it is possible, but difficult and not obvious at all. For example, it is known that the so-called *Wicks group*

$$\langle x, y \mid x^3y^4x^5y^7 = x^2y^3x^7y^8 = e \rangle$$

is isomorphic to C_{11}. On the other hand, without context it may be difficult to recognize well-known groups from one of its presentations. The group

$$\langle a, b \mid a^3 = b^2 = e \rangle$$

is in fact isomorphic to the *modular group* $PSL_2(\mathbb{Z})$. This is an infinite group. One can choose

$$a = \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix}, \; b = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

The *Tits group* is given in terms of generators and relations by

$$\langle a, b \mid a^2 = b^3 = (ab)^{13} = [a, b]^5 = [a, bab]^4 = (abababab^{-1})^6 = e \rangle.$$

It is a finite simple group of order

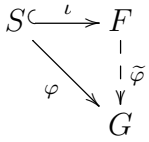
$$2^{11} \cdot 3^3 \cdot 5^2 \cdot 13 = 17971200.$$

Of course, we need to define presentations in terms of generators and relations more formally. For this we need to discuss free groups first.

4.1. Free groups

In most algebraic contexts a free object is an object which has a free basis.

Definition 4.1.1. A subset S of a group F is said to be a *free basis* for F, if every function $\varphi\colon S \to G$ to a group G can be extended uniquely to a homomorphism $\widetilde{\varphi}\colon F \to G$, such that $\widetilde{\varphi}(s) = \varphi(s)$ for all $s \in S$. A group F is said to be a *free group* if there is some subset which is a free basis for F.



The diagram commutes, i.e., we have $\varphi = \widetilde{\varphi} \circ \iota$. We shall see later that S must generate F, so that we will also say that F is *freely generated* by S.

EXAMPLE 4.1.2. 1. *The infinite cyclic group* $C_\infty = \langle a \rangle = \{a^j \mid j \in \mathbb{Z}\}$ *is a free group with free basis* $S = \{a\}$.

2. *The trivial group is a free group with the empty subset as free basis.*

3. *Not all groups are free. The additive groups* $\mathbb{Z}/n\mathbb{Z}$ *are not free for* $n \geq 2$.

If $\varphi\colon S \to G$ is any function, say $\varphi(a) = g \in G$ then φ extends uniquely to a homomorphism $\widetilde{\varphi}\colon C_\infty \to G$ by defining $\widetilde{\varphi}(a^j) = g^j$ for all $j \in \mathbb{Z}$. Note that C_∞ has another free basis, namely $S = \{a^{-1}\}$, but no other ones.
Assume that $\mathbb{Z}/n\mathbb{Z}$ is free with free basis S. Then S is non-empty because of $n \geq 2$. Let $x \in S$ and consider the map sending x to $1 \in G = \mathbb{Z}$. It cannot be extended to a group homomorphism from $\mathbb{Z}/n\mathbb{Z}$ to $\mathbb{Z}$, because every such homomorphism maps $\mathbb{Z}/n\mathbb{Z}$ to zero.

By a *word on* S we mean an expression of the form

$$a_1^{e_1} \cdots a_k^{e_k}$$

with $a_i \in S$ and $e_i = \pm 1$. A word on S is said to be (freely) *reduced* if it does not contain a subword of the form aa^{-1} or of the form $a^{-1}a$; such substrings are called *inverse pairs* of generators. If we start with any word w by successively canceling inverse pairs we arrive in a finite number of steps at a freely reduced word w' which we call a *reduced form* of w. We write $w \equiv w'$. There can be several different ways to proceed with the cancellations, but one can show that end result w' does not depend on the order in which the inverse pairs are removed:

LEMMA 4.1.3. *There is only one reduced form of a given word* w *on* S.

PROOF. We use induction on the length of w as a string of symbols in S, or slightly different, in $S \cup S^{-1}$. If w is reduced there is nothing to show. So suppose $w \equiv uxx^{-1}v$ and focus on this particular occurrence of an inverse pair which we distinguish by underlining as in $u\underline{xx^{-1}}v$. If we can show that every reduced form w' of w can be obtained by canceling this occurrence first, then the Lemma will follow by induction on the shorter word uv thus obtained.
Let w' be a reduced form of w. We know that w' is obtained by some sequence of cancellations. First suppose that the pair xx^{-1} itself we are focusing on is canceled at some step in this sequence. Then we can clearly rearrange the order so that this particular pair is canceled first. So this case is settled. Now xx^{-1} cannot remain in w' so at least one of these two symbols x and x^{-1} must be canceled at some step. The first cancellation must then look like $u_1\underline{x^{-1}x}x^{-1}v_1 \Rightarrow u_1x^{-1}v_1$ or $u_1x\underline{x^{-1}x}v_1 \Rightarrow u_1xv_1$. But in either case, the word obtained by cancellation is the same as that obtained by canceling the original pair. So we may cancel the original pair at this stage instead. Hence we are back in the first case and the Lemma is proved. □

We are now ready to define the free group F_S with free basis S.

PROPOSITION 4.1.4. *If* S *is any set, there is a free group* F_S *having* S *as a free basis.*

PROOF. Let F_S be the set of freely reduced words on S, including the empty word denoted by 1. Multiplication in F_S is defined by concatenation (also called juxtaposition). It is straightforward to check the group axioms. The empty word is the identity, and the inverse of $a_1^{e_1} \cdots a_k^{e_k}$ is $a_k^{-e_k} \cdots a_1^{-e_1}$. The associative law follows from the fact that the reduction of a word is independent of the order in which inverse pairs are removed. To see that F_S is free, consider any function $\varphi\colon S \to G$, where G is a group. We define

$$\widetilde{\varphi}(a_1^{e_1} \cdots a_k^{e_k}) = \varphi(a_1)^{e_1} \cdots \varphi(a_k)^{e_k}.$$

This map is the unique homomorphism extending φ. □

Note that this free group F_S is unique up to isomorphism. The proof consists of the standard *universal-property-yoga*, using the universal property of free groups in the definition.

COROLLARY 4.1.5. *Every group is a quotient group of a free group. Thus if G is a group there is a free group F and a normal subgroup N such that $G \cong F/N$.*

PROOF. Choose $S = G$ and $\varphi = \mathrm{id}$. Then φ extends uniquely to a homomorphism $\widetilde{\varphi}\colon F_G \to G$ with kernel N. Since φ is bijective, $\widetilde{\varphi}$ is surjective, and we have $G \cong F/\ker(\widetilde{\varphi}) = F/N$. □

Let us write $u =_G v$ if the words u and v are equal as group elements in G. Free groups with basis S are indeed generated by S.

PROPOSITION 4.1.6. *Let G be a group, and S a subset of G. Then G is free with basis S if and only if the following conditions hold:*

1. *S generates G.*
2. *If w is a word on S and $w =_G e$, then w is not freely reduced, that is w must contain an inverse pair.*

PROOF. Suppose that G is free. The free group F_S constructed in Proposition 4.1.4 is generated by S by definition. It is also unique. Hence we have $G \cong F_S$, and (1) is proved. It is also easy to see that (2) is satisfied. Conversely, assume that (1) and (2) hold. If $u =_G v$, and u and v are freely reduced, then uv^{-1} contains an inverse pair by (2). Hence the last symbol of u is the same as the last symbol of v. So inductively u and v must be identical. Thus different freely reduced words represent different elements of G. Hence the obvious extension of the identity on S is an isomorphism from F_S onto G, and G is free. □

PROPOSITION 4.1.7. *Let G be a free group with basis S and let S' be another basis. Then $|S| = |S'|$.*

PROOF. Any map from S to $\mathbb{Z}/2\mathbb{Z}$ uniquely extends to a homomorphism of G into $\mathbb{Z}/2\mathbb{Z}$. Moreover, every homomorphism $G \to \mathbb{Z}/2\mathbb{Z}$ can be obtained in this way (every homomorphism is completely defined by its values on a given generating set). Hence there are exactly $2^{|S|}$ different homomorphism from G into $\mathbb{Z}/2\mathbb{Z}$. This implies that

$$2^{|S|} = 2^{|S'|},$$

and then $|S| = |S'|$. □

COROLLARY 4.1.8. *Let S and S' be sets. Then $F_S \cong F_{S'}$ if and only if $|S| = |S'|$.*

DEFINITION 4.1.9. Let G be a free group on S. Then the cardinality of S is called the *rank* of G.

By Proposition 4.1.7 the cardinality of a basis of a free group G is an invariant of G which characterizes G uniquely up to an isomorphism. Hence the rank is well-defined.

DEFINITION 4.1.10. Let $n \in \mathbb{N}$. We denote by F_n the free group of rank n.

Note that F_1 is isomorphic to $\mathbb{Z}$, and hence abelian. All groups F_n for $n \geq 2$ are non-abelian. Indeed, if S has more than one element, then F_S is not abelian, and in fact the center of F_S is trivial.

LEMMA 4.1.11. *Let $n \leq m$. Then F_n is embeddable into F_m.*

PROOF. If $S \subseteq S'$, then the subgroup $\langle S \rangle$ generated by S in $F_{S'}$ is itself a free group with basis S. □

The next result shows that in some sense the reverse is also true for free groups of finite or countable infinite rank.

PROPOSITION 4.1.12. *Any countable free group G is embeddable into F_2.*

PROOF. To prove the result it suffices to find a free subgroup of countable rank in F_2. Let a, b be a basis of F_2 and put

$$x_n = b^{-n}ab^n$$

for all $n \geq 0$. Let $X = \{x_0, x_1, \ldots\}$. We claim that X freely generates the subgroup $\langle X \rangle$ in F_2. Indeed, let $w = x_{i_1}^{e_1} \cdots x_{i_n}^{e_n}$ be a reduced non-empty word in $X \cup X^{-1}$. Then w can also be viewed as a word in $\{a, b\}$:

$$w = b^{-i_1}a^{e_1}b^{i_1} \cdots b^{-i_n}a^{e_n}b^{i_n}.$$

Now w is reduced in X, so that any reduction of w as word on $\{a, b\}$ does not affect a^{e_j} and $a^{e_{j+1}}$ in the subword

$$b^{-i_j}a^{e_j}b^{i_j} \cdot b^{-i_{j+1}}a^{e_{j+1}}b^{i_{j+1}}.$$

Hence the literals a^{e_j} and $a^{e_{j+1}}$ are present in the reduced form of w as a word in $\{a, b\}$. Hence the reduced form of w is non-empty, so $w \neq_{F_2} e$. By Proposition 4.1.6, $\langle X \rangle$ is free. It clearly has countable rank. □

REMARK 4.1.13. Note that subspaces of vector spaces cannot have bigger dimension than the ambient space. The free group F_2 however contains subgroups that are isomorphic to free groups of higher rank, even countable infinite rank.

An important result on free groups is the Theorem of Nielsen and Schreier.

THEOREM 4.1.14 (Nielsen-Schreier). *Subgroups of free groups are free. In case G is a free group on n generators, and H is a subgroup of finite index e, then H is free of rank*

$$1 + e(n - 1).$$

Nielsen proved this in 1921 for finitely generated subgroups, and in fact gave an algorithm for deciding whether a word lies in the subgroup, and Schreier proved the general case in 1927. Nowadays there are several proofs available, the most elegant ones using topology, and in particular covering spaces – see Serre 1980.

4.2. Presentations by generators and relations

Free groups enable us to generate generic groups over a given set; in order to force generators to satisfy a given list of group theoretic equations, we divide out a suitable normal subgroup.

DEFINITION 4.2.1. Let G be a group and S a subset of G. The *normal subgroup of G generated by S* is the smallest normal subgroup of G containing S. It is denoted by N_S.

DEFINITION 4.2.2. Let S be a set, $R \subseteq S \cup S^{-1}$, F_S be the free group generated by S, and N_R be the normal subgroup of F_S generated by R. Then the group

$$\langle S \mid R \rangle = F_S/N_R$$

is said to be generated by S with the relations R. If G is a group with $G \cong \langle S \mid R \rangle$, then $\langle S \mid R \rangle$ is called a *presentation of G*.

EXAMPLE 4.2.3. 1. *$\langle a \mid \emptyset \rangle$ is a presentation of the infinite cyclic group.*

2. *$\langle a, b \mid a^{-1}bab^{-2} = b^{-1}aba^{-2} = e \rangle$ is a presentation of the trivial group.*

3. *The group given by $\langle a, b \mid ababa = e \rangle$ is abelian.*

For 2. note that $a^{-1}ba = b^2$ and $b^{-1}ab = a^2$, so that

$$a = a^{-1}a^2 = a^{-1}b^{-1}ab = (a^{-1}ba)^{-1}b = b^{-2}b = b^{-1},$$

so that $a^2 = b^{-1}ab = a^2b$ and hence $b = a = 1$. For 3. we compute

$$\begin{aligned} e &= ababa \\ &= (ba)(ababa)(ba)^{-1} \\ &= baaba. \end{aligned}$$

It follows that

$$\begin{aligned} e &= (baaba)(ababa)^{-1} \\ &= ba(abaa^{-1}b^{-1}a^{-1})b^{-1}a^{-1} \\ &= bab^{-1}a^{-1}. \end{aligned}$$

Hence the group is abelian. It is in fact the infinite cyclic group as we shall see.

PROPOSITION 4.2.4. *Let $G = \langle S \mid R \rangle$ and suppose that $\psi \colon S \to H$ is a function, where H is a group. Then ψ extends to a homomorphism $\psi \colon G \to H$ if and only if $\overline{\psi}(r) =_H e$ for all $r \in R$, where $\overline{\psi}$ is the formal extension of ψ to all words.*

PROOF. We have $G \cong F_S/N_R$. The original ψ extends to a homomorphism if and only if $N_R \subseteq \ker(\overline{\psi})$. Hence ψ extends to a homomorphism if and only if $\overline{\psi}(r) =_H e$ for all $r \in R$. □

EXAMPLE 4.2.5. *The group $G = \langle a, b \mid ababa = e \rangle$ is isomorphic to C_∞.*

We have $C_\infty \cong C = \langle t \mid \rangle$. Define ψ by $\psi(a) = t^{-2}$ and $\psi(b) = t^3$. Does ψ extend to a homomorphism ? We compute that

$$\overline{\psi}(ababa) = t^{-2}t^3t^{-2}t^3t^{-2} =_C e.$$

Hence, by Proposition 4.2.4 ψ extends to a homomorphism. Also the function φ defined on $\{t\}$ by $\varphi(t) = ab$ uniquely extends to a homomorphism $\varphi\colon C \to G$, because C is free with basis $\{t\}$. We have $\varphi \circ \psi = \psi \circ \varphi = \mathrm{id}$, because

$$(\psi \circ \varphi)(t) = \psi(ab) = t^{-2}t^3 = t,$$
$$(\varphi \circ \psi)(a) = \varphi(t^{-2}) = (ab)^{-2} = a,$$
$$(\varphi \circ \psi)(b) = \varphi(t^3) = (ab)^3 = b.$$

Hence $G \cong C = C_\infty$.

Particularly nice presentations of groups consist of a finite generating set and a finite set of relations:

Definition 4.2.6. A group G is *finitely presented* if there exists a finite generating set S and a finite set R of relations such that $G \cong \langle S \mid R\rangle$.

Clearly, any finitely presented group is finitely generated. The converse is not true in general:

Example 4.2.7. *The group*

$$G = \langle s, t \mid \{[t^n s t^{-n}, t^m s t^{-m}] = e \mid n, m \in \mathbb{Z}\}\rangle$$

is finitely generated, but not finitely presented, see [**1**].

This group is an example of a so-called *lamplighter group*. Note that it is not too difficult to show that there exist uncountably many finitely generated groups that are not finitely presented.

Definition 4.2.8. A group G is called *linear* if it can be embedded into the the group $GL_n(K)$ for some $n \geq 1$ and some field K.

