Group Theory

University of Vienna Summer 2024

Lecturer Balázs Szendrői

Lecture notes by Dietrich Burde 2017,
extended by Balázs Szendrői 2023

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.

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 $C_n = \langle r\rangle = \{e, r, r^2, \ldots, r^{n-1}\}$.

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

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

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 $\mathrm{Sym}(X)$.

For $X = \{1, 2, \ldots, n\}$ the group $\mathrm{Sym}(X)$ 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 $L\colon G \hookrightarrow \mathrm{Sym}(G)$. 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. For M a subset of X, a *symmetry* of M is an isometry of X fixing M. Symmetries of M form a subgroup $\mathrm{Sym}(M)$ of $\mathrm{Isom}(X)$.

DEFINITION 1.2.10. 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 1.2.11. 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 1.2.12. 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 1.2.13. 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 $z \mapsto z + 2\pi ik$ 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, normal subgroups and the Isomorphism Theorems

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 $H = G = \{e, g, g^2, \dots g^{p-1}\}$. □

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. For example, consider the quaternion group $Q_8 = \{1, -1, i, -i, j, -j, k, -k\}$ with group operation defined by $i^2 = j^2 = k^2 = -1$ and $ij = k$, $ji = -k$, $jk = i$, $kj = -i$ and $ki = j$, $ik = -j$. Of course, Q_8 is not abelian, as $ij = -ji$. It can be checked (see Exercises) that every subgroup of the quaternion group Q_8 is normal.

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 such that $\pi\colon G \to G/N$, $a \mapsto aN$ is a homomorphism with kernel N. Indeed, for a subgroup H of G, requiring that there should be a well-defined group operation on the set of cosets G/H so that the map $a \mapsto aH$ is a group homomorphism is equivalent to the requirement that H be normal in G.

We finally recall

THEOREM 1.3.16 (The Isomorphism Theorems).

(1) *Let $\varphi\colon G \to H$ be a group homomorphism. Then $K = \ker \varphi$ is a normal subgroup of G, and the map $g \mapsto gK$ induces an isomorphism of groups $G/K \cong \operatorname{im} \varphi$.*
(2) *Let G be a group. Let H be a subgroup of G, and let N be a normal subgroup of G. Then the following hold:*
   - *The product HN is a subgroup of G containing N as a normal subgroup.*
   - *The intersection $H \cap N$ is a normal subgroup of H.*
   - *The quotient groups HN/N and $H/(H \cap N)$ are isomorphic.*

EXAMPLE 1.3.17.

(1) The Special Linear group $SL_n(K)$ is the kernel of the group homomorphism

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

and hence a normal subgroup of $GL_n(K)$ with quotient group $GL_n(K)/SL_n(K) \cong K^\times$.
(2) The alternating group A_n is the kernel of the signature group homomorphism

$$\operatorname{sign} : S_n \to \{1, -1\}.$$

Hence $(S_n : A_n) = 2$ and A_n is a normal subgroup of S_n with quotient group $S_n/A_n \cong \{1, -1\} \cong C_2$.

1.4. Permutation groups

We already have defined the symmetric group S_n as $\mathrm{Sym}(X)$, where X has n elements. A permutation $\pi \in S_n$ is given by

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

Note that we are considering permutations as bijections, and we have the rule

$$(\pi_2 \circ \pi_1)(i) = \pi_2(\pi_1(i)).$$

As the group operation in S_n is composition, when computing the product $\pi_2\pi_1$ of two elements of the symmetric group S_n, the "right hand element is done first".

Given a permutation $\pi \in S_n$, 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. Algebraically, we can use the following

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

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

Then even permutations have sign $+1$, and odd permutations have sign -1.

We have $\mathrm{sign}(\sigma\circ\tau) = \mathrm{sign}(\sigma)\mathrm{sign}(\tau)$ for all $\sigma, \tau \in S_n$, so that $\mathrm{sign}\colon S_n \to \{\pm 1\}$, $\pi \mapsto \mathrm{sign}(\pi)$ 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 $\pi \in S_n$ as a disjoint product of cycles. For example,

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

The order of π is the lcm of the cycle orders, which are $2, 5$ and 1, hence the order of π is $\mathrm{lcm}(2, 5) = 10$. 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

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

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 [**6**]:

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 [**3**] 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 and Sylow theory

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 $p^r \,||\, |G|$ 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 $p \nmid m$, that $(H:1) \leq p^r$, 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. □

LEMMA 2.3.14. *Let $N_1, N_2 \lhd G$ be normal subgroups of a finite group G, of coprime order. Then elements of N_1 commute with elements of N_2.*

PROOF. Since N_1 and N_2 have relatively primes orders, $N_1 \cap N_2$ is the trivial group by Lagrange's theorem. For $a \in N_1$ and $b \in N_2$, we have

$$aba^{-1}b^{-1} = (aba^{-1})b^{-1} = a(ba^{-1}b^{-1}) \in N_1 \cap N_2,$$

so that

$$aba^{-1}b^{-1} = e$$

and reordering, we get $ab = ba$. □

COROLLARY 2.3.15. *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 l that

$$P_1 \cdots P_l \cong P_1 \times \cdots \times P_l.$$

For $l = 1$ there is nothing to prove, so that we may assume the statement for $l - 1$. Then $P_1 \cdots P_{l-1}$ and P_l are both normal subgroups of G, of relatively prime orders. Hence by Lemma 2.3.14, their elements commute in G. Hence the map

$$(P_1 \times \cdots \times P_{l-1}) \times P_l \to (P_1 \cdots P_{l-1}) \cdot P_l$$

defined by multiplying elements together, is an isomorphism also, proving the induction step. For $k = l$, we get that

$$P_1 \cdots P_k \cong P_1 \times \cdots \times P_k,$$

a subgroup of G of order $\prod_i p_i^{r_i}$, the order of G. Hence this subgroup must be the whole of G and so

$$G \cong P_1 \times \cdots \times P_k.$$

□

EXAMPLE 2.3.16. 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 2.3.15, $G = H \times K$, and both H and K are commutative. Hence G is commutative.

