Lecture Notes

Math 111A (Algebra)

Summer 2016

(Robert Boltje, UCSC)

Contents

1 Prerequisites

1.1 Notation (Numbers and sets) (a) $\mathbb{N} := \{1, 2, 3, \ldots\}$ denotes the set of positive integers. If we include the number 0 we use the symbol $\mathbb{N}_0 := \{0, 1, 2, \ldots, \}$. The set of all *integers* will be denoted by $\mathbb{Z} := \{\ldots, -2, -1, 0, 1, 2, \ldots\}$. Furthermore, we write $\mathbb{Q} := \{\frac{a}{b} \mid a \in \mathbb{Z}, b \in \mathbb{N}\}$ for the set of all *rational numbers*, $\mathbb{R}$ for the set of all *real numbers*, and $\mathbb{C} := \{a + bi \mid a, b \in \mathbb{R}\}$ for the set of *complex numbers*.

(b) If S is a set we write $|S| \in \mathbb{N}_0 \cup \{\infty\}$ for the *cardinality* of S, i.e., the number of elements of S. The empty set has cardinality 0 and is denoted by $\emptyset$. We call S a *finite set* if $|S| < \infty$. If T is a subset of S we indicated this by writing $T \subseteq S$. If T is a *proper* subset of S, i.e., $T \subseteq S$ and $T \neq S$, then we indicate this by $T \subset S$.

1.2 Definition (Functions) Assume that $f\colon S \to T$ is a function between two sets S and T.

(a) The function f is called *surjective* if every element in T can be written as $f(s)$ for some $s \in S$. And f is called *injective* if for any two elements $s_1, s_2 \in S$ with $s_1 \neq s_2$ one has $f(s_1) \neq f(s_2)$. If f is injective and surjective, we call f *bijective*. In this case, for every $t \in T$, there exists a unique element $s \in S$ with $f(s) = t$, and we denote the map that sends t to s by $f^{-1}\colon T \to S$. This map is called the *inverse* of f and it satisfies $f^{-1} \circ f = \mathrm{id}_S$ and $f \circ f^{-1} = \mathrm{id}_T$. Note that the function f is bijective if and only if there exists a function $g\colon T \to S$ such that $g \circ f = \mathrm{id}_S$ and $f \circ g = \mathrm{id}_T$ (see Exercise 1(a)-(c)). Here, id_S denotes the *identity function* of S. It is defined by $\mathrm{id}_S(s) = s$ for all $s \in S$.

(b) If $U \subseteq S$ we set $f(U) := \{f(u) \mid u \in U\}$, the *image of U under f*. Note that $f(U) \subseteq T$. And if $V \subseteq T$ we set $f^{-1}(V) := \{s \in S \mid f(s) \in V\}$, the *preimage of V under f*. Note that $f^{-1}(V) \subseteq S$. We emphasize that the symbol $f^{-1}(V)$ is defined even if f is not bijective. In the case that f is bijective, the preimage of V under f coincides with the image of V under f^{-1}, so that there is no ambiguity with this notation.

1.3 Proposition (Division with remainder) *Let $n \in \mathbb{N}$ and let $a \in \mathbb{Z}$. Then there exist unique numbers $q \in \mathbb{Z}$ and $r \in \{0, 1, \ldots, n-1\}$ such that $a = qn + r$. The number q is called the* quotient *and the number r is called the* remainder *of the division of a by n.*

> For example, if $n = 5$ and $a = 17$ then $q = 3$ and $r = 2$ ($17 = 3 \cdot 5 + 2$), and if $n = 5$ and $a = -17$ then $q = -4$ and $r = 3$ ($-17 = (-4) \cdot 5 + 3$).

Proof Since the union of the integer 'intervals' $\{qn, qn+1, qn+2, \ldots, qn+(n-1)\}$, $q \in \mathbb{Z}$, is equal to $\mathbb{Z}$, there must exist $q \in \mathbb{Z}$ with $qn \leqslant a \leqslant qn+(n-1)$. We set $r := a - qn$. This shows the existence of the numbers q and r. Assume that one also has $a = q'n + r'$ for

numbers $q' \in \mathbb{Z}$ and $r' \in \{0, 1, \ldots, n-1\}$. Then $n > |r - r'| = |q'n - qn| = |q' - q|n \geqslant 0$. This implies $|q' - q| = 0$, and then $|r - r'| = 0$. □

1.4 Definition (Congruences) Let $n \in \mathbb{N}$. For integers $a, b \in \mathbb{Z}$, we write

$$a \equiv b \mod n \quad (\text{or also } a \overset{n}{\equiv} b)$$

if n divides $a - b$ (notation $n \mid a - b$), i.e., if there exists $q \in \mathbb{Z}$ with $a - b = qn$. In this case we say that a and b are *congruent modulo* n. The statement $a \equiv b \mod n$ is called a *congruence modulo* n.

For instance: $17 \equiv 2 \mod 5$, and $-4 \equiv 6 \mod 10$.