Linear groups are a very important class of groups. Not all groups are linear. For example, the group $\mathrm{Aut}(F_n)$ for $n \geq 3$ is not linear, see Formanek and Procesi 1992 (but $\mathrm{Aut}(F_2)$ is linear). Also, most of the *Baumslag-Solitar* groups $BS(m, n)$ for $n, m \in \mathbb{Z}$, given by the presentation

$$BS(m, n) = \langle a, b | ba^m b^{-1} = a^n\rangle$$

are not linear. In fact, $BS(m, n)$ is linear if and only if $n = 1$, or if $m = 1$, or if $|m| = |n|$. So the simplest example here of a finitely generated group which is not linear is $BS(2, 3)$. On the other hand all free groups are linear. To show this we will start with the so-called *Ping-Pong Lemma*.

Lemma 4.2.9 (Ping-Pong). *Let G be a group generated by a and b. Suppose that G acts on a set X such that there exist two non-empty subsets A and B of X, such that $A \cap B = \emptyset$, and*

$$a^n.B \subseteq A,\ b^n.A \subseteq B$$

for all integers $n \neq 0$. Then G is freely generated by a and b.

Proof. Let w be a non-empty reduced word in $\{a^{\pm 1}, b^{\pm 1}\}$. We may assume that w begins and ends with $a^{\pm 1}$, for if not then for m large enough a conjugate $w_1 = a^m w a^{-m}$ does, and $w = 1$ if and only if $w_1 = 1$. Let

$$w = a^{n_1} b^{m_1} \cdots a^{n_{k-1}} b^{m_{k-1}} a^{n_k}$$

with $n_i, m_i \neq 0$. Then

$$\begin{aligned} w.B &= a^{n_1}b^{m_1}\cdots a^{n_{k-1}}b^{m_{k-1}}a^{n_k}.B \\ &\subseteq a^{n_1}b^{m_1}\cdots a^{n_{k-1}}b^{m_{k-1}}.A \\ &\subseteq a^{n_1}b^{m_1}\cdots a^{n_{k-1}}.B \\ &\subseteq \cdots \\ &\subseteq a^{n_1}.B \\ &\subseteq A. \end{aligned}$$

It follows that $w \neq_G e$, and so a and b freely generate G. □

COROLLARY 4.2.10. *The matrices*

$$A = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}$$

generate a free subgroup isomorphic to F_2 in $SL_2(\mathbb{Z})$.

PROOF. Denote by $G = \langle A, B\rangle$ the subgroup of $SL_2(\mathbb{Z})$ generated by A and B. It acts on $X = \mathbb{R}^2$, and if we set $V = \{(x, y)^t \mid |x| < |y|\}$ and $W = \{(x, y)^t \mid |x| > |y|\}$, then $A^n.V \subseteq W$ and $B^n.W \subseteq V$ for all $n \neq 0$. Since $V \cap W = \emptyset$ we can apply the Ping-Pong Lemma, and G is freely generated by A and B. □

PROPOSITION 4.2.11. *Any free group is linear.*

PROOF. Let G be a free group. We first assume that G has countable rank. By Proposition 4.1.12 G is embeddable into F_2, which embeds into $SL_2(\mathbb{C})$. Hence G is linear. Now assume that G has uncountable rank c. Then one can show that G embeds into $SL_2(F(t))$, where F is any field of cardinality c. This proof requires some more arguments. Alternatively one can use *ultraproducts*. If for fixed d, every finitely generated subgroup H of G has a faithful representation j_H in $G_H = \mathrm{GL}_d(K_H)$ for some field K_H, then G has a faithful representation into $\mathrm{GL}(K)$, where K is an ultraproduct of the K_H. For details see *mathoverflow*, question 124965. □

DEFINITION 4.2.12. A group G is called *residually finite* if for any nontrivial element $g \in G$ there exists a homomorphism $\varphi\colon G \to H$ into a finite group H so that $\varphi(g) \neq e$.

Clearly, finite groups are residually finite, and subgroups of residually finite groups are residually finite. The simplest possible example of a non-residually finite group is the Baumslag-Solitar group $BS(2, 3)$. Linear groups provide a rich source of residually finite groups:

THEOREM 4.2.13 (Malcev 1940). *A finitely generated linear group is residually finite.*

Since $SL_n(\mathbb{Z})$ is finitely generated, e.g., by the elementary matrices $\{I_n + E_{ij} \mid i \neq j\}$, we obtain the following result.

PROPOSITION 4.2.14. *The group $SL_n(\mathbb{Z})$ is residually finite.*

There is also a direct proof using *principal congruence subgroups of level N*,

$$\Gamma(N) := \ker(SL_n(\mathbb{Z}) \to SL_n(\mathbb{Z}/N\mathbb{Z})) = \{X \in SL_n(\mathbb{Z}) \mid X \equiv I_n \bmod N\}.$$

These are normal subgroups of $SL_n(\mathbb{Z})$ of finite index, given by

$$(SL_n(\mathbb{Z}) : \Gamma(N)) = |SL_n(\mathbb{Z}/N\mathbb{Z})| = N^{n^2-1}\prod_{p|N}\left(\prod_{i=2}^{n}\left(1 - \frac{1}{p^i}\right)\right).$$

We have

$$\Gamma(M) \supseteq \Gamma(N) \Leftrightarrow M \mid N,$$

that is, "to contain is to divide". So for primes p we have

$$\bigcap_{p\in\mathbb{P}} \Gamma(p) = \{I_n\}.$$

This shows that $SL_n(\mathbb{Z})$ is residually finite.

THEOREM 4.2.15. *Any free group of countable rank is residually finite.*

PROOF. A free group of countable rank embeds into $SL_2(\mathbb{Z})$, see Corollary 4.2.10, which is residually finite. □

4.3. Dehns fundamental problems

In his paper in 1912 Max Dehn explicitly raised three decision problems about finitely presented groups.

I. The word problem: *Let G be a group given by a finite presentation. Does there exist an algorithm to determine of an arbitrary word w in the generators of G whether or not $w =_G e$?*

II. The conjugacy problem: *Let G be a group given by a finite presentation. Does there exist an algorithm to determine of an arbitrary pair of words u and v in the generators of G whether or not u and v define conjugate elements of G?*

III. The isomorphism problem: *Does there exist an algorithm to determine of an arbitrary pair of finite presentations whether or not the groups they present are isomorphic?*

Dehn came to these problems while looking at the fundamental groups of 2-dimensional surfaces. The question as to whether a given loop is homotopic to the identity is the word problem, whether two loops are freely homotopic is the conjugacy problem and whether the fundamental groups of two surfaces are isomorphic reflects the problem as to whether the spaces are homeomorphic. It took almost 50 years before all of Dehn's questions were finally answered. First, Novikov proved the remarkable

THEOREM 4.3.1 (Novikov-Boone 1954). *There exists a finitely presented group with an unsolvable word problem.*

Notice that such a group with an unsolvable word problem also has an unsolvable conjugacy problem. Novikov's proof was a combinatorial tour-de-force. New and simpler proofs were obtained by Boone in 1959 and Britton in 1961. Adyan in 1957 proved a most striking negative theorem about finitely presented groups. We first need a definition.

DEFINITION 4.3.2. An invariant property P of a finitely presented group G is called *Markov*, if there exists a finitely presented group G_+ with property P, and if there exists a finitely presented group G_- which cannot be embedded in any finitely presented group having property P.

The group G_+ is called the positive witness, G_- the negative witness for the Markov property P. For example, the properties of being trivial, finite, abelian, having solvable word problem, simple or free are Markov properties. Having rank 2 is *not* a Markov property since every finitely presented group can be embedded in a finitely presented group of rank 2 by the Higman-Neumann-Neumann embedding.

THEOREM 4.3.3 (Adyan 1957, Rabin 1958). *Let P be a Markov property. Then there is no algorithm which decides whether or not any finitely presented group has this property P.*

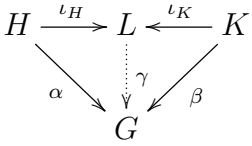
COROLLARY 4.3.4. *The isomorphism problem for finitely presented groups is recursively unsolvable.*

It follows that, from an algorithmic standpoint, finitely presented groups represent a completely intractable class. Of course, certain subclasses, such as finitely generated free groups, or one-relator groups (finitely presented with only one relation) behave much better. Here the word problem is solvable. Finitely presented, residually finite groups also have solvable word problem.
The isomorphism problem for finitely presented solvable groups is recursively undecidable; but on the other hand it has a positive solution for finitely generated *nilpotent* groups – see Grunewald and Segal 1980. In fact they proved somewhat more. In particular their techniques, which make use of the theory of arithmetic and algebraic groups, give rise to a positive solution to the isomorphism problem for finite dimensional Lie algebras over $\mathbb{Q}$, a problem that had been open for almost a century.

4.4. Free products

The free product is an operation that takes two groups H and K and constructs a new group $H * K$. The result contains both H and K as subgroups, is generated by the elements of these subgroups, and is the "most general" group having these properties. Unless one of the groups H and K is trivial, the free product is always infinite. Free products arise in algebraic topology when comparing the fundamental groups of two (or more) topological spaces to the fundamental group of the space obtained by joining them at a point. The free product of two groups is the *coproduct* in the category of groups. This arises in homological algebra.

DEFINITION 4.4.1. Suppose that H and K are two groups. A group L is said to be the free product of H and K, denoted by $L = H * K$ if there are homomorphisms $\iota_H \colon H \to L$ and $\iota_K \colon K \to L$ satisfying the following condition: for any pair of homomorphisms $\alpha \colon H \to G$ and $\beta \colon K \to G$ where G is any group, there is a unique homomorphism $\gamma \colon L \to G$ such that $\alpha = \gamma \circ \iota_H$ and $\beta = \gamma \circ \iota_K$.



As usual, the universal property shows that the free product is unique, up to isomorphism, if it exists. The existence is not difficult to show since we can write down a presentation for $H * K$ from presentations of H and K.

PROPOSITION 4.4.2. *The free product $H * K$ of two groups H and K exists.*

PROOF. Let $H = \langle S \mid D \rangle$ and $K = \langle T \mid E \rangle$ be presentations of H and K. By changing one of the alphabets if necessary, we can assume S and T are disjoint. Then a presentation for $H * K$ can be obtained by joining these together, thus

$$H * K = \langle S \cup T \mid D \cup E \rangle.$$

The required maps ι_H and ι_K are just the homomorphisms induced by the inclusions on generators. Both of these are monomorphisms. For instance, if we define $\varphi\colon H * K \to H$ by $s \mapsto s$ and $t \mapsto 1$ for all $s \in S$ and all $t \in T$, then φ defines a homomorphism and $\varphi \circ \iota_H$ is the identity on H. So ι_H is a monomorphism. It also follows from this argument that $H \cap K = \{e\}$. Finally, given homomorphisms α and β as in the definition, the required γ is given by $\gamma(s) = \alpha(s)$ for $s \in S$ and $\gamma(t) = \beta(t)$ for $t \in T$. Then γ defines a homomorphism; since the definition was forced on us, this is the unique such map. □

The construction can be generalized to any number of factors.

EXAMPLE 4.4.3. 1. $F_m * F_n \cong F_{m+n}$ *for all* $n, m \in \mathbb{N}$.

2. $C_2 * C_2 = \langle x, y \mid x^2 = y^2 = e\rangle \cong D_\infty = \langle s, t \mid s^2 = (st)^2 = e\rangle$.

3. $C_2 * C_3 \cong PSL_2(\mathbb{Z})$.

The free product $F_1 * F_2$ of free groups F_1 and F_2 is always a free group because free groups have no relations. In particular we have $F_m * F_n \cong F_{m+n}$. For $n = m = 1$ we obtain $\mathbb{Z} * \mathbb{Z} \cong F_2$. The infinite dihedral group $D_\infty = \mathrm{Isom}(\mathbb{Z})$ is isomorphic to the free product $C_2 * C_2$, which can be seen by identifying the reflections at 0 resp. at $1/2$ with the generators of $C_2 * C_2$.

By an *alternating word* in $H * K$ we mean an expression $h_1k_1 \cdots h_mk_m$, where by convention one or both of h_1 or k_m may not be present. Such an alternating expression is said to be *reduced* if each $h_i \neq_H e$ and each $k_i \neq_K e$ when present.

THEOREM 4.4.4 (Normal Form). *Every element of the free product $H * K$ is equal to a unique alternating expression $h_1k_1 \cdots h_mk_m$ with $h_i \neq_H e$ and each $k_i \neq_K e$ when present. Here uniqueness means that if two such expressions are equal in $H * K$, say*

$$h_1k_1 \cdots h_mk_m =_{H*K} h'_1k'_1 \cdots h'_nk'_n$$

then $n = m$ and each $h_i =_H h'_i$ and each $k_i =_H k'_i$.

PROOF. That any element is equal to an alternating expression is clear from the presentation. We have to show uniqueness. Let Ω denote the set of all reduced alternating expressions. With each element $h \in H$ we associate a permutation $\varphi(h)$ in the group $\mathrm{Sym}(\Omega)$ of all permutations of by the rule

$$\varphi(h)(h_1k_1 \cdots h_mk_m) = \begin{cases} k_1h_2 \cdots h_mk_m & \text{if } h = h_1^{-1} \\ (hh_1)k_1 \cdots h_mk_m & \text{if } h \neq h_1^{-1} \end{cases}$$

where we understand the first case includes the possibility h_1 is not present and $h = 1$. Also in the second case h_1 is not necessarily present. It is easy to check that $\varphi(h^{-1}) = (\varphi(h))^{-1}$ and that for $h, h' \in H$ we have $\varphi(h)\varphi(h') = \varphi(hh')$. Thus the map $h \mapsto \varphi(h)$ defines a homomorphism from H to $\mathrm{Sym}(\Omega)$. In an entirely analogous way we define an action of K on Ω and hence a homomorphism $\psi\colon K \to \mathrm{Sym}(\Omega)$. We thus obtain a homomorphism $\varphi * \psi\colon H * K \to \mathrm{Sym}(\Omega)$. Now if $h_1k_1 \cdots h_mk_m$ is a reduced alternating expression, then the permutation $(\varphi * \psi)(h_1k_1 \cdots h_mk_m)$ sends the empty expression to $h_1k_1 \cdots h_mk_m$. Hence $h_1k_1 \cdots h_mk_m \neq 1$ in $H * K$ unless it is the empty expression. By induction this implies uniqueness. For suppose

$$h_1k_1 \cdots h_mk_m =_{H*K} h'_1k'_1 \cdots h'_nk'_n$$

where both sides are reduced alternating expressions. Then

$$e = h'_1k'_1 \cdots h'_n(k'_nk_m^{-1})h_m^{-1} \cdots h_1^{-1}$$

and hence the right hand side is not reduced by what we have proved. Since the original expressions were reduced, we must have $k_m = k'_n$ and so by induction the two expressions are identical. □

The following is an alternate version of the normal form theorem. It follows immediately from the above proof.

PROPOSITION 4.4.5. *A group G is the free product of its subgroups H and K if and only if the following two conditions hold:*

1. *H and K generate G, that is every element of G is equal to some alternating expression $h_1k_1 \cdots h_mk_m$.*
2. *If $w \equiv h_1k_1 \cdots h_mk_m$ is an alternating expression and if $w =_G e$ then for some i either $h_i =_H e$ or $k_i =_K e$.*

EXAMPLE 4.4.6. *The group $G = H * K$ with $H = \langle a \mid a^2 = e\rangle \cong C_2$ and $K = \langle b \mid b^3 = e\rangle \cong C_3$ has the presentation $G = \langle a, b \mid a^2 = b^3 = e\rangle$, and ab has infinite order.*

A power of ab has the form $(ab)^n = abab \cdots ab$ which is an alternating word. By the normal form results, if $(ab)^n =_G e$ then either $a =_H e$ or $b =_K e$ and neither is the case. Hence ab has infinite order in G. More generally we have the following result.