REMARK 2.3.17. The same argument shows that every group of order p^2q with primes $p < q$ and $q \not\equiv 1 \bmod p$ is commutative.

PROPOSITION 2.3.18. *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 2.3.14 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 2.3.19. Every group of order 15 is cyclic.

PROPOSITION 2.3.20. *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 2.3.21. *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 2.3.22. *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 2.3.23. *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. Applications to (non)-simple groups

Recall that a group G is *simple*, if it has no nontrivial normal subgroup. Note that a p-group can never be simple; indeed, by Proposition 2.2.7, every p-group G has a nontrivial center $Z(G) \leq G$, which is certainly a non-trivial normal subgroup. We can apply the Sylow Theorems to show that groups of more general order also have non-trivial proper normal subgroups, and hence they too cannot be simple. We start with a Lemma.

LEMMA 2.4.1. *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

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

Let $N = \ker(\theta)$, a normal subgroup of G; N fixes the identity coset, so $N \leq H$. 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. □

PROPOSITION 2.4.2. *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 2.4.1 shows that H is normal. Since $|H| = q^r$, this is a proper normal subgroup. □

Here is another result of the same nature, whose proof also uses Sylow theory.

PROPOSITION 2.4.3. *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. □

All these results are special cases of the following famous result of Burnside, which we mention without proof.

THEOREM 2.4.4 (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 2.4.5. *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. $\square$

CHAPTER 3

Semidirect products and applications

3.1. On automorphism groups

Recall from Definition 1.2.6 that for completely general reasons, the set of automorphisms $\mathrm{Aut}(G)$ of a group G itself forms a group. The inner automorphisms of G are the automorphims $i_g : G \to G$ given by $i_g(x) = gxg^{-1}$. Inner automorphisms form a subgroup $\mathrm{Inn}(G) \leq \mathrm{Aut}(G)$ of the automorphism group of G.

LEMMA 3.1.1. *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 (check!) with kernel $Z(G)$ (check!). By the isomorphism theorem, $G/\ker(\varphi) \cong \mathrm{im}(\varphi)$, which gives the claim. □

EXAMPLE 3.1.2. 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 3.1.3. $\mathrm{Inn}(G)$ *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 3.1.4. Let G be a group. The quotient group

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

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 3.1.5. *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.

3.2. Semidirect products

A semidirect product of two groups is a generalization of the direct product, involving group automorphisms.

Let N be a normal subgroup of a group 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 3.2.1. 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 3.2.2. 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 3.2.3. 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, and $Q = \langle (12) \rangle$ 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. Q_8 cannot be written as a semidirect product of two non-trivial subgroups.

Turning things round, given two groups N and Q and a homomorphism $\theta\colon Q \to \mathrm{Aut}(N)$, we can construct the semidirect product $N \rtimes_\theta Q$ (sometimes called the outer semidirect product) as follows. As a set, let $G = N \times Q$. Define the composition in G by

$$(n, q)(n', q') = (n \cdot \theta(q)(n'), qq'). \tag{3.1}$$

Proposition 3.2.4. *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 3.2.5. 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 $q \in Q, n \in N$.

3.3. Applications to classification questions

EXAMPLE 3.3.1. 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 3.2.3, and we have $D_3 \cong S_3$.

EXAMPLE 3.3.2. 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 2.3.18.

PROPOSITION 3.3.3. *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 2.4.1, 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 3.3.4. *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 3.3.5. 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.

Bibliography

[1] M. Artin, Algebra, Pearson, 2nd edition 2010.

[2] G. Baumslag: *Wreath products and finitely presented groups.* Math. Zeitschrift **75** (1961), 22–28.

[3] 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.

[4] H. G. Bray: *A note on CLT groups.* Pacific Journal of Mathematics **27** (1968), no. 2., 229–231.

[5] F. Barry, D. MacHale, A. N. Shé: *Some Supersolvability conditions for finite groups.* Math. Proceedings of the Royal Irish Academy **167** (1996), 163–177.

[6] 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.

[7] W. Feit, J. Thompson: *Solvability of groups of odd order.* Pacific J. Math. **13** (1963), 775–1029.

[8] G. Higman: *Enumerating p-groups. I: Inequalities.* Proc. London Math. Soc. (3) **10** (1960), 24–30.

[9] D. E. Joyce, The 17 plane symmetry groups, `https://www2.clarku.edu/faculty/djoyce/wallpaper/seventeen.html`.

[10] L. Pyber: *Enumerating finite groups of given order.* Annals of Math. (2) **137** (1993), no. 1, 203–220.