1.5 Proposition *Let $n \in \mathbb{N}$.*

(a) *Congruence modulo n defines an equivalence relation on $\mathbb{Z}$. The equivalence class that contains an integer a is also called the* congruence class of a modulo n. *The congruence class of a modulo n is equal to*

$$a + n\mathbb{Z} := \{a + nk \mid k \in \mathbb{Z}\}.$$

(b) *If a, b, c, d are integers and if $a \equiv b \mod n$ and $c \equiv d \mod n$ then*

$$\begin{aligned} a + c &\equiv b + d \mod n, \\ a - c &\equiv b - d \mod n, \\ ac &\equiv bd \mod n, \end{aligned}$$

In other words, one can add, subtract and multiply congruences.

(c) *If $a, b, c \in \mathbb{Z}$ and if $a \equiv b \mod n$ then $a + c \equiv b + c \mod n$, $a - c \equiv b - c \mod n$ and $ac = bc \mod n$.*

(d) *If $r \in \{0, 1, \ldots, n-1\}$ is the remainder of the division of a by n then $a \equiv r \mod n$.*

(e) *The set of integers is partitioned into n distinct congruence classes modulo n, namely the classes of the numbers $0, 1, \ldots, n-1$.*

Proof (a) Reflexivity: For every $a \in \mathbb{Z}$ we have $a \equiv a \mod n$, since $a - a = 0 \cdot n$. Symmetry: If $a \equiv b \mod n$ then one can write $a - b = qn$ for some $q \in \mathbb{Z}$. This implies $b - a = (-q)n$ and therefore $b \equiv a \mod n$. Transitivity: If $a \equiv b \mod n$ and $b \equiv c \mod n$ then one can write $a - b = q_1 n$ and $b - c = q_2 n$ for some $q_1, q_2 \in \mathbb{Z}$. Adding these two equations we obtain $a - c = (q_1 + q_2)n$ and therefore $a \equiv c \mod n$.

If b belongs to the congruence class of a modulo n then $b \equiv a \mod n$ and there exists $q \in \mathbb{Z}$ such that $b - a = qn$. This implies that $b = a + nq \in a + n\mathbb{Z}$. Conversely, if $b \in a + n\mathbb{Z}$ then there exists $q \in \mathbb{Z}$ with $b = a + nq$. This implies $b - a = nq$ and $b \equiv a \mod n$. Therefore, b belongs to the congruence class of a modulo n.

(b) Since $a \equiv b \mod n$ and $c \equiv d \mod n$ there exist $q_1, q_2 \in \mathbb{Z}$ such that $a - b = q_1 n$ (1) and $c - d = q_2 n$ (2). Adding equation (1) and (2) yields $(a + c) - (b + d) = (q_1 + q_2)n$ and therefore $a + c \equiv b + d \mod n$. Subtracting equation (2) from equation (1) yields $(a-c)-(b-d) = (q_1-q_2)n$ and therefore $a-c \equiv b-d \mod n$. Finally, multiplying equation (1) by c yields $ac - bc = q_1 cn$ and multiplying equation (2) by b yields $bc - bd = q_2 bn$. Adding these two equations now gives $ac - bd = (q_1 c + q_2 b)n$ and therefore, $ac \equiv bd \mod n$

(c) These are special cases of (b) with $c = d$.

(d) If $a = qn + r$ with $q \in \mathbb{Z}$ then $a \equiv qn + r \equiv 0 + r \equiv r \mod n$, by (c). Since congruence modulo n is an equivalence relation, we obtain $a \equiv r \mod n$.

(e) By (d) every congruence class modulo n is equal to the congruence class containing one of the elements $0, 1, \ldots, n-1$. On the other hand, if $0 \leqslant r < s \leqslant (n-1)$ then r and s lie in different congruence classes, since $0 < s - r < n$. □

> For instance, if $n = 2$ then the set of even integers is one congruence class and the set of odd integers is the other congruence class modulo 2. And if $n = 3$, the three congruence classes modulo 3 are given by $\{\ldots, -6, -3, 0, 3, 6, \ldots\}$, $\{\ldots, -5, -2, 1, 4, 7, \ldots\}$ and $\{\ldots, -4, -1, 2, 5, 8, \ldots\}$.

1.6 Corollary *Let $n \in \mathbb{N}$ and let $a, b \in \mathbb{Z}$. Let r_1 and r_2 be the remainders of the division of a and b by n, respectively. Then:*

$$a \equiv b \mod n \iff r_1 = r_2 \,.$$

Proof Write $a = q_1 n + r_1$ and $b = q_2 n + r_2$ with $q_1, q_2 \in \mathbb{Z}$ and $r_1, r_2 \in \{0, 1, \ldots, n-1\}$ according to Proposition 1.3. Then a lies in the congruence class of r_1 and b lies in the congruence class of r_2 by Proposition 1.5(d). So, a and b are congruent modulo n if and only if r_1 and r_2 are. But, by Proposition 1.5(e), this is the case if and only if $r_1 = r_2$. □

Exercises for §1

1. Let S and T be sets and let $f\colon S \to T$ be a function. Prove the following statements:

(a) If U is a set and $g\colon T \to U$ is a function such that $g \circ f$ is injective then also f is injective.

(b) If R is a set and $h\colon R \to S$ is a function such that $f \circ h$ is surjective then also f is surjective.