LEMMA 4.4.7. *In the free product $H * K$, every element of finite order is conjugate to an element of H or of K. If both H and K are non-trivial, then $H * K$ has elements of infinite order; in fact every reduced alternating word of even length has infinite order.*

PROOF. An alternating word $h_1k_1 \cdots h_mk_m$ is said to be *cyclically reduced* if it is reduced and either has length 1 or even length. By cyclically permuting and reducing as often as possible one arrives at a cyclically reduced word. Hence any alternating word is conjugate to a cyclically reduced word in $H * K$. If a cyclically reduced word w has length at least 2, the w has infinite order in $H * K$, for the same reasons that ab had infinite order in the above example. Hence an element of finite order must be conjugate to an element of length 1, that is an element of H or K. □

We want to mention the following result. The proof is not difficult, but we will omit it here.

PROPOSITION 4.4.8. *If H and K are residually finite, then their free product $H * K$ is residually finite.*

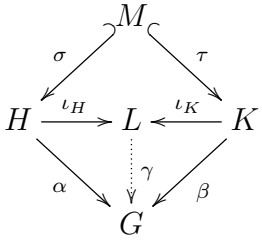
We recover Theorem 4.2.15, that free groups are residually finite.

COROLLARY 4.4.9. *Free groups of countable rank are residually finite.*

PROOF. A free group is a free product of infinite cyclic groups, which are residually finite. In fact, any finitely generated abelian group is residually finite, because for every non-identity element there is a normal subgroup of finite index not containing it. Hence every free group is residually finite by Proposition 4.4.8. □

We can also generalize free products to *free products with amalgamation*. This arises again naturally in topology: by the theorem of *Seifert and van Kampen*, the fundamental group of a space glued together of several (say two) components is a free amalgamated product of the fundamental groups of the components over the fundamental group of the intersection (the two subspaces and their intersection have to be non-empty and path-connected).

DEFINITION 4.4.10. Suppose that groups H and K have an isomorphic subgroup M, so that there are a pair of embeddings $\sigma\colon M \hookrightarrow H$ and $\tau\colon M \hookrightarrow K$. The group L is *the free product of H and K with amalgamated subgroup M*, denoted by $L = H *_M K$, if there are maps $\iota_H\colon H \to L$ and $\iota_K\colon K \to L$ such that $\iota_H \circ \sigma = \iota_K \circ \tau$ satisfying the following condition: for any pair of homomorphisms $\alpha\colon H \to G$ and $\beta\colon K \to G$ such that $\alpha \circ \sigma = \beta \circ \tau$ where G is any group, there is a unique homomorphism $\gamma\colon L \to G$ such that $\alpha = \gamma \circ \iota_H$ and $\beta = \gamma \circ \iota_K$.



Again it is easy to see that the free product L of H and K with amalgamated subgroup M exists and is unique. We can just write down a presentation for $L = H *_M K$. Suppose that H and K are given by presentations, say $H = \langle S \mid D\rangle$ and $K = \langle T \mid E\rangle$. Also suppose that $M = \langle Q \mid V\rangle$. Only the generators of M are relevant here. By changing one of the alphabets if necessary, we can assume S and T are disjoint. Then a presentation for $H *_M K$ can be obtained by joining these together and identifying the images of M, thus

$$H *_M K = \langle S \cup T \mid D \cup E,\ \sigma(q) = \tau(q)\ \forall\ q \in Q\rangle.$$

The required maps ι_H and ι_K are just the homomorphisms induced by the inclusions on generators. Both of these are monomorphisms, but this is not obvious. Also one can show $H \cap K = \sigma(M) = \tau(M)$, but again this is not obvious. We leave the details for the reader.

EXAMPLE 4.4.11. 1. *For the trivial group $M = 1$ we obtain $H *_M K = H * K$.*

2. *One can show that the group $SL_2(\mathbb{Z})$ is isomorphic to the free amalgamated product $C_6 *_{C_2} C_4$.*

CHAPTER 5

Group extensions

Given a group G and a normal subgroup N of G we may decompose G in a way into N and G/N. The study of group extensions is related to the converse problem. Given N and Q, we try to understand what different groups G can arise containing a normal subgroup N with quotient $G/N \cong Q$. Such groups are called *extensions of N by Q*. If N is abelian, then there is a natural Q-action on N, making N a Q-module. In that case the cohomology group $H^2(Q, N)$ classifies the equivalence classes of such group extensions which give rise to the given Q-module structure on N.

Group homology and cohomology is usually treated in homological algebra. This deals with category theory and in particular with the theory of derived functors. We will only focus on group theory here, see [**11**].

5.1. Split extensions and semidirect products

We start with the definition of exact sequences.

Definition 5.1.1. A sequence of groups and group homomorphisms

$$\cdots \to A_{n-1} \xrightarrow{\alpha_n} A_n \xrightarrow{\alpha_{n+1}} A_{n+1} \to \cdots$$

is called *exact at A_n* if $\operatorname{im} \alpha_n = \ker \alpha_{n+1}$. The sequence is called *exact* if it is exact at each group.

Example 5.1.2. 1. *The sequence $1 \xrightarrow{\alpha_1} A \xrightarrow{\alpha_2} 1$ is exact if and only if $A = 1$ is the trivial group.*

2. *The sequence $1 \xrightarrow{\alpha} A \xrightarrow{\beta} B \xrightarrow{\gamma} 1$ is exact if and only if A is isomorphic to B.*

Indeed, $1 = \operatorname{im} \alpha_1 = \ker \alpha_2 = A$ in the first case, and $1 = \operatorname{im} \alpha = \ker \beta$, $\operatorname{im} \beta = \ker \gamma = B$ in the second, so that

$$A \cong A/\ker \beta \cong \operatorname{im} \beta = B.$$

Example 5.1.3. *A "short exact sequence" is given by*

$$1 \to A' \xrightarrow{\alpha} A \xrightarrow{\beta} A'' \to 1$$

From the exactness we conclude that α is injective, β is surjective and

$$A' \cong \alpha(A') = \ker \beta.$$

Hence $\alpha(A')$ being a kernel is a normal subgroup of A. Sometimes we will identify A' with its image $\alpha(A')$. Furthermore we have

$$A/\ker \beta \cong \beta(A) = A''.$$

Hence A'' is isomorphic to the quotient A/A'.

DEFINITION 5.1.4. Let N and Q be groups. An *extension of N by Q* is a group G such that

(1) G contains N as a normal subgroup.
(2) The quotient G/N is isomorphic to Q.

An extension of groups defines a short exact sequence and vice versa: if G is an extension of N by Q then

$$1 \to N \xrightarrow{\iota} G \xrightarrow{\pi} Q \to 1$$

is a short exact sequence where $\iota : N \hookrightarrow G$ is the inclusion map and $\pi : G \twoheadrightarrow G/N$ is the canonical epimorphism. If

$$1 \to A' \xrightarrow{\alpha} A \xrightarrow{\beta} A'' \to 1$$

is a short exact sequence, then A is an extension of $\alpha(A') \cong A'$ by $\beta(A) \cong A''$, see Example 5.1.3.

EXAMPLE 5.1.5. *Given any two groups N and Q, their direct product $G = Q \times N$ is an extension of N by Q, and also an extension of Q by N.*

EXAMPLE 5.1.6. 1. *The cyclic group C_6 is an extension of C_3 by C_2. Hence we obtain the short exact sequence*

$$1 \to C_3 \to C_6 \to C_2 \to 1.$$

2. *The symmetric group respectively the dihedral group $S_3 \cong D_3$ is an extension of C_3 by C_2, but not of C_2 by C_3. We obtain the short exact sequence*

$$1 \to C_3 \to D_3 \to C_2 \to 1.$$

In the first case, C_3 is a normal subgroup of C_6 with quotient isomorphic to C_2. In the second case let $C_3 = \langle (123) \rangle$. This is a normal subgroup of D_3 since the index is $(D_3 : C_3) = 2$. The quotient is isomorphic to $C_2 = \langle (12) \rangle$. Note that C_2 is not a normal subgroup of D_3.

Let $M/L/K$ be a tower of field extensions such that the field extensions M/K and L/K are normal. Denote by

$$\begin{aligned} Q &:= \mathrm{Gal}(L/K), \\ N &:= \mathrm{Gal}(M/L), \\ G &:= \mathrm{Gal}(M/K). \end{aligned}$$

Then G is a group extension of N by Q since $N \lhd G$ and $Q \cong G/N$ by Galois theory. In this way be obtain some examples of group extensions.

EXAMPLE 5.1.7. *Let $M/L/K$ be $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}(\sqrt{2})/\mathbb{Q}$. Then*

$$\begin{aligned} Q &:= \mathrm{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) \cong C_2 \\ N &:= \mathrm{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}(\sqrt{2})) \cong C_2 \\ G &:= \mathrm{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}) \cong C_2 \times C_2 \end{aligned}$$

This yields the short exact sequence

$$1 \to C_2 \to C_2 \times C_2 \to C_2 \to 1.$$

Let us prove that $G \cong C_2 \times C_2$. Since $[\mathbb{Q}(\sqrt{2},\sqrt{3}) : \mathbb{Q}] = 4$ the group G has four elements: the automorphisms

$$(\sqrt{2},\sqrt{3}) \mapsto \begin{cases} (\sqrt{2},\sqrt{3}) \\ (-\sqrt{2},\sqrt{3}) \\ (\sqrt{2},-\sqrt{3}) \\ (-\sqrt{2},-\sqrt{3}) \end{cases}$$

Hence all non-trivial elements of G have order 2.

EXAMPLE 5.1.8. *Let $M/L/K$ be $\mathbb{Q}(\sqrt{2},\sqrt{2+\sqrt{2}})/\mathbb{Q}(\sqrt{2})/\mathbb{Q}$. Then*

$$\begin{aligned} Q &:= \mathrm{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) \cong C_2 \\ N &:= \mathrm{Gal}(\mathbb{Q}(\sqrt{2},\sqrt{2+\sqrt{2}})/\mathbb{Q}(\sqrt{2})) \cong C_2 \\ G &:= \mathrm{Gal}(\mathbb{Q}(\sqrt{2},\sqrt{2+\sqrt{2}})/\mathbb{Q}) \cong C_4 \end{aligned}$$

This yields the short exact sequence

$$1 \to C_2 \to C_4 \to C_2 \to 1.$$

To show that the Galois group of $\mathbb{Q}(\sqrt{2},\sqrt{2+\sqrt{2}})$ over $\mathbb{Q}$ is cyclic of order 4, we will use the following well known result:

LEMMA 5.1.9. *Let K be a field of characteristic different from 2 and assume that a is not a square in K. Let $L := K(\sqrt{a})$. Then there exists a tower of normal field extensions $M/L/K$ with $\mathrm{Gal}(M/K) \cong C_4$ if and only if $a \in K^2 + K^2$. In that case there exist $s,t \in K,\ t \neq 0$ such that $M = L(\sqrt{s+t\sqrt{a}})$.*

In our case $K = \mathbb{Q},\ L = \mathbb{Q}(\sqrt{2})$ and $a = 2$. Since $2 = 1^2 + 1^2$ we have $\mathrm{Gal}(M/K) \cong C_4$ and with $s = 2, t = 1$,

$$M = L(\sqrt{2+\sqrt{2}}) = \mathbb{Q}(\sqrt{2},\sqrt{2+\sqrt{2}}).$$

DEFINITION 5.1.10. Let $1 \to N \xrightarrow{\alpha} G \xrightarrow{\beta} Q \to 1$ be a given group extension. Denote by $\tau : Q \cong G/\alpha(N) \to G$ the map assigning each coset $x \in G/\alpha(N)$ a representative $\tau(x) \in G$. Any such function $\tau : Q \to G$ is called a *transversal function*.

By definition we have $\beta(\tau(x)) = x$, i.e.,

$$\beta\tau = \mathrm{id}_{|Q}\,.$$

In general a transversal function need not be a homomorphism. If it is however we obtain a special class of extensions.

DEFINITION 5.1.11. An extension $1 \to N \xrightarrow{\alpha} G \xrightarrow{\beta} Q \to 1$ is called *split* if there is a transversal function $\tau : Q \to G$ which is a group homomorphism. In that case τ is called a *section*.

Sometimes this is called right-split, whereas left-split means that there exists a homomorphism $\sigma\colon G \to N$ such that $\sigma\alpha = \mathrm{id}_{|N}$. For the category of groups however, the properties right-split and left-split need not be equivalent.

EXAMPLE 5.1.12. *The extensions of Example* 5.1.6 *are both split:*

$$1 \to C_3 \to C_6 \to C_2 \to 1$$
$$1 \to C_3 \to D_3 \to C_2 \to 1$$

On the other hand the extension

$$1 \to C_2 \to C_4 \to C_2 \to 1$$

of Example 5.1.8 *is not split.*

Since a transversal function τ in these examples is given by its values on $[0]$ and $[1]$ in C_2, it is easily seen that we can find a section for the first two examples. As to the last extension it is clear that C_2 does not have a complement in C_4. But this implies that the extension is not splitting as we will see in the following.

DEFINITION 5.1.13. Two subgroups $N, Q \leq G$ are called *complementary* if $N \cap Q = 1$ and $G = NQ$.

In general, $NQ = \{nq \mid n \in N,\, q \in Q\}$ is not a subgroup of G. In fact, it is a subgroup if and only if $NQ = QN$. Hence in particular it is a subgroup if $N \lhd G$ or $Q \lhd G$.

EXAMPLE 5.1.14. *The subgroups $N = \langle(123)\rangle$ and $Q = \langle(12)\rangle$ are complementary subgroups in $G = S_3$. The subgroups $N = \langle(12)\rangle$ and $Q = \langle(234)\rangle$ of $G = S_4$ are not complementary.*

The first case is clear, for the second note that $|NQ| = |N| \cdot |Q| \cdot |N \cap Q|^{-1} = 6$, hence $NQ \neq S_4$.

LEMMA 5.1.15. *Let $N, Q \leq G$ be subgroups. Then N and Q are complementary if and only if each element $g \in G$ has a unique representation $g = nq$ with $n \in N$, $q \in Q$.*

PROOF. If N and Q are complementary then $G = NQ$, hence each element $g \in G$ has a representation $g = nq$. To show the uniqueness assume that $g = nq = mp$ with $n, m \in N$ and $p, q \in Q$. Then $n^{-1}gp^{-1} = qp^{-1} = n^{-1}m \in N \cap Q = 1$ and hence $m = n$ and $p = q$. Conversely the unique representation implies $G = NQ$ and $N \cap Q = 1$. □

DEFINITION 5.1.16. A group G is called *inner semidirect product* of N by Q if

(1) N is a normal subgroup of G.
(2) N and Q are complementary in G.

In that case we will now write $G = Q \ltimes N$. Often it is also written $G = N \rtimes Q$.

EXAMPLE 5.1.17. *Both S_3 and C_6 are inner semidirect products of C_3 by C_2.*

This says that in contrast to direct products, an inner semidirect product G of N by Q is not determined up to isomorphism by the two subgroups. It will also depend on how N is normal in G.

EXAMPLE 5.1.18. *The groups S_n and D_n are inner semidirect products as follows:*

$$S_n = C_2 \ltimes A_n$$
$$D_n = C_2 \ltimes C_n$$

Clearly $A_n \lhd S_n$ and C_2, A_n are complementary subgroups in S_n. Recall that

$$D_n = \langle s, t \mid s^n = t^2 = 1,\, tst = s^{-1} \rangle$$

and write $C_n = \langle s \rangle, C_2 = \langle t \rangle$. Then $C_n \lhd D_n$ and C_n and C_2 are complementary in D_n.

An inner semidirect product of N by Q is also an extension of N by Q since $Q \cong G/N$. More precisely we have:

PROPOSITION 5.1.19. *For a group extension $1 \to N \xrightarrow{\alpha} G \xrightarrow{\beta} Q \to 1$ the following assertions are equivalent:*

(1) *There is a group homomorphism $\tau : Q \to G$ with $\beta\tau = \mathrm{id}_{|Q}$.*
(2) *$\alpha(N) \cong N$ has a complement in G, i.e., $G \cong Q \ltimes N$.*

COROLLARY 5.1.20. *G is an inner semidirect product of N by Q if and only if G is a split extension of N by Q.*

PROOF. Let τ be a section. We will show that $\tau(Q)$ then is a complement of $\alpha(N) = \ker\beta$ in G. So let $g \in \ker\beta \cap \tau(Q)$. With $g = \tau(q)$ for some $q \in Q$ it follows

$$1 = \beta(g) = \beta(\tau(q)) = q$$

Since τ is a homomorphism $g = \tau(q) = \tau(1) = 1$. So we have

$$\alpha(N) \cap \tau(Q) = 1$$

Now let $g \in G$ and define $x := \beta(g) \in Q$. Then $\tau(x) \in G$ and

$$\beta(g\tau(x^{-1})) = \beta(g) \cdot \beta(\tau(x^{-1})) = xx^{-1} = 1$$

so that $g\tau(x^{-1}) = \alpha(n)$ for some $n \in N$ since it lies in $\ker\beta = \alpha(N)$. Using $\tau(x)^{-1} = \tau(x^{-1})$ we obtain $g = \alpha(n)\tau(x)$, i.e.,

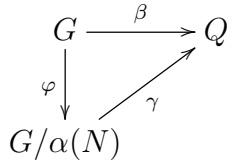
$$G = \alpha(N)\tau(Q)$$

Since α and τ are monomorphisms we have $G \cong Q \ltimes N$, $Q \cong \tau(Q)$ and $N \cong \alpha(N)$.

For the converse direction let C be a complement of $\alpha(N)$ in G, i.e.,

$$C \cap \alpha(N) = 1$$
$$C \cdot \alpha(N) = G$$

The homomorphism lemma now says that $\alpha(N) \subset \ker\beta$ implies the existence of a unique homomorphism $\gamma : G/\alpha(N) \to Q$ such that the following diagram commutes:



In fact, γ is defined by $\gamma(g\alpha(N)) = \beta(g)$. Let us now restrict φ to the complement C. We still denote this map by φ. By assumption it is an isomorphism, given by $c \mapsto c\alpha(N)$ for $c \in C$. Hence there exists a unique homomorphism $\gamma : G/\alpha(N) \to Q$ satisfying

$$\gamma(\varphi(c)) = \gamma(c\alpha(N)) = \beta(c)$$

for all $c \in C$, i.e., $\gamma \circ \varphi = \beta$. Note that γ is an isomorphism. Hence the map

$$\tau : Q \to C \subset G,\; q \mapsto \varphi^{-1}(\gamma^{-1}(q))$$

is a homomorphism with

$$\beta(\tau(q)) = (\gamma \circ \varphi)(\varphi^{-1}(\gamma^{-1}(q))) = q$$

hence with $\beta\tau = \mathrm{id}_{|Q}$. □

EXAMPLE 5.1.21. *The following exact sequences are both split:*

$$1 \to A_n \xrightarrow{\iota} S_n \xrightarrow{sign} \{\pm 1\} \to 1$$
$$1 \to SL_n(k) \xrightarrow{\iota} GL_n(k) \xrightarrow{det} k^\times \to 1$$

It follows that $S_n \cong C_2 \ltimes A_n$ *and* $GL_n(k) \cong k^\times \ltimes SL_n(k)$.

Since $\ker \mathrm{sign} = A_n$ we see that the first sequence is exact. It also splits. Let $\pi \in S_n$ be a transposition and define $\tau\colon \{\pm 1\} \to S_n$ by $\tau(1) = \mathrm{id}$ and $\tau(-1) = \pi$. Then τ is a section. For the second sequence define $\tau : k^\times \to GL_n(k)$ by

$$a \mapsto \begin{pmatrix} 1 & \dots & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots \\ 0 & \dots & 1 & 0 \\ 0 & \dots & 0 & a \end{pmatrix}$$

This is a section since $\tau(ab) = \tau(a)\tau(b)$ and $(\beta \circ \tau)(a) = \det \tau(a) = a$.

DEFINITION 5.1.22. Let N, Q be two groups and $\varphi : Q \to \mathrm{Aut}(N)$ be a homomorphism. Define a multiplication on $Q \times N$ as follows:

$$(x, a)(y, b) = (xy, \varphi(y)(a) \cdot b) \tag{5.1}$$

for $x, y \in Q$ and $a, b \in N$. Then $Q \times N$ together with this multiplication becomes a group which is denoted by $G = Q \ltimes_\varphi N$. It is called the *outer semidirect product* of N by Q with respect to φ.

Note that this corresponds to Definition 2.4.6, where we wrote the group law on $N \times Q$, instead of $Q \times N$. We have $\varphi(xy) = \varphi(y) \circ \varphi(x)$ for all $x, y \in Q$. The product on the RHS denotes the composition of automorphisms in $\mathrm{Aut}(N)$. Let us verify the group axioms. The element $(1, 1)$ is a left unit element in G:

$$(1, 1)(x, a) = (x, \varphi(x)(1) \cdot a) = (x, a)$$

A left inverse element to (x, a) is given by (x^{-1}, b^{-1}) where $b = \varphi(x^{-1})(a)$:

$$\begin{aligned}(x^{-1}, b^{-1})(x, a) &= (x^{-1}x, \varphi(x)(b^{-1}) \cdot a) = (1, \varphi(x)(\varphi(x^{-1})(a^{-1})) \cdot a) \\ &= (1, a^{-1}a) = (1, 1)\end{aligned}$$

since $b^{-1} = (\varphi(x^{-1})(a))^{-1} = \varphi(x^{-1})(a^{-1})$. Finally the multiplication is associative.

$$\begin{aligned}[(x,a)(y,b)](z,c) &= (xy, \varphi(y)(a)\cdot b)(z,c) = (xyz, \varphi(z)(\varphi(y)(a)\cdot b)\cdot c)\\ &= (xyz, ((\varphi(z)\circ\varphi(y))(a)\cdot\varphi(z)(b)\cdot c)\\ (x,a)[(y,b)(z,c)] &= (x,a)(yz, \varphi(z)b\cdot c) = (xyz, \varphi(yz)(a)\cdot\varphi(z)(b)\cdot c)\end{aligned}$$

Since φ is a homomorphism both sides coincide.

We want to explain the relation between an inner and outer semidirect product. If

$$1 \to N \xrightarrow{\alpha} G \xrightarrow{\beta} Q \to 1$$

is a short exact sequence, then G acts on the normal subgroup $\alpha(N) \lhd G$ by conjugation:

$$G \times \alpha(N) \to \alpha(N), \quad (g, \alpha(a)) \mapsto g^{-1}\alpha(a)g$$

Definition 5.1.23. The assignment $\gamma(g) = g^{-1}\alpha(a)g$ defines a homomorphism $\gamma : G \to \mathrm{Aut}(\alpha(N))$. The restriction on the quotient $G/\alpha(N) \cong Q$ is also denoted by $\gamma : Q \to \mathrm{Aut}(N)$.

Proposition 5.1.24. *Let $G = Q \ltimes_\varphi N$ be an outer semidirect product of N by Q. Then G defines a split short exact sequence*

$$1 \to N \xrightarrow{\alpha} G \underset{\beta}{\overset{\tau}{\leftrightarrows}} Q \to 1$$

where the maps α, β, τ are given by

$$\alpha(a) = (1,a), \quad \beta((x,a)) = x, \quad \tau(x) = (x,1)$$

such that

$$\alpha \circ \varphi(x) = \gamma(\tau(x)) \circ \alpha \tag{5.2}$$

Proof. We show first that $\alpha(N)$ is normal in G so that $\gamma : Q \to \mathrm{Aut}(N)$ is well defined. Let $(x,a) \in G$ and $(1,c) \in \alpha(N)$.

$$\begin{aligned}(x,a)^{-1}(1,c)(x,a) &= (x^{-1}, \varphi(x^{-1})(a^{-1}))\cdot(x, \varphi(x)(c)\cdot a)\\ &= (1,\ a^{-1}\cdot\varphi(x)(c)\cdot a) \in \alpha(N)\end{aligned}$$

Applying this computation we obtain for all $a \in N$

$$\begin{aligned}\gamma(\tau(x))[\alpha(a)] &= \tau(x)^{-1}\alpha(a)\tau(x) = (x,1)^{-1}(1,a)(x,1)\\ &= (1, \varphi(x)(a)) = \alpha[\varphi(x)(a)]\end{aligned}$$

which gives (5.2). Since obviously α is a monomorphism and β is an epimorphism with $\beta\tau = \mathrm{id}$ we obtain a split short exact sequence. The group G is also an inner semidirect product of $\alpha(N)$ by $\tau(Q)$. □

Conversely the following result holds.

PROPOSITION 5.1.25. *Each split short exact sequence* $1 \to N \xrightarrow{\alpha} G \xrightarrow{\beta} Q \to 1$ *defines via* (5.2) *an outer semidirect product* $Q \ltimes_\varphi N$ *which is isomorphic to* G.

PROOF. Since α is a monomorphism (5.2) defines a homomorphism $\varphi : Q \to \mathrm{Aut}(N)$. Define the map $\psi : Q \ltimes_\varphi N \to G$ by

$$\psi[(x,a)] = \tau(x) \cdot \alpha(a) \tag{5.3}$$

By Lemma (5.1.15) the map ψ is bijective. Moreover it is a homomorphism. We have

$$\begin{aligned}\psi[(x,a)(y,b)] &= \psi[(xy, \varphi(y)(a) \cdot b)] = \tau(xy) \cdot \alpha(\varphi(y)(a)) \cdot \alpha(b) \\ &= \tau(x)\tau(y) \cdot \alpha(\varphi(y)(a)) \cdot \alpha(b)\end{aligned}$$

by (5.1) and the fact that τ is a homomorphism. On the other hand

$$\begin{aligned}\psi[(x,a)]\psi[(y,b)] &= \tau(x)\alpha(a) \cdot \tau(y)\alpha(b) = \tau(x)\tau(y) \cdot \big(\tau(y)^{-1}\alpha(a)\tau(y)\big) \cdot \alpha(b) \\ &= \tau(x)\tau(y) \cdot \gamma(\tau(y))(\alpha(a)) \cdot \alpha(b) = \tau(x)\tau(y) \cdot \alpha(\varphi(y)(a)) \cdot \alpha(b)\end{aligned}$$

□

EXAMPLE 5.1.26. *Let* C_2 *act on* C_n *by the automorphism* $x \mapsto x^{-1}$. *Then* $D_n \cong C_2 \ltimes_\varphi C_n$.

The homomorphism $\varphi : C_2 \to \mathrm{Aut}(C_n)$ is defined by $\varphi(1) = \mathrm{id}$, $\varphi(-1)(x) = x^{-1}$.

The following well known result shows that certain group extensions are always semidirect products.

SCHUR-ZASSENHAUS 5.1.27. *Let* N *and* Q *be finite groups of coprime order. Then every short exact sequence* $1 \to N \xrightarrow{\alpha} G \xrightarrow{\beta} Q \to 1$ *splits. Hence each extension of* N *by* Q *is a semidirect product.*

We will prove this theorem later, see Proposition 6.5.6. There is an elegant proof for the case that N is abelian using the second cohomology group $H^2(Q, N)$. The general case can be proved with an induction over the order of N reducing the problem to a central extension. An above extension is called *central* if $\alpha(N) \subset Z(G)$ is satisfied. In that case N is abelian. In fact, the above result has first been proved by Schur in 1902 for central extensions.
Note that the result need not be true if the orders are not coprime. A short exact sequence $1 \to C_2 \to G \to C_2 \to 1$ may split or may not. Take $G = C_2 \times C_2$ or $G = C_4$ respectively.

5.2. Equivalent extensions and factor systems

How can we describe all possible extensions G of a group N by another group Q? We will view extensions as short exact sequences $1 \to N \xrightarrow{\alpha} G \xrightarrow{\beta} Q \to 1$. There will be a natural equivalence relation on the set of such extensions. As a preparation we will need the following Lemma.

LEMMA 5.2.1. *Suppose that we have the following commutative diagram of groups and homomorphisms with exact rows:*

$$\begin{array}{ccccccccc} 1 & \longrightarrow & A & \xrightarrow{\alpha} & B & \xrightarrow{\beta} & C & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle g} & & \downarrow{\scriptstyle h} & & \\ 1 & \longrightarrow & A' & \xrightarrow{\gamma} & B' & \xrightarrow{\delta} & C' & \longrightarrow & 1 \end{array}$$

If f and h are both injective, respectively surjective, then so is g. In particular, if f and h are isomorphisms, so is g.

PROOF. By assumption we know that α, γ are injective, β, δ are surjective and $\operatorname{im}\alpha = \ker\beta$, $\operatorname{im}\gamma = \ker\delta$. Since the diagram commutes we have

$$\gamma f = g\alpha, \quad h\beta = \delta g \tag{5.4}$$

Assume first that f and h are injective. We will show that g then is also injective. Let $g(b) = 1$ for some $b \in B$. Then by (5.4)

$$1 = \delta(g(b)) = h(\beta(b)) \quad \Longrightarrow \quad \beta(b) = 1$$

since h is injective. It follows $b \in \ker\beta = \operatorname{im}\alpha$, hence $\alpha(a) = b$ for some $a \in A$. Then again by (5.4)

$$1 = g(b) = g(\alpha(a)) = \gamma(f(a)) \quad \Longrightarrow \quad f(a) = 1$$

since γ is injective. But f is also injective hence $a = 1$ and $b = \alpha(1) = 1$. This proves the injectivity of g.
For the second part assume now that f and h are surjective. We will show that g is also surjective. Let $b' \in B'$ be given. Since h is surjective there is a $c \in C$ such that $h(c) = \delta(b') \in C'$. Since β is surjective there is a $b \in B$ such that $\beta(b) = c$. It follows

$$\delta(g(b)) = h(\beta(b)) = h(c) = \delta(b')$$

so that $\delta\left(g(b)^{-1}b'\right) = 1$ and $g(b)^{-1}b' \in \ker\delta = \operatorname{im}\gamma$. it follows $g(b)^{-1}b' = \gamma(a')$ for some $a' \in A'$. Since f is surjective there is an $a \in A$ such that $f(a) = a'$ so that, using (5.4)

$$g(\alpha(a)) = \gamma(f(a)) = \gamma(a') = g(b)^{-1}b'$$

which implies $b' = g(b) \cdot g(\alpha(a)) = g(b \cdot \alpha(a))$. Hence g is surjective. □

The following result involving 10 groups and 13 group homomorphisms generalizes the above Lemma.

LEMMA 5.2.2. *Consider the following commutative diagram of groups and homomorphisms with exact rows.*

$$\begin{array}{ccccccccccc} A_1 & \xrightarrow{\alpha_1} & A_2 & \xrightarrow{\alpha_2} & A_3 & \xrightarrow{\alpha_3} & A_4 & \xrightarrow{\alpha_4} & A_5 \\ \downarrow{\scriptstyle f_1} & & \downarrow{\scriptstyle f_2} & & \downarrow{\scriptstyle f_3} & & \downarrow{\scriptstyle f_4} & & \downarrow{\scriptstyle f_5} \\ B_1 & \xrightarrow{\beta_1} & B_2 & \xrightarrow{\beta_2} & B_3 & \xrightarrow{\beta_3} & B_4 & \xrightarrow{\beta_4} & B_5 \end{array}$$

Then the following holds.

(a) *If f_2, f_4 are onto and f_5 is one-to-one, then f_3 is onto.*
(b) *If f_2, f_4 are one-to-one and f_1 is onto, then f_3 is one-to-one.*
(c) *In particular, if f_1, f_2 and f_4, f_5 are isomorphisms, so is f_3.*

The proof is done in a completely analogous way and is left to the reader.