(c) Show that if $g, h\colon T \to S$ are functions satisfying $g \circ f = \mathrm{id}_S$ and $f \circ h = \mathrm{id}_T$ then f is bijective and $g = h = f^{-1}$. (Use (a) and (b)).

(d) Show that for subsets V_1 and V_2 one has $f^{-1}(V_1 \cup V_2) = f^{-1}(V_1) \cup f^{-1}(V_2)$ and $f^{-1}(V_1 \cap V_2) = f^{-1}(V_1) \cap f^{-1}(V_2)$. (Here, f is not assumed to be bijective.)

(e) Show that for subsets U_1 and U_2 one has $f(U_1 \cup U_2) = f(U_1) \cup f(U_2)$ and $f(U_1 \cap U_2) \subseteq f(U_1) \cap f(U_2)$. Give an example where the last inclusion is not an equality.

2. Assume that n is a natural number. Let $d_0, d_1, \ldots, d_r \in \{0, \ldots, 9\}$ be its decimals, read from right to left; that is, $n = d_0 + d_1 10 + d_2 10^2 + \cdots + d_r 10^r$.

(a) Show that $n \equiv d_0 + \cdots + d_r \mod 9$.

(b) Show that n is divisible by 9 if and only if $d_0 + \cdots + d_r$ is divisible by 9.

(c) Show that n is divisible by 3 if and only if $d_0 + \cdots + d_r$ is divisible by 3.

(d) Show that $n \equiv d_0 - d_1 + d_2 - + \cdots \mod 11$.

(e) Show that n is divisible by 11 if and only if $d_0 - d_1 + - \cdots$ is divisible by 11.

(f) Compute the remainder of 2015 after division by 11, without carrying out the division.

2 Binary operations, binary structures, homomorphisms

2.1 Definition A *binary operation* on a set S is a function

$$*\colon S \times S \to S\,.$$

For $a, b \in S$, we usually write $a * b$ instead of $*(a, b)$. We also say the $(S, *)$ is a *binary structure*.

> The choice of the symbol $*$ is arbitrary. One could have used any other symbol, as for example "$\triangle$", "$\square$", "$\bullet$", etc. For specific examples of binary operations one uses more descriptive symbols. If the operation is "addition" one uses usually "$+$", if it is "multiplication", one uses "$\cdot$", and if it is the "composition of functions" one usually uses "$\circ$".

2.2 Examples (a) $+\colon \mathbb{N} \times \mathbb{N} \to \mathbb{N}$, $(a, b) \mapsto a + b$, defines a binary operation on the set of natural numbers.

(b) $-\colon \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$, $(a, b) \mapsto a - b$, defines a binary operation on the set of integers.

(c) $*\colon \mathbb{Q} \times \mathbb{Q} \to \mathbb{Q}$, $(a, b) \mapsto \frac{a+b}{2}$, defines a binary operation on the set of rational numbers.

(d) For any sets X and Y let $F(X, Y)$ denote the set of functions $f\colon X \to Y$. Then, for every set X, the composition of functions defines a binary operation on the set $F(X, X)$, namely $(f, g) \mapsto f \circ g$.

(e) For any set X let $\mathcal{P}(X)$ denote the *power set* of X, i.e., the set of all subsets of X. Then $(\mathcal{P}(X), \cup)$ and $(\mathcal{P}(X), \cap)$ are binary structures.

2.3 Definition Let $*\colon S \times S \to S$ be a binary operation on a set S. We say that a subset T of S is *closed* under $*$ if for any two elements $a, b \in T$ one also has $a * b \in T$. In this case, $(T, *)$ is again a binary structure.

> For instance, $\mathbb{N}$ is closed in $(\mathbb{Z}, +)$, but not in $(\mathbb{Z}, -)$.

2.4 Definition Let $*\colon S \times S \to S$ be a binary operation on a set S.

(a) $*$ is called *commutative* if $a * b = b * a$ for all $a, b \in S$.

(b) $*$ is called *associative* if $(a * b) * c = a * (b * c)$ for all $a, b, c \in S$.

(c) An element $e \in S$ is called an *identity element* (or short an *identity*) for $*$ if $a * e = a = e * a$ for all $a \in S$.

2.5 Proposition *Let $*\colon S \times S \to S$ be a binary operation on a set S. Then S can have at most one identity element.*

Proof If e and e' are identity elements of S for $*$ then $e = e * e' = e'$. Here, the first equation uses that e' is an identity element, and the second equation uses that e is an identity element. □

2.6 Examples (a) $(\mathbb{N}, +)$ is a commutative and associative binary structure. It does not have an identity element.

(b) $(\mathbb{N}_0, +)$ is an associative and commutative binary structure with identity element 0.

(c) $(\mathbb{Z}, -)$ is not commutative, not associative, and has no identity element.

(d) $(\mathbb{Q}, *)$ with $a * b = \frac{a+b}{2}$ is a commutative binary structure. It is not associative and does not have an identity element.

(e) Let X be a set. Then, $(F(X, X), \circ)$ is an associative binary structure with identity element id_X. If X has more than 1 element then it is not commutative.