DEFINITION 5.2.3. Let N and Q be groups. Two extensions G and G' of N by Q are called *equivalent* if there exists a homomorphism $\varphi : G \to G'$ such that the following diagram with exact rows becomes commutative:

$$\begin{array}{ccccccccc} 1 & \longrightarrow & N & \xrightarrow{\alpha} & G & \xrightarrow{\beta} & Q & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle \mathrm{id}} & & \downarrow{\scriptstyle \varphi} & & \downarrow{\scriptstyle \mathrm{id}} & & \\ 1 & \longrightarrow & N & \xrightarrow{\gamma} & G' & \xrightarrow{\delta} & Q & \longrightarrow & 1 \end{array}$$

If the extensions G and G' are equivalent then they are automatically isomorphic as groups since φ is then an isomorphism by Lemma 5.2.2. The converse however need not be true. There exist inequivalent extensions G and G' which are isomorphic as groups. Classifying inequivalent group extensions is in general much finer than classifying non-isomorphic groups. We will see that in the next example. Formally we will write

$$(G, \alpha, \beta) \simeq (G', \gamma, \delta)$$

for two equivalent group extensions. In that case there exists a homomorphism $\varphi : G \to G'$ such that $\gamma = \varphi\alpha$ and $\beta = \delta\varphi$. This defines an equivalence relation. Clearly the relation is reflexive since $(G, \alpha, \beta) \simeq (G, \alpha, \beta)$ with $\varphi = \mathrm{id}$. It is symmetric since $(G, \alpha, \beta) \simeq (G', \gamma, \delta)$ implies $(G', \gamma, \delta) \simeq (G, \alpha, \beta)$ with $\varphi^{-1} : G' \to G$. To show transitivity consider the following diagram:

$$\begin{array}{ccccccccc} 1 & \longrightarrow & N & \xrightarrow{\alpha} & G & \xrightarrow{\beta} & Q & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle \mathrm{id}} & & \downarrow{\scriptstyle \varphi} & & \downarrow{\scriptstyle \mathrm{id}} & & \\ 1 & \longrightarrow & N & \xrightarrow{\gamma} & G' & \xrightarrow{\delta} & Q & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle \mathrm{id}} & & \downarrow{\scriptstyle \varphi'} & & \downarrow{\scriptstyle \mathrm{id}} & & \\ 1 & \longrightarrow & N & \xrightarrow{\varepsilon} & G'' & \xrightarrow{\kappa} & Q & \longrightarrow & 1 \end{array}$$

Assume that $(G, \alpha, \beta) \simeq (G', \gamma, \delta)$ and $(G', \gamma, \delta) \simeq (G'', \varepsilon, \kappa)$. It follows that there are homomorphisms $\varphi : G \to G'$ and $\varphi' : G' \to G''$ such that

$$\gamma = \varphi\alpha,\ \beta = \delta\varphi,\ \varepsilon = \varphi'\gamma,\ \delta = \kappa\varphi'$$

Defining $\varphi'' := \varphi'\varphi : G \to G''$ it follows

$$\varepsilon = \varphi'\gamma = \varphi'\varphi\alpha = \varphi''\alpha$$
$$\beta = \delta\varphi = \kappa\varphi'\varphi = \kappa\varphi''$$

Hence we have $(G, \alpha, \beta) \simeq (G'', \varepsilon, \kappa)$.

EXAMPLE 5.2.4. *Let p be a prime. Then there are p inequivalent extensions G of C_p by C_p. Since G has order p^2 it is either isomorphic to $C_p \times C_p$ or to C_{p^2}.*

Besides the split exact sequence $1 \to C_p \to C_p \times C_p \to C_p \to 1$ consider the following $p-1$ short exact sequences

$$1 \to C_p \xrightarrow{\alpha} C_{p^2} \xrightarrow{\beta_i} C_p \to 1$$

where $C_p = \langle a \rangle = \{1, a, a^2, \ldots, a^{p-1}\}$ and $C_{p^2} = \langle g \rangle = \{1, g, g^2, \ldots, g^{p^2-1}\}$ and the homomorphisms α and β are given by

$$\begin{aligned} \alpha &: C_p \to C_{p^2}, \quad a \mapsto g^p \\ \beta_i &: C_{p^2} \to C_p, \quad g \mapsto a^i, \quad i = 1, 2, \ldots, p-1 \end{aligned}$$

The sequences are exact since $\beta_i(\alpha(a)) = \beta_i(g^p) = a^{pi} = 1$ in C_p, hence $\operatorname{im}\alpha = \ker\beta_i$. We claim that any two extensions β_i and β_j for $i \neq j$ are inequivalent. Suppose $(C_p, \alpha, \beta_i) \simeq (C_p, \alpha, \beta_j)$, i.e.,

$$\begin{array}{ccccccccc} 1 & \longrightarrow & C_p & \xrightarrow{\alpha} & C_{p^2} & \xrightarrow{\beta_i} & C_p & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle \mathrm{id}} & & \downarrow{\scriptstyle \varphi} & & \downarrow{\scriptstyle \mathrm{id}} & & \\ 1 & \longrightarrow & C_p & \xrightarrow{\alpha} & C_{p^2} & \xrightarrow{\beta_j} & C_p & \longrightarrow & 1 \end{array}$$

and $\alpha = \varphi\alpha,\ \beta_i = \beta_j\varphi$. It follows

$$g^p = \alpha(a) = \varphi(\alpha(a)) = \varphi(g^p) = \varphi(g)^p$$

Now $\varphi(g) = g^r$ generates C_{p^2} since φ is an isomorphism. Hence $p \nmid r$ and $g^p = \varphi(g^p) = g^{pr}$ in C_{p^2}. This implies $r \equiv 1(p)$. On the other hand we have

$$a^i = \beta_i(g) = \beta_j(\varphi(g)) = \beta_j(g^r) = a^{jr}$$

in C_p. It follows $i \equiv jr(p)$. Together with $r \equiv 1(p)$ we have $i \equiv j(p)$ or $i = j$ and $\beta_i = \beta_j$. So we have proved the claim.

REMARK 5.2.5. There are exactly p equivalence classes of extensions of C_p by C_p. We will see later that they are in bijection with the elements in the group $H^2(C_p, C_p) \cong C_p$ where C_p acts trivially on C_p.

We will now reduce the classification of group extensions to so called *factor systems*. Schreier's theorem yields a bijection between the equivalence classes of group extensions and the equivalence classes of the associated parameter systems.

DEFINITION 5.2.6. Let N and Q be two groups. A pair of functions (f, T)

$$\begin{aligned} f &: Q \times Q \to N \\ T &: Q \to \operatorname{Aut}(N) \end{aligned}$$

is called a *factor system* to N and Q if

$$f(xy, z)T(z)(f(x, y)) = f(x, yz)f(y, z) \tag{5.5}$$

$$T(y) \circ T(x) = \gamma\left(f(x, y)\right) \circ T(xy) \tag{5.6}$$

$$f(1, 1) = 1 \tag{5.7}$$

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

The second condition (5.6) means, using the definition of γ

$$T(y)\,(T(x)(n)) = f(x,y)^{-1}T(xy)(n)f(x,y)$$

for all $n \in N$. Sometimes T is referred to as the automorphism system.

REMARK 5.2.7. If we choose $f(x,y) \equiv 1$ then (f,T) is called the *trivial* factor system. In that case T is a homomorphism by (5.6) and (5.5) reduces to $1 = 1$.

Condition (5.7) corresponds to a normalization. The first two conditions already imply the following conditions:

LEMMA 5.2.8. *Let (f,T) be a pair of functions as above where only conditions* (5.5) *and* (5.6) *are satisfied. Then it follows*

$$T(1) = \gamma(f(1,1)) \tag{5.8}$$

$$f(x,1) = f(1,1) \tag{5.9}$$

$$f(1,y) = T(y)(f(1,1)) \tag{5.10}$$

for all $x, y \in Q$.

PROOF. By (5.6) we have $T(1) \circ T(1) = \gamma(f(1,1))T(1)$ so that $T(1) = \gamma(f(1,1))$. It follows $f(1,1)^{-1}f(x,1)f(1,1) = T(1)(f(x,1))$ and hence

$$\begin{aligned} f(x,1)f(1,1) &= f(1,1)T(1)(f(x,1)) \\ &= f(x,1)T(1)(f(x,1)) \end{aligned}$$

where we have used (5.5) with $z = y = 1$ for the last equation. This shows (5.9).
Setting $x = y = 1$ in (5.5) we obtain

$$f(1,z)T(z)(f(1,1)) = f(1,z)f(1,z)$$

Multiplying $f(1,z)^{-1}$ from the left yields (5.10). □

COROLLARY 5.2.9. *Let (f,T) be a factor system to N and Q. Then*

$$f(x,1) = f(1,y) = 1 \tag{5.11}$$

$$T(1) = \mathrm{id}_{|N} \tag{5.12}$$

for all $x, y \in Q$.

PROOF. By (5.7) it follows $T(1) = \gamma(f(1,1)) = \gamma(1) = \mathrm{id}_{|N}$. Furthermore $f(x,1) = f(1,1) = 1$ and $f(1,y) = T(y)(1) = 1$ since $T(y)$ is an automorphism of N. □

We can associate a factor system with each group extension as follows.

PROPOSITION 5.2.10. *Each group extension $1 \to N \xrightarrow{\alpha} G \xrightarrow{\beta} Q \to 1$ together with a transversal function $\tau : Q \to G$ defines a factor system (f_τ, T_τ).*

This associated factor system depends not only on the extension, but also on the choice of a transversal function τ.

PROOF. Let $x \in Q \simeq G/\alpha(N)$ be a coset of $\alpha(N)$ in G and τ a fixed transversal function $x \mapsto \tau(x)$. It satisfies $\beta\tau = \mathrm{id}$ on Q. Since $\alpha(N)$ is normal in G, the element $\tau(x)^{-1}\alpha(n)\tau(x)$ is in $\alpha(N)$. We will denote it by

$$\alpha(T_\tau(x)(n)) = \tau(x)^{-1}\alpha(n)\tau(x) \tag{5.13}$$

where $T_\tau(x)(n) \in N$. This defines automorphisms $T_\tau(x)$ of N and a map $T_\tau : Q \to \mathrm{Aut}(N)$. Since β is a homomorphism we have

$$\beta(\tau(xy)^{-1}\tau(x)\tau(y)) = (\beta\tau)((xy)^{-1}) \cdot (\beta\tau)(x)(\beta\tau)(y) = (xy)^{-1}xy = 1$$

and hence $\tau(xy)^{-1}\tau(x)\tau(y) \in \ker\beta = \alpha(N)$. It follows that there exists a unique element $f_\tau(x,y) \in N$ such that

$$\tau(x)\tau(y) = \tau(xy)\alpha(f_\tau(x,y)) \tag{5.14}$$

Now we have to verify the conditions (5.5),(5.6),(5.7) for the pair (f_τ, T_τ) which we will denote by (f,T). We set

$$\tau(1) = 1 \tag{5.15}$$

This condition is not essential, but it helps simplify some of the computations. By (5.14) we have

$$\tau(1)\tau(1) = \tau(1)\alpha(f(1,1))$$

hence $\alpha(f(1,1)) = 1$ and $f(1,1) = 1$. Hence (5.7) is satisfied. By using (5.13) and (5.14) we obtain

$$\begin{aligned}(\alpha T(y)T(x))(n) &= \tau(y)^{-1}\tau(x)^{-1}\alpha(n)\tau(x)\tau(y)\\ &= (\alpha(f(x,y))^{-1} \cdot \tau(xy)^{-1}\alpha(n)\tau(xy) \cdot \alpha(f(x,y))\\ &= (\alpha(f(x,y))^{-1} \cdot \alpha(T(xy)(n)) \cdot \alpha(f(x,y))\end{aligned}$$

This implies (5.6). Using (5.14) we have

$$\begin{aligned}\tau((xy)z) &= \tau(xy)\tau(z)\,(\alpha(f(xy,z))^{-1}\\ &= \tau(x)\tau(y)\,(\alpha(f(x,y))^{-1} \cdot \tau(z)\,(\alpha(f(xy,z))^{-1}\\ \tau(x(yz)) &= \tau(x)\tau(yz)\,(\alpha(f(x,yz))^{-1}\\ &= \tau(x)\tau(y)\tau(z)\,(\alpha(f(y,z))^{-1}\,(\alpha(f(x,yz))^{-1}\end{aligned}$$

Using the associativity in G both terms must be equal, i.e.,

$$\begin{aligned}\alpha(f(x,yz))\alpha(f(y,z)) &= \alpha(f(xy,z)) \cdot \tau(z)^{-1}\alpha(f(x,y))\tau(z)\\ &= \alpha(f(xy,z) \cdot \alpha(T(z)(f(x,y))\end{aligned}$$

Since α is a monomorphism we obtain (5.5). □

Now we have associated a factor system (T_τ, f_τ) to a group extension and a transversal function τ. Does every factor system (f,T) arise in such a way ? The answer is given by the following proposition.

PROPOSITION 5.2.11. *For each factor system (f,T) to N and Q there is a group extension G of N by Q such that $(f,T) = (f_\tau, T_\tau)$ for a suitable choice of a transversal function τ.*

PROOF. Given (f,T) we define a group structure on $G = Q \times N$ as follows.

$$(x,a)\circ(y,b) = (xy, f(x,y)T(y)(a)b) \tag{5.16}$$

for $x,y \in Q$ and $a,b \in N$. This generalizes the construction of the outer semidirect product. If we choose the trivial factor system $f(x,y) = 1$ for all $x,y \in Q$, then $T : Q \to \mathrm{Aut}(N)$ is a homomorphism and the above definition coincides with the outer semidirect product $Q \ltimes_T N$. We need to show that the group laws are satisfied, that G is a group extension of N by Q and that (f_τ, T_τ) is exactly (f,T) with a suitable choice of τ. We start with the associativity. We have

$$\begin{aligned}(x,a)\circ[(y,b)\circ(z,c)] &= (x,a)\circ[yz, f(y,z)T(z)(b)c] \\ &= (xyz, f(x,yz)T(yz)(a)f(y,z)T(z)(b)c),\end{aligned}$$

and

$$\begin{aligned}[(x,a)\circ(y,b)]\circ(z,c) &= [xy, f(x,y)T(y)(a)b]\circ(z,c) \\ &= (xyz, f(xy,z)T(z)\big(f(x,y)T(y)(a)b\big)c) \\ &= (xyz, f(xy,z)T(z)(f(x,y))\cdot T(z)(T(y)(a)b)c) \\ &= (xyz, f(xy,z)T(z)(f(x,y))\cdot\gamma(f(y,z))(T(yz)(a))\cdot T(z)(b)c) \\ &= (xyz, f(x,yz)\cdot f(y,z)\gamma(f(y,z))(T(yz)(a))\cdot T(z)(b)c) \\ &= (xyz, f(x,yz)T(yz)(a)f(y,z)T(z)(b)c).\end{aligned}$$

In the second computation we have first used that $T(z)$ is an automorphism of N, then (5.6) and (5.5). Let $b := f(x,x^{-1})T(x^{-1})(a)$. Then (x^{-1},b^{-1}) is the inverse of (x,a).

$$(x,a)\circ(x^{-1},b^{-1}) = (xx^{-1}, f(x,x^{-1})T(x^{-1})(a)\cdot b^{-1}) = (1,1)$$

Clearly $(1,1)$ is the unit element

$$(1,1)\circ(y,b) = (y, f(1,y)T(y)(1)b) = (y,b)$$

Now define $\beta : G \to Q$ by $(x,a) \mapsto x$. This map is a surjective homomorphism:

$$\beta((x,a))\circ\beta((y,b)) = xy = \beta\big((xy, f(x,y)T(y)(a)b\big) = \beta((x,a)\circ(y,b))$$

where we have used (5.16) in the last step. The map $(1,a) \mapsto a$ is an isomorphism from $\ker\beta = \{(1,a) \mid a \in N\}$ to N:

$$(1,a)\circ(1,b) = (1, f(1,1)T(1)(a)b) = (1,ab)$$

The map $\alpha : N \to G$ defined by $a \mapsto (1, a)$ is a monomorphism. We obtain a short exact sequence $1 \to N \xrightarrow{\alpha} G \xrightarrow{\beta} Q \to 1$ and hence an extension G of N by Q.