(f) Let X be a set. The binary structures $(\mathcal{P}(X), \cup)$ and $(\mathcal{P}(X), \cap)$ are commutative, associative and have identity elements, namely $\emptyset$ and X, respectively.

2.7 Remark (a) If $(S, *)$ is an associative binary structure then one can omit parenthesis. Expressions like $a * b * c$ or $a * b * c * d$ are then unambiguous. In fact, no matter how one groups these expressions by parentheses, they give the same result. This can be proved with little effort by induction on the number of factors. For instance, repeated application of the associativity law gives $((a * b) * c) * d = (a * b) * (c * d) = a * (b * (c * d))$.

(b) One can define or depict a binary operation $*$ on a finite set S by a square table. If $S = \{a, b, c\}$, for instance, then $*$ is depicted in the form

$*$	a	b	c
a	$a * a$	$a * b$	$a * c$
b	$b * a$	$b * b$	$b * c$
c	$c * a$	$c * b$	$c * c$

We will call such tables often 'multiplication tables'. Usually there is no preferred ordering of the elements of a set S. Different orderings usually lead to different multiplication tables of the same binary structure. The following tables describe 4 different binary structures:

$+$	0
0	0

$\cdot$	0	1
0	0	0
1	0	1

$\cdot$	1	0
1	1	0
0	0	0

$\cdot$	1	-1
1	1	-1
-1	-1	1

$+_2$	0	1
0	0	1
1	1	0

The second and third table describe the *same* binary structure. The fourth and fifth describe so-called *isomorphic* binary structures. It will be explained in the next definition what this precisely means. A binary operation is commutative if and only if the associated table is symmetric with respect to the diagonal. However, associativity cannot be read off the table as quickly.

2.8 Definition Let $(S, *)$ and $(T, \square)$ be binary structures.

(a) A function $f\colon S \to T$ is called a *homomorphism of binary structures* from $(S, *)$ to $(T, \square)$ if

$$f(a * b) = f(a) \square f(b)$$

for all $a, b \in S$. A bijective homomorphism is called an *isomorphism*.

(b) $(S, *)$ and $(T, \square)$ are called *isomorphic*, and we write $(S, *) \cong (T, \square)$, if there exists an isomorphism $f\colon S \to T$.

2.9 Examples (a) The binary structures $(\{0, 1\}, +_2)$ and $(\{1, -1\}, \cdot)$ from Remark 2.7 are isomorphic. In fact, the function $f\colon \{0, 1\} \to \{1, -1\}$ given by $f(0) = 1$ and $f(-1) = -1$ is an isomorphism. In terms of tables this just means the following: If one applies the function f to every element in the first table then one obtains the second table (possibly after reordering the elements in the second set).

(b) We write $\mathbb{R}_{>0}$ for the set of positive real numbers. With this notation, $(\mathbb{R}, +) \cong (\mathbb{R}_{>0}, \cdot)$, since the exponential function $\exp\colon \mathbb{R} \to \mathbb{R}_{>0}$, $x \mapsto e^x$, is an isomorphism. In fact, the function exp is bijective and $e^{a+b} = e^a \cdot e^b$, for all $a, b \in \mathbb{R}$.

2.10 Proposition *Let $(S, *)$, $(T, \square)$ and $(U, \triangle)$ be binary structures.*

(a) *If $f\colon (S, *) \to (T, \square)$ is an isomorphism and $e \in S$ is an identity element for $*$ then $f(e) \in T$ is an identity element for $\square$.*

(b) *If $f\colon (S, *) \to (T, \square)$ is an isomorphism then $f^{-1}\colon (T, \square) \to (S, *)$ is also an isomorphism.*

(c) *If $f\colon (S, *) \to (T, \square)$ and $g\colon (T, \square) \to (U, \triangle)$ are homomorphisms then also $g \circ f\colon (S, *) \to (U, \triangle)$ is a homomorphism. If f and g are isomorphisms then also $g \circ f$ is an isomorphism and $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.*

(d) *'Being isomorphic' is an equivalence relation on binary structures.*

Proof (a) Let $b \in T$. We need to show that $f(e) \square b = b = b \square f(e)$. Since f is surjective, there exists $a \in S$ such that $f(a) = b$. Therefore, $f(e) \square b = f(e) \square f(a) = f(e * a) = f(a) = b$ and, similarly, $b \square f(e) = b$.

(b) Since f is bijective, also f^{-1} is bijective. Therefore it suffices to show that, for all $b, b' \in T$, one has $f^{-1}(b \square b') = f^{-1}(b) * f^{-1}(b')$. Since f is surjective, there exist $a, a' \in S$ such that $f(a) = b$ and $f(a') = b'$. But then we have

$$f^{-1}(b \square b') = f^{-1}(f(a) \square f(a')) = f^{-1}(f(a * a')) = a * a' = f^{-1}(b) * f^{-1}(b') \,.$$

(c) Let $a, a' \in S$. Then

$$(g \circ f)(a * a') = g(f(a * a')) = g(f(a) \square f(a')) = g(f(a)) \triangle g(f(a')) = (g \circ f)(a) \triangle (g \circ f)(a').$$

This shows that $g \circ f$ is a homomorphism.

If f and g are isomorphisms then $g \circ f$ is a homomorphism by the first part of (c) and it is also bijective, since f and g are bijective. Thus, $g \circ f$ is an isomorphism. Finally, $(g \circ f) \circ (f^{-1} \circ g^{-1}) = \mathrm{id}_U$ and $(f^{-1} \circ g^{-1}) \circ (g \circ f) = \mathrm{id}_S$, since composition of functions is associative. Thus, $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

(d) Reflexivity follows from the fact that the identity map is always an isomorphism from a binary structure to itself. Symmetry follows from part (b), and transitivity follows from part (c). □

2.11 Remark An isomorphism $f\colon (S, *) \to (T, \square)$ does the following. It matches up the elements of S with the elements of T such that the binary operations on S and T are respected in the following sense: If $a * b = c$ holds in S then $f(a) \square f(b) = f(c)$ holds in T. In other words, if one applies f to all entries in a multiplication table of $(S, *)$, one obtains a multiplication table of $(T, \square)$.

If $(S, *)$ and $(T, \square)$ are isomorphic binary structures then every true statement that only involves S and $*$ can be translated via an isomorphism $f\colon S \to T$ into a similar true statement about T and $\square$. In this sense, $(S, *)$ and $(T, \square)$ have the same properties and every isomorphism transfers a property of S to the same property of T.

For instance, if $(S, *)$ and $(T, \square)$ are isomorphic, then $(S, *)$ is commutative if and only if $(T, \square)$ is commutative, and $(S, *)$ is associative if and only if $(T, \square)$ is associative (See Exercise 4).

Exercises for §2

1. Let $S = \{a, b, c, d, e\}$ and let $*$ be the binary operation on S defined by the following table:

$*$	a	b	c	d	e
a	a	b	c	b	d
b	b	c	a	e	c
c	c	a	b	b	a
d	b	e	b	e	d
e	d	b	a	d	c

(a) Is $*$ commutative?

(b) Is $*$ associative?

2. Suppose that $*$ is an associative and commutative binary operation on a set S. Show that the subset

$$T := \{a \in S \mid a * a = a\}$$

of S is closed under $*$.

3. Let $f\colon \mathbb{Q} \to \mathbb{Q}$ defined by $f(x) = 3x - 1$.

(a) Show that f is bijective and compute f^{-1}.

(b) Find a binary operation $*$ on $\mathbb{Q}$ such that $f\colon (\mathbb{Q}, +) \to (\mathbb{Q}, *)$ is an isomorphism.

(c) Find a binary operation $*$ on $\mathbb{Q}$ such that $f\colon (\mathbb{Q}, *) \to (\mathbb{Q}, +)$ is an isomorphism.

4. Assume that $(S, *)$ and $(T, \square)$ are isomorphic binary structures.

(a) Show that $(S, *)$ is commutative if and only if $(T, \square)$ is commutative.

(b) Show that $(S, *)$ is associative if and only if $(T, \square)$ is associative.

3 Groups

3.1 Definition (a) A binary structure $(G, *)$ is called a *group* if it satisfies the following axioms:

(i) $*$ is associative.

(ii) $(G, *)$ has an identity element e.

(iii) For every element $a \in G$ there exists an element $a' \in G$ with $a*a' = e = a'*a$.

(b) A group $(G, *)$ is called an *abelian* group if $*$ is commutative.

(c) If $(G, *)$ is a group, the number of elements in G is called the *order* of G and it is denoted by $|G|$. A group is called a *finite group* if its order is finite.

3.2 Remark Every group $(G, *)$ is a binary structure. The notions of *homomorphism* and *isomorphism* between two groups are the same as those of the underlying binary structures. Again, two groups are called *isomorphic*, if there exists an isomorphism between them. Note that if $(S, *)$ and $(T, \Box)$ are isomorphic binary structures and one of them is a group, then also the other one is a group (See Exercise 1).

3.3 Proposition *Let $(G, *)$ be a group.*

(a) *The left and right cancellation laws hold: If a, b, c are elements of G with $a*b = a*c$ then $b = c$; and if $a, b, c \in G$ satisfy $b * a = c * a$ then $b = c$.*

(b) *For $a, b \in G$, the equation $a * x = b$ has a unique solution in G and also the equation $x * a = b$ has a unique solution in G.*

(c) *For every element $a \in G$, there exists precisely one element $a' \in G$ satisfying $a * a' = e = a' * a$. This element will be called the* inverse *of a, and it will be denoted by a^{-1}.*

(d) *For $a, b \in G$, one has $(a * b)^{-1} = b^{-1} * a^{-1}$. Moreover $e^{-1} = e$.*

Proof (a) Assume that $a * b = a * c$. By the group axiom (iii), there exists an element $a' \in G$ such that $a' * a = e$. Therefore, $b = e * b = (a' * a) * b = a' * (a * b) = a' * (a * c) = (a' * a) * c = e * c = c$. Similarly, one shows that the right cancellation law holds.