The next step is to choose a transversal function $\tau : Q \to G$. The most natural choice is $\tau(x) = (x, 1)$. Since

$$\begin{aligned}\tau(x) \circ \tau(y) &= (x, 1) \circ (y, 1) = (xy, f(x, y)),\\ \tau(xy)\alpha(f(x, y)) &= (xy, 1) \circ (1, f(x, y)) = (xy, f(xy, 1)T(1)(1)f(x, y)\\ &= (xy, f(x, y))\end{aligned}$$

we have $\tau(x)\tau(y) = \tau(xy)\alpha(f(x, y))$. Comparing with (5.14), where $f_\tau(x, y)$ was uniquely determined, it follows $f_\tau = f$. Using (5.5) with $y = x^{-1}$ and $f(1, x) = f(x, 1) = 1$ we obtain $T(x)(f(x, x^{-1}) = f(x^{-1}, x)$. Since $T(x)$ is an automorphism it follows

$$T(x)(f(x, x^{-1})^{-1}) = f(x^{-1}, x)^{-1} \tag{5.17}$$

so that, using the formula for the composition of three elements from above

$$\begin{aligned}(x, 1)^{-1} \circ (1, a) \circ (x, 1) &= (x^{-1}, f(x^{-1}, x)^{-1}) \circ (1, a) \circ (x, 1)\\ &= (x \cdot 1 \cdot x^{-1}, f(x^{-1}, x)T(x)\left(f(x^{-1}, x)^{-1}\right) f(1, x)T(x)(a) \cdot 1)\\ &= (1, T(x)(a))\end{aligned}$$

This is just $\tau(x)^{-1}\alpha(a)\tau(x) = \alpha(T(x)(a))$ and a comparison with (5.13) shows $T_\tau = T$. □

Example 5.2.12. *Consider the extension* $1 \to C_2 \xrightarrow{\alpha} C_4 \xrightarrow{\beta} C_2 \to 1$ *where* $N = C_2 = \langle a\rangle$, $C_4 = \langle g\rangle$, $Q = C_2 = \langle x\rangle$ *and* $\alpha(a) = g^2$, $\beta(g) = x$. *Determine the associated factor system* (f_τ, T_τ) *where* τ *is given by* $\tau(1) = 1$, $\tau(x) = g$.

$T_\tau : C_2 \to \mathrm{Aut}(C_2)$ is given by $T_\tau(1) = T_\tau(x) = \mathrm{id}$ since $\alpha(T_\tau(x)(a)) = \tau(x)^{-1}\alpha(a)\tau(x) = g^{-1}g^2g = g^2$ and hence $T_\tau(x)(a) = a$. The map $f_\tau : C_2 \times C_2 \to C_2$ is given by

$$f(1, 1) = f(1, x) = f(x, 1) = 1,\ f(x, x) = a$$

We have to show only the last condition. It is $g \cdot g = \tau(x)\tau(x) = \alpha(f(x, x))$ so that $f(x, x) = a$.

Example 5.2.13. *Determine the group extension* $1 \to C_2 \xrightarrow{\alpha} G \xrightarrow{\beta} C_2 \to 1$ *to the above factor system* (f_τ, T_τ).

The group $G = \{(1, 1), (1, a), (x, 1), (x, a)\}$ has the following multiplication

$$(x, a) \circ (y, b) = (xy, f(x, y)ab)$$

Using $x^2 = a^2 = 1$ we obtain

$$\begin{aligned}(x, a)^4 = ((x, a) \circ (x, a))^2 &= (x^2, f(x, x)a^2)^2 = ((1, a))^2\\ &= (1, a) \circ (1, a) = (1, f(1, 1)a^2) = (1, 1)\end{aligned}$$

Since $(x,a)^2 = (1,a) \neq (1,1)$ the group G is isomorphic to C_4.

So far we have constructed a correspondence between factor systems (f,T) to N and Q and group extensions G of N by Q. However, the correspondence is not yet one-to-one. There are many factor systems (f_τ, T_τ) associated with one group extension. We will introduce an equivalence relation on the set of factor systems.

LEMMA 5.2.14. *Let $1 \to N \xrightarrow{\alpha} G \xrightarrow{\beta} Q \to 1$ be a group extension and (f,T), (f',T') two associated factor systems. Then there is a map $h : Q \to N$ such that*

$$T'(x) = \gamma(h(x)) \circ T(x) \tag{5.18}$$

$$f'(x,y) = h(xy)^{-1} f(x,y) \cdot T(y)(h(x)) \cdot h(y) \tag{5.19}$$

PROOF. The associated factor systems (f,T) and $f',T')$ arise by two transversal functions $\tau : Q \to G$ and $\tau' : Q \to G$. They just assign a given coset two representatives. Hence

$$\tau'(x) = \tau(x)\ell(x) \tag{5.20}$$

with a map $\ell : Q \to \alpha(N)$. Define $h : Q \to N$ by $\alpha(h(x)) = \ell(x)$. Using (5.13) we obtain

$$\begin{aligned} \alpha(T'(x)(n)) &= \tau'(x)^{-1}\alpha(n)\tau'(x) = \ell(x)^{-1} \cdot \tau(x)^{-1}\alpha(n)\tau(x) \cdot \ell(x) \\ &= \alpha\left(h(x)^{-1}\right) \cdot \alpha\left(T(x)(n)\right) \cdot \alpha(h(x)) \end{aligned}$$

so that $\alpha \circ T'(x) = \alpha \circ \gamma(h(x)) \circ T(x)$ and (5.18) follows. Using (5.14) we obtain

$$\begin{aligned} \alpha\left(f'(x,y)\right) &= \tau'(xy)^{-1}\tau'(x)\tau'(y) = \ell(xy)^{-1} \cdot \tau(xy)^{-1} \cdot \tau(x)\ell(x)\tau(y)\ell(y) \\ &= \ell(xy)^{-1}\alpha(f(x,y)) \cdot \tau(y)^{-1}\alpha(h(x))\tau(y) \cdot \ell(y) \\ &= \ell(xy)^{-1}\alpha(f(x,y)) \cdot \alpha(T(y))(h(x)) \cdot \ell(y) \\ &= \alpha\left(h(xy)^{-1}\right) \cdot \alpha(f(x,y)) \cdot \alpha(T(y)(h(x)) \cdot \alpha(h(y)) \end{aligned}$$

This implies (5.19). □

The Lemma tells us how to define the equivalence relation.

DEFINITION 5.2.15. Let (f,T) and (f',T') be two factor systems to N and Q. They are called *equivalent* if there is a map $h : Q \to N$ such that (5.18) and (5.19) are satisfied, and $h(1) = 1$.

If we take $h(x) = 1$ for all $x \in Q$ then it follows immediately $(f,T) = (f',T')$. Different choices of the transversal function τ lead to equivalent factor systems in our correspondence. Next we show that the equivalence relation is compatible with equivalent group extensions.

PROPOSITION 5.2.16. *Equivalent group extensions*

$$\begin{array}{ccccccccc} 1 & \longrightarrow & N & \xrightarrow{\alpha} & G & \xrightarrow{\beta} & Q & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle \mathrm{id}} & & \downarrow{\scriptstyle \varphi} & & \downarrow{\scriptstyle \mathrm{id}} & & \\ 1 & \longrightarrow & N & \xrightarrow{\gamma} & G' & \xrightarrow{\delta} & Q & \longrightarrow & 1 \end{array}$$

define equivalent factor systems.

PROOF. Choose any transversal function τ to the extension $1 \to N \xrightarrow{\alpha} G \xrightarrow{\beta} Q \to 1$ and let (f, T) denote the associated factor system. Let (f', T') the factor system associated with the extension $1 \to N \xrightarrow{\alpha} G \xrightarrow{\beta} Q \to 1$ and the following $\tau' : Q \to G$:

$$\tau'(x) = \varphi(\tau(x)) \tag{5.21}$$

Since $\gamma = \varphi\alpha$ and $\beta = \delta\varphi$ we have $\delta\tau' = \delta\varphi\tau = \beta\tau = \mathrm{id}$. So τ' is really a transversal function. Its choice is such that (f', T') coincides with (f, T). Hence the two factor systems are equivalent. In fact, by (5.13) we have

$$\begin{aligned} \gamma\left(T'(x)(a)\right) &= \tau'(x)^{-1}\gamma(a)\tau'(x) = \tau'(x)^{-1}\varphi(\alpha(a))\tau'(x) \\ &= \varphi(\tau(x)^{-1}) \cdot \varphi(\alpha(a)) \cdot \varphi(\tau(x)) = \varphi\big(\tau(x)^{-1}\alpha(a)\tau(x)\big) \\ &= (\varphi \circ \alpha)(T(x)(a)) = \gamma(T(x)(a)) \end{aligned}$$

Since γ is injective we have $T' = T$. Using (5.14) we have

$$\begin{aligned} \tau'(xy)\gamma(f'(x,y)) &= \tau'(x)\tau'(y) = \varphi(\tau(x)) \cdot \varphi(\tau(y)) \\ &= \varphi(\tau(x)\tau(y)) = \varphi[\tau(xy) \cdot \alpha(f(x,y))] \\ &= (\varphi\tau)(xy) \cdot (\varphi\alpha)(f(x,y)) = \tau'(xy)\gamma(f(x,y)) \end{aligned}$$

This implies $f'(x, y) = f(x, y)$ or $f' = f$. □

PROPOSITION 5.2.17. *Let N, Q be groups and (f, T), (f', T') be two factor systems to N and Q. If the factor systems are equivalent, so are the associated group extensions.*

PROOF. Assume that (f, T) and (f', T') are equivalent, so that there is a map $h : Q \to N$ satisfying (5.18) and (5.19). Let G, G' be the group extensions of N by Q as constructed in proposition 5.2.11. As a set, $G = G' = Q \times N$. We need to show that both extensions are equivalent, i.e., that there is a homomorphism $\varphi : G \to G'$ such that the diagram of proposition 5.2.16 commutes. We define φ by

$$(x, a) \mapsto (x, h(x)^{-1}a) \tag{5.22}$$

Clearly this map is bijective. It is also a homomorphism with respect to the composition (5.16).

$$\begin{aligned}\varphi(g\circ h) &= \varphi((x,a)\circ(y,b)) = \varphi\big((xy, f(x,y)T(y)(a)b)\big)\\ &= (xy, h(xy)^{-1}f(x,y)T(y)(a)b),\end{aligned}$$

$$\begin{aligned}\varphi(g)\circ\varphi(h) &= (x,h(x)^{-1}a)\circ(y,h(y)^{-1}b)\\ &= (xy, f'(x,y)\cdot T'(y)(h(x)^{-1}a)\cdot h(y)^{-1}b)\\ &= (xy, f'(x,y)\cdot[\gamma(h(y))\circ T(y)]((h(x)^{-1}a)h(y)^{-1}b))\\ &= (xy, h(xy)^{-1}f(x,y)T(y)(h(x))h(y)\cdot\\ &\qquad [\gamma(h(y))\circ T(y)]((h(x)^{-1}a)h(y)^{-1}b))\\ &= (xy, h(xy)^{-1}f(x,y)T(y)(h(x))\cdot T(y)(h(x)^{-1}a)h(y)h(y)^{-1}b)\\ &= (xy, h(xy)^{-1}f(x,y)T(y)(a)b).\end{aligned}$$

In the second computation we have used also (5.18) and (5.19). It remains to show that the diagram commutes. Since $h(1)=1$ we have $h(1)^{-1}=1$, so that we obtain

$$\begin{aligned}(\varphi\alpha)(a) &= \varphi((1,a)) = (1,h(1)^{-1}a) = (1,a) = \gamma(a)\\ (\delta\varphi)((x,a)) &= \delta((x,h(x)^{-1}a)) = x = \beta((x,a))\end{aligned}$$

It follows $\gamma=\varphi\alpha$ and $\beta=\delta\varphi$. □

Now we can formulate the main result of this section.

THEOREM 5.2.18 (Schreier). *Let N and Q be two groups. By associating every extension of N by Q a factor system one obtains a one-to-one correspondence between the set of equivalence classes of extensions of N by Q and the set of equivalence classes of factor systems to N and Q.*

In particular, if the factor set associated with the extension G of N by Q is equivalent to the *trivial* factor set then the extension G is equivalent to some semidirect product of N by Q. Conversely, the factor set associated with a semidirect product is equivalent to the trivial factor set.

CHAPTER 6

Cohomology of groups

We shall give here the original definition of the cohomology groups which is, unlike the definition of the derived functors, quite concrete.

6.1. G-modules

If G is a group, we define a G-module M to be an abelian group, written additively, on which G acts as endomorphisms. That means the following:

DEFINITION 6.1.1. Let G be a group. A *left G-module* is an abelian group M together with a map

$$G \times M \to M, \quad (g, m) \mapsto gm$$

such that, for all $g, h \in G$ and $m, n \in M$,

$$\begin{aligned} g(m+n) &= gm + gn \\ (gh)m &= g(hm) \\ 1m &= m \end{aligned}$$

Equivalently a left G-module is an abelian group M together with a group homomorphism

$$T\colon G \to \mathrm{Aut}(M)$$

where the correspondence is given by

$$T(g)(m) = gm \quad \forall\, m \in M$$

As in representation theory, we can transform this to a more familiar concept. Let $\mathbb{Z}[G]$ denote the group ring of G. This is the free $\mathbb{Z}$-module with the elements of G as base and in which multiplication is defined by

$$\left(\sum_g n_g g\right)\left(\sum_h m_h h\right) = \sum_{g,h} n_g m_h (gh)$$

where $n_g, m_h \in \mathbb{Z}$ and the sums are finite. For example, let $G = \mathbb{Z} = \langle t \rangle$. Then $\{t^i\}_{i\in\mathbb{Z}}$ is a $\mathbb{Z}$-basis of $\mathbb{Z}[G]$. Hence $\mathbb{Z}[G] = \mathbb{Z}[t, t^{-1}]$ is the ring of Laurent polynomials.
If M is a G-module, then M becomes a $\mathbb{Z}[G]$-module if we define

$$\left(\sum_g n_g g\right) m = \sum_g n_g (gm)$$

Conversely, if M is a $\mathbb{Z}[G]$-module, then M becomes a G-module if we define $gm := (1g)m$.

EXAMPLE 6.1.2. *Let M be any abelian group and define*

$$gm = m$$

for all $g \in G$, $m \in M$. This action of G is called the trivial action, and M is called a trivial G-module.

EXAMPLE 6.1.3. *The module $M = \mathbb{Z}[G]$ with the action*

$$h\left(\sum_g n_g g\right) = \sum_g n_g hg$$

is called the regular G-module.

DEFINITION 6.1.4. Let M be a G-module. Define

$$M^G = \{m \in M \mid gm = m \text{ for all } g \in G\}.$$

Then M^G is a submodule of M which is called the *module of invariants*.

If M is a trivial G-module then $M^G = M$.

DEFINITION 6.1.5. Let M, N be two G-modules. A homomorphism of G-modules is a map $\varphi\colon M \to N$ such that

$$\begin{aligned}\varphi(m + m') &= \varphi(m) + \varphi(m')\\ \varphi(gm) &= g\varphi(m)\end{aligned}$$

for all $g \in G$ and $m, m' \in M$. We write $\mathrm{Hom}_G(M, N)$ for the set of all G-module homomorphisms $\varphi\colon M \to N$.

6.2. The n-th cohomology group

Let A be a G-module and let $C^n(G, A)$ denote the set of functions of n variables

$$f : G \times G \times \cdots \times G \to A$$

into A. For $n = 0$ let $C^0(G, A) = \mathrm{Hom}(1, A) \cong A$. The elements of $C^n(G, A)$ are called *n-cochains*. The set $C^n(G, A)$ is an abelian group with the usual definitions of addition and the element 0:

$$\begin{aligned}(f + g)(x_1, \ldots, x_n) &= f(x_1, \ldots, x_n) + g(x_1, \ldots, x_n)\\ 0(x_1, \ldots, x_n) &= 0\end{aligned}$$

We now define homomorphisms $\delta = \delta_n : C^n(G, A) \to C^{n+1}(G, A)$.