(b) By axiom (iii) there exists $a' \in G$ with $a * a' = e = a' * a$. Therefore, $a * (a' * b) = (a * a') * b = e * b = b$ and $x = a' * b$ is a solution. If also $a * y = b = a * x$ then the left cancellation law implies $y = x$. Similarly, one shows the second part.

(c) By axiom (iii) there exists an element $a' \in G$ such that $a * a' = e$ and $a' * a = e$. By Part (b), a' is uniquely determined by either of these two properties.

(d) One has $(a*b)*(b^{-1}*a^{-1}) = ((a*b)*b^{-1})*a^{-1} = (a*(b*b^{-1}))*a^{-1} = (a*e)*a^{-1} = a*a^{-1} = e$ and similarly one has $(b^{-1}*a^{-1})*(a*b) = e$. Therefore, $b^{-1}*a^{-1}$ is the inverse element of $a*b$. Finally, since $e*e = e$, the element e is the inverse of e. □

3.4 Remark (a) If the binary operation of a group is written *additively*, i.e., using the symbol '+', then one usually denotes the identity element by 0 and the inverse of an element a by $-a$. If the binary operation is written *multiplicatively*, i.e, using the symbols $\cdot$, $\circ$, or the general symbol $*$ then we always denote the inverse of an element a by a^{-1}. In the multiplicative case we often denote the identity element by 1 instead of e. It is a standard convention that additive notation may only be used for commutative groups.

(b) The statements in Proposition 3.3(a) and (b) imply that in the multiplication table of a finite group, every group element occurs precisely once in every row and every column.

3.5 Examples (a) $(\mathbb{Z}, +)$ is an abelian group.

(b) $(\{1, -1\}, \cdot)$ is an abelian group.

(c) Let $n \in \mathbb{N}$ and let $\mathbb{Z}_n := \{0, 1, \ldots, n-1\}$. We define a binary operation $+_n$ on the set $\mathbb{Z}_n$ by the following rule. If $a, b \in \mathbb{Z}_n$, let $a +_n b$ be the remainder of $a + b$ after division by n. Note that $a +_n b \equiv a + b \mod n$, by Proposition 1.5(d). We show that $(\mathbb{Z}_n, +_n)$ is an abelian group. First we check that $+_n$ is associative. Let $a, b, c \in \mathbb{Z}_n$. Then $(a +_n b) +_n c \equiv (a +_n b) + c \equiv (a + b) + c = a + (b + c) \equiv a + (b +_n c) \equiv a +_n (b +_n c) \mod n$. Since $(a +_n b) +_n c$ and $a +_n (b +_n c)$ are elements in $\{0, 1, \ldots, n-1\}$, the above congruence implies $(a +_n b) +_n c = a +_n (b +_n c)$. Clearly, 0 is an identity element of $(\mathbb{Z}_n, +_n)$. Also, if $a \in \{1, \ldots, n-1\}$ then $n - a \in \{1, \ldots, n-1\}$ and $a +_n (n - a) = 0$. Thus every $a \in \{1, \ldots, n-1\}$ has an inverse element. Also $a = 0$ has an inverse element, namely 0. Finally, $+_n$ is clearly commutative.

The table of $(\mathbb{Z}_4, +_4)$, for instance, is given by

$+_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

(c) $\mathrm{GL}_2(\mathbb{R}) := \{A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in \mathbb{R}, \det(A) = ad - bc \neq 0\}$ is a group under multiplication, called the *general linear group* of 2×2-matrices over $\mathbb{R}$. The identity

element is the identity matrix $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. The inverse element of $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is equal to

$$\begin{pmatrix} d/\det(A) & -b/\det(A) \\ -c/\det(A) & a/\det(A) \end{pmatrix} = \frac{1}{\det(A)} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}.$$

(d) For every set X, the set $\mathrm{Sym}(X)$ of bijective functions $\pi\colon X \to X$, together with the composition of such functions, is a group. It is called the *symmetric group* of X. Elements of $\mathrm{Sym}(X)$ are also called *permutations* of X. The identity element is the identity function id_X and the inverse element of a permutation π is the inverse function π^{-1}.

If $n \in \mathbb{N}$ and $X = \{1, \ldots, n\}$ then we usually write $\mathrm{Sym}(n)$ instead of $\mathrm{Sym}(X)$. An element π of $\mathrm{Sym}(n)$ is usually written in the form

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

In $\mathrm{Sym}(3)$, for instance, we have

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}.$$

Note that $|\mathrm{Sym}(n)| = n! = n \cdot (n-1) \cdot (n-2) \cdots 3 \cdot 2 \cdot 1$, since we have n choices for the image of the element 1, then $n-1$ remaining choices for the image of the element 2, and so on.

(e) If $(G_1, *_1)$ and $(G_2, *_2)$ are two groups then the set $G_1 \times G_2$ together with the binary operation $*$ defined by $(a_1, a_2) * (b_1, b_2) := (a_1 *_1 b_1, a_2 *_2 b_2)$ is again a group. The identity element is (e_1, e_2), if e_i denotes the identity element of $(G_i, *_i)$, and $(a_1, a_2)^{-1} = (a_1^{-1}, a_2^{-1})$.