DEFINITION 6.2.1. If $f \in C^n(G, A)$ then define $\delta_n(f)$ by

$$\begin{aligned}\delta_n(f)(x_1, \ldots, x_{n+1}) &= x_1 f(x_2, \ldots, x_{n+1}) \\ &\quad + \sum_{i=1}^{n} (-1)^i f(x_1, \ldots, x_{i-1}, x_i x_{i+1}, \ldots, x_{n+1}) \\ &\quad + (-1)^{n+1} f(x_1, \ldots, x_n)\end{aligned}$$

For $n = 0, 1, 2, 3$ we obtain

$$\begin{aligned}(\delta_0 f)(x_1) &= x_1 f - f \\ (\delta_1 f)(x_1, x_2) &= x_1 f(x_2) - f(x_1 x_2) + f(x_1) \\ (\delta_2 f)(x_1, x_2, x_3) &= x_1 f(x_2, x_3) - f(x_1 x_2, x_3) + f(x_1, x_2 x_3) - f(x_1, x_2) \\ (\delta_3 f)(x_1, x_2, x_3, x_4) &= x_1 f(x_2, x_3, x_4) - f(x_1 x_2, x_3, x_4) + f(x_1, x_2 x_3, x_4) \\ &\quad - f(x_1, x_2, x_3 x_4) + f(x_1, x_2, x_3)\end{aligned}$$

For $n = 0$, f is considered as an element of A so that $x_1 f$ makes sense.

We will show that $\delta^2(f) = 0$ for every $f \in C^n(G, A)$, i.e., $\delta_{n+1}\delta_n = 0$ for all $n \in \mathbb{N}$ and hence $\operatorname{im} \delta_n \subseteq \ker \delta_{n+1}$.

LEMMA 6.2.2. *It holds $\delta_{n+1}\delta_n(C^n(G, A)) = 0$ for all $n \in \mathbb{N}$. Hence the following sequence is a complex.*

$$A \xrightarrow{\delta_0} C^1(G, A) \xrightarrow{\delta_1} \cdots \xrightarrow{\delta_{n-1}} C^n(G, A) \xrightarrow{\delta_n} C^{n+1}(G, A) \xrightarrow{\delta_{n+1}} \cdots$$

PROOF. Let $f \in C^n(G, A)$. We want to show $\delta^2(f)(x_1, \ldots, x_{n+2}) = 0$. Define $g_j \in C^{n+1}(G, A)$ for $0 \leq j \leq n + 1$ by

$$g_j(x_1, \ldots, x_{n+1}) = \begin{cases} x_1 f(x_2, \ldots, x_{n+1}), & j = 0 \\ (-1)^j f(x_1, \ldots, x_j x_{j+1}, \ldots, x_{n+1}), & 1 \leq j \leq n \\ (-1)^{n+1} f(x_1, \ldots, x_n), & j = n + 1 \end{cases}$$

This means

$$(\delta f)(x_1, \ldots, x_{n+1}) = \sum_{j=0}^{n+1} g_j(x_1, \ldots, x_{n+1})$$

Then define $g_{ji} \in C^{n+2}(G, A)$ for $0 \leq i \leq n + 2$ by

$$g_{ji}(x_1, \ldots, x_{n+2}) = \begin{cases} x_1 g_j(x_2, \ldots, x_{n+2}), & i = 0 \\ (-1)^i g_j(x_1, \ldots, x_i x_{i+1}, \ldots, x_{n+2}), & 1 \leq i \leq n + 1 \\ (-1)^{n+2} g_j(x_1, \ldots, x_{n+1}), & i = n + 2 \end{cases}$$

This means

$$(\delta g_j)(x_1, \ldots, x_{n+2}) = \sum_{i=0}^{n+2} g_{ij}(x_1, \ldots, x_{n+2})$$

It follows

$$\delta^2(f)(x_1,\dots,x_{n+2}) = \sum_{j=0}^{n+1}(\delta g_j)(x_1,\dots,x_{n+2}) = \sum_{j=0}^{n+1}\sum_{i=0}^{n+2} g_{ij}(x_1,\dots,x_{n+2})$$

We will show that for all $0 \le j \le n+1$ and all $j+1 \le i \le n+2$

$$(g_{ji} + g_{i-1,j})(x_1,\dots,x_{n+2}) = 0 \tag{6.1}$$

This will imply our result as follows. Write down all g_{ji} as an $(n+2)\times(n+3)$ array and cancel out each pair $(g_{ji}, g_{i-1,j})$ starting with $j=0$ and $i=1,\dots,n+2$, then $j=1$ and $i=2,\dots n+2$, until $j=n+1$ and $i=n+2$. Then all entries of the array are canceled out and we obtain $\delta^2(f) = \sum_{j=0}^{n+1}\sum_{i=0}^{n+2} g_{ij} = 0$.
It remains to show (6.1). Assume first $1 \le j \le n$. If $i > j+1$ then

$$\begin{aligned} g_{ji}(x_1,\dots,x_{n+2}) &= (-1)^i g_j(x_1,\dots,x_ix_{i+1},\dots,x_{n+2}) \\ &= (-1)^i g_j(\tau_1,\dots,\tau_{n+1}) \\ &= (-1)^{i+j} f(\tau_1,\dots,\tau_j\tau_{j+1},\dots,\tau_{n+1}) \\ &= (-1)^{i+j} f(x_1,\dots,x_jx_{j+1},\dots,x_ix_{i+1},\dots,x_{n+2}) \end{aligned}$$

with

$$\begin{gathered}(\tau_1,\dots,\tau_j,\tau_{j+1},\dots,\tau_i,\tau_{i+1},\dots,\tau_{n+1}) = \\ (x_1,\dots,x_j,x_{j+1},\dots,x_ix_{i+1},x_{i+2},\dots,x_{n+2}).\end{gathered}$$

On the other hand we have

$$\begin{aligned} g_{i-1,j}(x_1,\dots,x_{n+2}) &= (-1)^j g_{i-1}(x_1,\dots,x_jx_{j+1},\dots,x_{n+2}) \\ &= (-1)^j g_{i-1}(\sigma_1,\dots,\sigma_j,\dots,\sigma_{n+1}) \\ &= (-1)^{i-1+j} f(\sigma_1,\dots,\sigma_{i-1}\sigma_i,\dots,\sigma_{n+1}) \\ &= (-1)^{i+j-1} f(x_1,\dots,x_jx_{j+1},\dots,x_ix_{i+1},\dots,x_{n+2}) \end{aligned}$$

with

$$\begin{gathered}(\sigma_1,\dots,\sigma_{j-1},\sigma_j,\dots,\sigma_{i-1},\sigma_i,\dots,\sigma_{n+1}) = \\ (x_1,\dots,x_{j-1},x_jx_{j+1},\dots,x_i,x_{i+1},\dots,x_{n+2}).\end{gathered}$$

It follows $g_{ij} + g_{i-1,j} = 0$. If $i = j+1$ we obtain in the same way

$$\begin{aligned} g_{ji}(x_1,\dots,x_{n+2}) &= (-1)^{i+j} f(x_1,\dots,x_{i-1}x_ix_{i+1},\dots,x_{n+2}) \\ &= -g_{i-1,j}(x_1,\dots,x_{n+2}) \end{aligned}$$

The remaining cases $j=0$ and $j=n+1$ follow similarly. □

Define the subgroups $Z^n(G,A) = \ker\delta_n$ and $B^n(G,A) = \operatorname{im}\delta_{n-1}$. For $n=0$ let $B^0(G,A) = 0$. Since $B^n(G,A) \subseteq Z^n(G,A)$ we can form the factor group:

Definition 6.2.3. The *n-th cohomology group* of G with coefficients in A is given by the factor group

$$H^n(G,A) = Z^n(G,A)/B^n(G,A) = \ker\delta_n/\operatorname{im}\delta_{n-1}$$

6.3. The zeroth cohomology group

For $n = 0$ we have

$$H^0(G, A) = Z^0(G, A) = \{a \in A \mid xa = a \; \forall \, x \in G\} = A^G.$$

Hence $H^0(G, A) = A^G$ is the module of invariants.

Let L/K be a finite Galois extension with Galois group $G = Gal(L/K)$. Then L and $L^\times$ are G-modules. Here L is regarded as a group under addition and $L^\times$ is the multiplicative group of units in L. We have

$$H^0(G, L^\times) = (L^\times)^G = K^\times$$

Let p be a prime and C_p the cyclic group of order p.

EXAMPLE 6.3.1. *Let $A = C_p$ be a $G = C_p$-module. Then $xa = a$ for all $x \in C_p$, i.e., A is a trivial C_p-module. We have*

$$H^0(C_p, C_p) = C_p$$

Denote by xa the action of G on A. Let $T : C_p \to \mathrm{Aut}(C_p) \cong C_{p-1}$ be the homomorphism defined by $xa = T(x)a$. Now $\ker T$ being a subgroup of C_p must be trivial or equal to C_p, since p is prime. However $\ker T = 1$ is impossible since T is not injective. In fact, C_p is not contained in $\mathrm{Aut}(C_p)$. Hence it follows $\ker T = C_p$ and $T(C_p) = \{id\}$. This means $xa = T(x)a = a$. Since A is a trivial C_p-module it follows $A^G = A$.

LEMMA 6.3.2. *Let M be a G-module, and regard $\mathbb{Z}$ as a trivial G-module. Then*

$$H^0(G, M) = M^G \cong \mathrm{Hom}_G(\mathbb{Z}, M)$$

PROOF. A G-module homomorphism $\varphi : \mathbb{Z} \to M$ is uniquely determined by $\varphi(1)$, and $m \in M$ is the image of 1 under φ if and only if it is fixed by G, i.e., if $m \in M^G$.

$$gm = g(\varphi(1)) = \varphi(g \cdot 1) = \varphi(1) = m$$

Here $g \cdot 1 = 1$ since G acts trivially on $\mathbb{Z}$. □

6.4. The first cohomology group

If A is a G-module then

$$Z^1(G, A) = \{f : G \to A \mid f(xy) = xf(y) + f(x)\}$$
$$B^1(G, A) = \{f : G \to A \mid f(x) = xa - a \text{ for some } a \in A\}$$

The 1-cocycles are also called crossed homomorphisms of G into A. A 1-coboundary is a crossed homomorphism, i.e., $\delta_1\delta_0 = 0$. For the convenience of the reader we repeat the calculation. Let $f = \delta_0(a)(x_1) = x_1a - a$ and compute

$$\begin{aligned}(\delta_1\delta_0)(a)(x, y) = \delta_1(f)(x, y) &= xf(y) - f(xy) + f(x) \\ &= x(ya - a) - (xy)a + a + xa - a \\ &= 0\end{aligned}$$

Hence $(\delta_1\delta_0)(a) = 0$. Let A be a trivial G-module. Then a crossed homomorphism is just a group homomorphism, i.e., $Z^1(G, A) = \mathrm{Hom}(G, A)$, $B^1(G, A) = 0$ and

$$H^1(G, A) = \mathrm{Hom}(G, A)$$

is the set of group homomorphisms from G into A.

REMARK 6.4.1. We want to consider sometimes right G-modules instead of left G-modules. If A is a left $\mathbb{Z}[G]$-module with action $(x, a) \mapsto xa$, then $a * x = xa$ defines a right module action with multiplication $y * x = xy$ in G: $a * (x * y) = (yx)a = y(xa) = (a * x) * y$. Then the definition of 1-cocycles and 1-coboundaries becomes

$$Z^1(G, A) = \{f : G \to A \mid f(x * y) = f(x) * y + f(y)\}$$
$$B^1(G, A) = \{f : G \to A \mid f(x) = a * x - a \text{ for some } a \in A\}$$

PROPOSITION 6.4.2. *Let A be a G-module. There exists a bijection between $H^1(G, A)$ and the set of conjugacy classes of subgroups $H \leq G \ltimes A$ complementary to A in which the conjugacy class of G maps to zero.*

PROOF. There is a bijection between subgroups $H \leq G \ltimes A$ complementary to A and 1-cocycles $h \in Z^1(G, A)$. If H is complementary to A then $H = \tau(G)$ for a section $\tau : G \to G \ltimes A$ for $\pi : G \ltimes A \to G$. Writing $\tau(x) = (x, h(x))$ with $h : G \to A$ we have $H = \{(x, h(x)) \mid x \in G\}$. We want to show that $h \in Z^1(G, A)$. The multiplication in $G \ltimes A$ is given by (5.1), with $\varphi(y)a = ay$ for $y \in G$ and $a \in A$. Note that this is a right action. Since we write A additively, the formula becomes

$$(x, a)(y, b) = (xy, ay + b)$$

Since $\tau(xy) = \tau(x)\tau(y)$ we have

$$(xy, h(xy)) = (x, h(x))(y, h(y)) = (xy, h(x)y + h(y))$$

so that $h(xy) = h(x)y + h(y)$. The converse is also clear. Moreover two complements are conjugate precisely when their 1-cocycles differ by a 1-coboundary: for $a \in A \leq G \ltimes A$ the set aHa^{-1} consists of all elements of the form

$$(1, a)(x, h(x))(1, -a) = (x, ax - a - h(x))$$

Hence the cosets of $B^1(G, A)$ in $Z^1(G, A)$ correspond to the A-conjugacy classes of complements H in A, or in $G \ltimes A$ since $G \ltimes A = HA$. □

COROLLARY 6.4.3. *All the complements of A in $G \ltimes A$ are conjugate iff $H^1(G, A) = 0$.*

We have the following result on cohomology groups of *finite* groups.

PROPOSITION 6.4.4. *Let G be a finite group and A be a G-module. Then every element of $H^1(G, A)$ has a finite order which divides $|G|$.*

PROOF. Let $f \in Z^1(G, A)$ and $a = \sum_{y \in G} f(y)$. Then $xf(y) - f(xy) + f(x) = 0$. Summing over this formula we obtain

$$\begin{aligned} 0 &= x \sum_{y \in G} f(y) - \sum_{y \in G} f(xy) + f(x) \sum_{y \in G} 1 \\ &= xa - a + |G| f(x) \end{aligned}$$

It follows that $|G|f(x) \in B^1(G, A)$, which implies
$|G|Z^1(G, A) \subseteq B^1(G, A)$. Hence $|G|H^1(G, A) = 0$. □

COROLLARY 6.4.5. *Let G be a finite group and A be a finite G-module such that $(|G|, |A|) = 1$. Then $H^1(G, A) = 0$.*

PROOF. We have $|A|f = 0$ for all $f \in C^1(G, A)$. Then the order of $[f] \in H^1(G, A)$ divides $(|G|, |A|) = 1$. Hence the class $[f]$ is trivial. □

REMARK 6.4.6. We will show later that $H^n(G, A) = 0$ for all $n \in \mathbb{N}$ if the conditions of the corollary are satisfied.

We shall conclude this section by proving the following result which can be found already in Hilbert's book *Die Theorie der algebraischen Zahlkörper* of 1895. It is called Hilbert's Satz 90 and we present a generalization of it due to Emmy Noether.