3.6 Examples (Groups of order 1, 2, 3 and 4) We already know that for any given $n \in \mathbb{N}$ there exists at least one group of order n, namely $(\mathbb{Z}_n, +_n)$. For some natural numbers n, this is the only group of order n, in the sense that every group of order n is isomorphic to this one. We will see below that this is the case for $n = 1, 2, 3$. However, we will also see that there are precisely two isomorphism classes of groups of order 4.

(a) Every group with just one element is called a *trivial group*. This element must be the identity element. Its multiplication table is given by

$*$	e
e	e

Clearly, any two groups of order 1 are isomorphic, since the unique function between them is an isomorphism.

(b) If a group has two elements, and one denotes these elements by e (the identity element) and a, then there is only one possibility for the multiplication table (see Remark 3.4(b)), namely

$*$	e	a
e	e	a
a	a	e

This group is isomorphic to $(\mathbb{Z}_2, +_2)$ under the isomorphism $e \mapsto 0$, $a \mapsto 1$. Thus, any group of order 2 is isomorphic to $(\mathbb{Z}_2, +_2)$.

(c) If a group has three elements, and one denotes them by e, a and b, then again there is only one possibility for the multiplication table by Remark 3.4(b), namely

$*$	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

This group is isomorphic to $(\mathbb{Z}_3, +_3)$, since $e \mapsto 0$, $a \mapsto 1$, $b \mapsto 2$ is an isomorphism. Thus, every group of order 3 is isomorphic to $(\mathbb{Z}_3, +_3)$.

(d) We already constructed two groups of order 4, namely $(\mathbb{Z}_4, +_4)$ and the direct product $\mathbb{Z}_2 \times \mathbb{Z}_2$. If one abbreviates the elements of the latter group by $e = (0,0)$, $x = (1,0)$, $y = (0,1)$, $z = (1,1)$, their operation tables are given by

$+_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

and

$*$	e	x	y	z
e	e	x	y	z
x	x	e	z	y
y	y	z	e	x
z	z	y	x	e

These two groups are not isomorphic, since $a * a = e$ for every element a of the second group, but the same is not true for every element in the first group: For instance $1 +_4 1 \neq 0$. (Here we used that fact that an isomorphism maps the identity element of one group to the identity element of the other group, cf. Proposition 2.10(a).) Every group isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$ is called a *Klein 4-group* (named after the mathematician Felix Klein).

It is not difficult to verify that every other group of order 4 is isomorphic to one of those two. In fact, assume that $G = \{e, a, b, c\}$ is a group of order 4 with binary

operation $*$. Using again the property from Remark 3.4(b), one obtains only four possible multiplication tables, namely

$*$	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

$*$	e	a	b	c
e	e	a	b	c
a	a	c	e	b
b	b	e	c	a
c	c	b	a	e

$*$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	a	e
c	c	b	e	a

$*$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

The first of these four groups is isomorphic to $(\mathbb{Z}_4, +_4)$ under the isomorphism $e \mapsto 0$, $a \mapsto 1$, $b \mapsto 2$, $c \mapsto 3$. The second is also isomorphic to $(\mathbb{Z}_4, +_4)$, under the isomorphism $e \mapsto 0$, $a \mapsto 1$, $b \mapsto 3$, $c \mapsto 2$. The third is again isomorphic to $(\mathbb{Z}_4, +_4)$, this time under the isomorphism $e \mapsto 0$, $a \mapsto 2$, $b \mapsto 1$, $c \mapsto 3$. Finally, the fourth group is isomorphic to the Klein 4-group under the isomorphism $e \mapsto e$, $a \mapsto x$, $b \mapsto y$, $c \mapsto z$. Altogether we know now that there are precisely two isomorphism classes of groups of order 4.

> Note that for any given natural number n, there are only finitely many isomorphism classes of binary structures $(S, *)$ with $|S| = n$. In fact there are at most n^{n^2} such isomorphism classes, as one sees quickly by counting the possible multiplication tables. Similarly, one sees that for a given natural number n, there are only finitely many isomorphism classes of groups of order n. However, there is no explicit formula that gives the number of isomorphism classes of groups of order n.

The easy proof of the following proposition is left to reader (see Exercise 2).

3.7 Proposition *Assume that $(G, *)$ and $(H, \square)$ are groups and that $f\colon G \to H$ is a homomorphism.*

(a) *Let e_G and e_H denote the identity elements of G and H, respectively. Then one has $f(e_G) = e_H$.*

(b) *For every $a \in G$ one has $f(a^{-1}) = f(a)^{-1}$.*

Exercises for §3

1. Let $(S, *)$ and $(T, \square)$ be isomorphic binary structures. Show that $(S, *)$ is a group if and only if $(T, \square)$ is a group.

2. Assume that $(G, *)$ and $(H, \square)$ are groups and that $f\colon (G, *) \to (H, \square)$ is a homomorphism.

(a) Let e_G and e_H denote the identity elements of G and H, respectively. Show that $f(e_G) = e_H$.

(b) Show that one has $f(a^{-1}) = f(a)^{-1}$ for every $a \in G$.

3. Assume that $(G, *)$ is a group and that every element $a \in G$ satisfies $a * a = 1$. Show that $(G, *)$ is abelian.