PROPOSITION 6.4.7. *Let L/K be a finite Galois extension with Galois group $G = Gal(L/K)$. Then we have $H^1(G, L^\times) = 1$ and $H^1(G, L) = 0$.*

PROOF. We have to show $Z^1 = B^1$ in both cases. Let $f \in Z^1(G, L^\times)$. This implies $f(\sigma) \neq 0$ for all $\sigma \in G$ since $f : G \to L^\times$. The 1-cocycle condition is, written multiplicatively, $f(\sigma\tau) = f(\sigma)\sigma f(\tau)$ or $\sigma f(\tau) = f(\sigma)^{-1} f(\sigma\tau)$. The 1-coboundary condition is $g(\sigma) = \sigma(a)/a$ for a constant a. By a well known result on the linear independence of automorphisms it follows that there exists a $\beta \in L^\times$ such that

$$\alpha := \sum_{\tau \in G} f(\tau)\tau(\beta) \neq 0$$

It follows that for all $\sigma \in G$

$$\begin{aligned}\sigma(\alpha) &= \sum_{\tau \in G} \sigma(f(\tau))\sigma(\tau(\beta)) = \sum_{\tau \in G} f(\sigma)^{-1} f(\sigma\tau)\sigma\tau(\beta) = f(\sigma)^{-1} \sum_{\tau \in G} f(\tau)\tau(\beta) \\ &= f(\sigma)^{-1}\alpha\end{aligned}$$

It follows $f(\sigma) = \frac{\alpha}{\sigma(\alpha)} = \frac{\sigma(\alpha^{-1})}{\alpha^{-1}}$, hence $f \in B^1(G, L^\times)$.
For the second part, let $f \in Z^1(G, L)$. Since L/K is separable there exists a $\beta \in L$ such that

$$a := \sum_{\tau \in G} \tau(\beta) = Tr_{L/K}(\beta) \neq 0$$

Setting $\gamma = a^{-1}\beta$ we obtain $\sum_{\tau \in G} \tau(\gamma) = 1$ since $\tau(a) = a$ and $\tau(a^{-1}) = a^{-1}$. Let

$$x := \sum_{\tau \in G} f(\tau)\tau(\gamma)$$

Hence we obtain for all $\sigma \in G$

$$\begin{aligned}\sigma(x) &= \sum_{\tau \in G} \sigma(f(\tau))\sigma\tau(\gamma) = \sum_{\tau \in G} f(\sigma\tau)\sigma\tau(\gamma) - f(\sigma)\sigma\tau(\gamma) \\ &= x - f(\sigma)\end{aligned}$$

It follows $f(\sigma) = x - \sigma(x) = \sigma(-x) - (-x)$, hence $f \in B^1(G, L)$. □

REMARK 6.4.8. We have $H^n(G, L) = 0$ for all $n \in \mathbb{N}$, but not $H^n(G, L^\times) = 1$ in general.

6.5. The second cohomology group

Let G be a group and A be an abelian group. We recall the definition of a factor system, written additively for A. A pair of functions (f, T), $f : G \times G \to A$ and $T : G \to \mathrm{Aut}(A)$ is called factor system to A and G if

$$f(xy, z) + f(x, y)z = f(x, yz) + f(y, z) \tag{6.2}$$

$$T(xy) = T(y)T(x) \tag{6.3}$$

$$f(1, 1) = 0 \tag{6.4}$$

where $f(x, y)z = T(z)(f(x, y))$. Now let

$$0 \to A \xrightarrow{\alpha} E \xrightarrow{\beta} G \to 1$$

be an abelian group extension of A by G. This equips A with a natural G-module structure. We obtain $T(x)(a) = xa$, or $T(x)(a) = ax$, for $x \in G$ and $a \in A$, which is independent of a transversal function. In fact, the extension induces an (anti)homomorphism $T_\tau : G \to \mathrm{Aut}(A)$ with a transversal function $\tau : G \to E$, see chapter 1. Since A is abelian it follows $\gamma_{h(x)} = \mathrm{id}_{|A}$ so that $T_{\tau'}(x) = \gamma_{h(x)}T_\tau(x) = T_\tau(x)$. If we fix T and hence the G-module structure on A, then the set of factor systems $f = (f, T)$ to A and G forms an abelian group with respect to addition: $(f + g)(x, y) = f(x, y) + g(x, y)$. It follows from (6.2) that this group is contained in the group

$$Z^2(G, A) = \{f : G \times G \to A \mid f(y, z) - f(xy, z) + f(x, yz) - f(x, y)z = 0\}$$

where we have considered A as a right G-module. One has to rewrite the 2-cocycle condition from definition (6.2.1) for a right G-module according to remark (6.4.1). Recall that

$$B^2(G, A) = \{f : G \times G \to A \mid f(x, y) = h(y) - h(xy) + h(x)y\}$$

is a subgroup of $Z^2(G, A)$ and the factor group is $H^2(G, A)$. Indeed, a 2-coboundary is a 2-cocycle. The sum of the following terms equals zero.

$$\begin{aligned} f(y, z) &= h(z) - h(yz) + h(y)z \\ -f(xy, z) &= -h(z) + h(xyz) - h(xy)z \\ f(x, yz) &= h(yz) - h(xyz) + h(x)yz \\ -f(x, y)z &= -h(y)z + h(xy)z - h(x)yz \end{aligned}$$

Theorem 6.5.1. *Let G be a group and A be an abelian group, and let M denote the set of group extensions*

$$0 \to A \xrightarrow{\alpha} E \xrightarrow{\beta} G \to 1$$

with a given G-module structure on A. Then there is a $1-1$ correspondence between the set of equivalence classes of extensions of A by G contained in M with the elements of $H^2(G, A)$. The class of split extensions in M corresponds to the class $[0] \in H^2(G, A)$. This class corresponds to the trivial class represented by the trivial factor system $f(x, y) = 0$.

Proof. By Theorem 5.2.18 the set of equivalence classes of such extensions is in bijective correspondence with the equivalence classes of factor systems $f \in Z^2(G, A)$. Two factor systems are equivalent if and only if they differ by a 2-coboundary in $B^2(G, A)$: by (5.19) we have

$$f_{\tau'}(x, y) = f_\tau(x, y) - h(xy) + h(x)y + h(y)$$

Note that there is exactly one normalized 2-cocycle in each cohomology class, i.e., with $f(1,1) = 0$. Hence two extensions of A by G contained in M are equivalent if and only if they determine the same element of $H^2(G,A)$. □

EXAMPLE 6.5.2. *Let $A = \mathbb{Z}/p\mathbb{Z}$ be a trivial $G = C_p$-module. Then*

$$H^2(G,A) \cong \mathbb{Z}/p\mathbb{Z}.$$

Here p is a prime. There are exactly p equivalence classes of extensions

$$0 \to \mathbb{Z}/p\mathbb{Z} \xrightarrow{\alpha} E \xrightarrow{\beta} C_p \to 1$$

EXAMPLE 6.5.3. *Consider the Galois extension $L/K = \mathbb{C}/\mathbb{R}$ with Galois group $G = Gal(\mathbb{C}/\mathbb{R}) \cong C_2$. Then we have*

$$H^2(G, L^\times) \cong \mathbb{Z}/2\mathbb{Z}$$

The proof is left as an exercise. In general we have $H^2(G, L^\times) \cong \mathrm{Br}(L/K)$, where $\mathrm{Br}(L/K)$ is the *relative Brauer group*. It consists of equivalence classes of central simple K-algebras S such that $S \otimes_K L \cong M_n(L)$. Two central simple K-algebras are called equivalent if their skew-symmetric components are isomorphic. For any field K the equivalence classes of finite-dimensional central simple K-algebras form an abelian group with respect to the multiplication induced by the tensor product.
The group $\mathrm{Br}(\mathbb{C}/\mathbb{R})$ consists of two equivalence classes. The matrix algebra $M_2(\mathbb{R})$ represents the class [0] and the real quaternion algebra $\mathbb{H}$ represents the class [1].
We will now generalize Proposition (6.4.4).

PROPOSITION 6.5.4. *Let G be a finite group and A be a G-module. Then every element of $H^n(G,A)$, $n \in \mathbb{N}$, has a finite order which divides $|G|$.*

PROOF. Let $f \in C^n(G,A)$ and denote

$$a(x_1, \ldots, x_{n-1}) = \sum_{y \in G} f(x_1, \ldots, x_{n-1}, y)$$

Summing the formula for δf and using

$$\sum_{y \in G} f(x_1, \ldots, x_{n-1}, x_n y) = a(x_1, \ldots, x_{n-1})$$

we obtain

$$\begin{aligned}\sum_{y \in G} (\delta f)(x_1, \ldots, x_n, y) &= x_1 a(x_2, \ldots, x_n) \\ &\quad + \sum_{i=1}^{n-1} (-1)^i a(x_1, \ldots, x_i x_{i+1}, \ldots, x_n) + (-1)^n a(x_1, \ldots, x_{n-1}) \\ &\quad + (-1)^{n+1} |G| f(x_1, \ldots, x_n) \\ &= (\delta a)(x_1, \ldots, x_n) + (-1)^{n+1} |G| f(x_1, \ldots, x_n)\end{aligned}$$

Hence if $\delta f = 0$, then $|G| f(x_1, \ldots, x_n) = \pm(\delta a)(x_1, \ldots, x_n)$ is an element of $B^n(G,A)$. Then $|G| Z^n(G,A) \subseteq B^n(G,A)$, so that $|G| H^n(G,A) = 0$. □

COROLLARY 6.5.5. *Let G be a finite group and A be a finite G-module such that $(|G|, |A|) = 1$. Then $H^n(G, A) = 0$ for all $n \geq 1$. In particular, $H^2(G, A) = 0$. Hence any extension of A by G is split.*

The last part is a special case of the Schur-Zassenhaus theorem, see (5.1.27). We will sketch the proof of the general case.

SCHUR-ZASSENHAUS 6.5.6. *If n and m are relatively prime, then any extension $1 \to A \xrightarrow{\alpha} E \xrightarrow{\beta} G \to 1$ of a group A of order n by a group G of order m is split.*

PROOF. If A is abelian, the extensions are classified by the groups $H^2(G, A)$, one group for every G-module structure on A. These are all zero, hence any extension of A by G is split.
In the general case we use induction on n. It suffices to prove that E contains a subgroup S of order m. Such a subgroup must be isomorphic to G under $\beta : E \to G$. For, if S is such a subgroup, then $S \cap A$ is a subgroup whose order divides $|S| = m$ and $|A| = n$. Then $S \cap A = 1$. Also $AS = E$ since $\alpha(A) = A$ is normal in E so that AS is a subgroup whose order is divided by $|S| = m$ and $|A| = n$ and so is a multiple of $nm = |E|$. It follows that E is a semidirect product and hence the extension of A by G is split.
Choose a prime p dividing n and let P be a p-Sylow subgroup of A, hence of E. Let Z be the center of P. We known that $Z \neq 1$. Let N be the normalizer of Z in E. A counting argument shows that $AN = E$ and $|N/(A \cap N)| = m$. Hence there is an extension $1 \to (A \cap N) \to N \to G \to 1$. If $N \neq E$, this extension splits by induction, so there is a subgroup of N, and hence of E, isomorphic to G. If $N = E$, then $Z \lhd E$ and the extension $1 \to A/Z \to E/Z \to G \to 1$ is split by induction. Let G' be a subgroup of E/Z isomorphic to G and let E' denote the set of all $x \in E$ mapping onto G'. Then E' is a subgroup of E, and $0 \to Z \to E' \to G' \to 1$ is an extension. As Z is abelian, the extension splits and there is a subgroup of E', hence of E, isomorphic to $G' \cong G$. □

6.6. The third cohomology group

We have seen that $H^n(G, A)$ for $n = 0, 1, 2$ have concrete group-theoretic interpretations. It turns out that this is also the case for $n \geq 3$. We will briefly discuss the case $n = 3$, which is connected to so called *crossed modules*. Such modules arise also naturally in topology.

DEFINITION 6.6.1. Let E and N be groups. A *crossed module* (N, α) over E is a group homomorphism $\alpha \colon N \to E$ together with an action of E on N, denoted by $(e, n) \mapsto {}^e n$ satisfying

$$ {}^{\alpha(m)}n = m\, n\, m^{-1} \tag{6.5} $$

$$ \alpha({}^e n) = e\, \alpha(n)\, e^{-1} \tag{6.6} $$

for all $n, m \in N$ and all $e \in E$.

EXAMPLE 6.6.2. *Let $E = \mathrm{Aut}(N)$ and $\alpha(n)$ be the inner automorphism associated to n. Then (N, α) is a crossed module over E.*

By definition we have ${}^{\alpha(m)}n = \alpha(m)(n) = m\, n\, m^{-1}$ and

$$\begin{aligned} \alpha({}^e n)(m) &= \alpha(e(n))(m) = e(n)me(n)^{-1} = e(ne^{-1}(m)n^{-1}) = e(\alpha(n)(e^{-1}(m))) \\ &= (e\alpha(n)e^{-1})(m) \end{aligned}$$

EXAMPLE 6.6.3. *Any normal subgroup $N \lhd E$ is a crossed module with E acting by conjugation and α being the inclusion.*

Let (N, α) be a crossed module over E and $A := \ker \alpha$. Then the sequence $0 \to A \xrightarrow{i} N \xrightarrow{\alpha} E$ is exact. Since $\operatorname{im} \alpha$ is normal in E by (6.6) $G = \operatorname{coker}(\alpha)$ is a group. This means that the sequence $N \xrightarrow{\alpha} E \xrightarrow{\pi} G \to 1$ is exact. Since A is central in N by (6.5), and since the action of E on N induces an action of G on A, we obtain a 4-term exact sequence

$$0 \to A \xrightarrow{i} N \xrightarrow{\alpha} E \xrightarrow{\pi} G \to 1 \tag{6.7}$$

where A is a G-module. It turns out that equivalence classes of exact sequences of this form are classified by the group $H^3(G, A)$. Let us explain the equivalence relation. Let G be an arbitrary group and A be an arbitrary G-module. Consider all possible exact sequences of the form (6.7), where N is a crossed module over E such that the action of E on N induces the given action of G on A. We take on these exact sequences the smallest equivalence relation such that two exact sequences as shown below are equivalent whenever their diagram is commutative:

$$\begin{array}{ccccccccc}
1 & \longrightarrow & A & \longrightarrow & N & \xrightarrow{\alpha} & E & \longrightarrow & G & \longrightarrow & 1 \\
 & & \downarrow{\scriptstyle \mathrm{id}} & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle g} & & \downarrow{\scriptstyle \mathrm{id}} & & \\
1 & \longrightarrow & A & \longrightarrow & N' & \xrightarrow{\alpha'} & E' & \longrightarrow & G & \longrightarrow & 1
\end{array}$$

Note that f and g need not be isomorphisms. We then have:

THEOREM 6.6.4. *There is a $1-1$ correspondence between equivalence classes of crossed modules represented by sequences as above and elements of $H^3(G, A)$.*

We omit the proof, which can be found in [**12**], Theorem 6.6.13.

Bibliography

[1] G. Baumslag: *Wreath products and finitely presented groups.* Math. Zeitschrift **75** (1961), 22–28.

[2] H. U. Besche, B. Eick, E. A. O'Brien: *A millennium project: constructing small groups.* Internat. J. Algebra Comput. **12** (2002), no. 5, 623-644.

[3] H. G. Bray: *A note on CLT groups.* Pacific Journal of Mathematics **27** (1968), no. 2., 229-231.

[4] F. Barry, D. MacHale, A. N. Shé: *Some Supersolvability conditions for finite groups.* Math. Proceedings of the Royal Irish Academy **167** (1996), 163–177.

[5] J. Dénes, P. Erdös, P. Turán: *On some statistical properties of the alternating group of degree n.* Extrait de L'Enseigment mathématique **15** (1969), no. 2, 89-99.

[6] W. Feit, J. Thompson: *Solvability of groups of odd order.* Pacific J. Math. **13** (1963), 775–1029.

[7] G. H Hardy, E. M. Wright: *An Introduction to the Theory of Numbers.* Oxford University Press (1979).

[8] G. Higman: *Enumerating p-groups. I: Inequalities.* Proc. London Math. Soc. (3) **10** (1960), 24–30.

[9] J. S. Milne: *Group Theory*, Version 3.13 (2013), 1–135.

[10] L. Pyber: *Enumerating finite groups of given order.* Annals of Math. (2) **137** (1993), no. 1, 203-220.

[11] M. Suzuki: *Group Theory I.* Grundlehren der Mathematischen Wissenschaften, Band 247, Springer Verlag **1982**.

[12] C. A. Weibel: *An introduction to homological algebra.* Cambridge University Press **1997**.