4. (a) Show that $\mathrm{Sym}(3)$ is not abelian.

(b) Let X be a set. Show that $\mathrm{Sym}(X)$ is abelian if and only if $|X| \leqslant 2$.

5. Show that the group $(\mathbb{Z}_6, +_6)$ is isomorphic to the direct product of the groups $(\mathbb{Z}_3, +_3)$ and $(\mathbb{Z}_2, +_2)$.

6. (a) Show that $(\mathbb{R} \smallsetminus \{0\}, \cdot)$ is a group.

(b) Show that $\det\colon (\mathrm{GL}_2(\mathbb{R}), \cdot) \to (\mathbb{R} \smallsetminus \{0\}, \cdot)$ is a homomorphism.

4 Subgroups

4.1 Remark From now on, if G is a general group, we will denote its binary operation with no symbol at all. Thus, for elements $a, b \in G$, we write ab for the binary operation applied to a and b. The identity element will be denoted by 1_G or just by 1 if there is no risk of confusion, and the inverse of an element $a \in G$ will be denoted by a^{-1}. Since groups are associative binary structures we can write expressions like $ab^{-1}cd$, for elements $a, b, c, d \in G$, without using any parentheses. For $a \in G$ and $n \in \mathbb{Z}$, we also define

$$a^n := \begin{cases} aa \cdots a & (n \text{ factors}) \text{ if } n > 0, \\ 1 & \text{if } n = 0, \\ a^{-1}a^{-1} \cdots a^{-1} & (|n| \text{ factors}) \text{ if } n < 0. \end{cases}$$

If $a \in G$ and $m, n \in \mathbb{Z}$ then

$$a^m a^n = a^{m+n} \quad \text{and} \quad (a^m)^n = a^{mn}.$$

This can be verified easily by distinguishing the 9 cases that m and n are positive, negative or equal to 0. Note that $(ab)^n$ is in general not equal to $a^n b^n$. However, if G is abelian, then this holds for all $a, b \in G$. Because the notations introduced are similar to the multiplication of numbers, we say that G is written *multiplicatively*. We refer to the binary operation as the *group multiplication* and to ab as the *product* of a and b.

Sometimes one prefers that a general group G is written *additively*. In this case the binary operation is written as $+$, the identity element is denoted by 0_G or just 0, and the inverse of $a \in G$ is written as $-a$. One also defines $a - b := a + (-b)$ for $a, b \in G$. For $n \in \mathbb{Z}$ and $a \in G$ one defines na, as the n-fold sum of a if n is positive, as 0 if $n = 0$, and as the $|n|$-fold sum of $-a$ if n is negative. Recall that the additive notation may only be used if G is abelian.

4.2 Definition Let G be a (multiplicatively written) group. A subset H of G is called a *subgroup* of G if it has the following three properties:

(i) $1_G \in H$.

(ii) H is closed under the binary operation of G, i.e., for all $a, b \in H$ also ab lies in H.

(iii) For all $a \in H$ also a^{-1} lies in H.

If H is a subgroup of G we indicate this by the notation $H \leqslant G$. If H is a subgroup of G and $H \neq G$ then we call H a *proper* subgroup of G and write $H < G$. The subgroup $H = \{1_G\}$ is called the *trivial* subgroup of G.

Note that a subgroup H of G, together with the binary operation of G restricted to H, is again a group in its own right. With this in mind, one has $1_G = 1_H$ and the inverse of an element $a \in H$ is the same if one views it as the inverse in the group H or in the group G.

4.3 Examples (a) $\mathbb{Z}$ is a subgroup of $(\mathbb{Q}, +)$.

(b) The *special linear group*

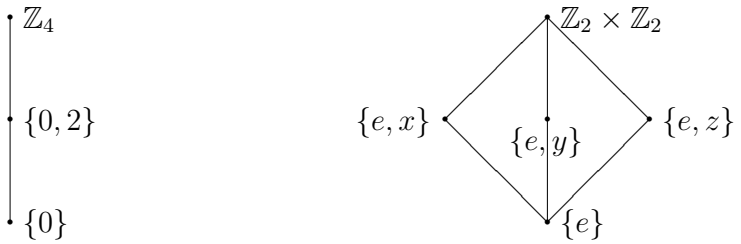
$$\mathrm{SL}_2(\mathbb{R}) := \{A \in \mathrm{GL}_2(\mathbb{R}) \mid \det(A) = 1\}$$

is a subgroup of $\mathrm{GL}_2(\mathbb{R})$, since $\det(AB) = \det(A)\det(B)$ for any two real 2×2-matrices A and B.

(c) $\{0, 2\}$ is a subgroup of $(\mathbb{Z}_4, +_4)$. The subset $\{0, 1, 2\}$ is not a subgroup of $(\mathbb{Z}_4, +_4)$, since it is not closed: $1 +_4 2 = 3$.

(d) $\mathbb{N}$ and $\mathbb{N}_0$ are not subgroups of $(\mathbb{Z}, +)$, since they don't contain the inverse of the element 1. However, the set $2\mathbb{Z}$ of even numbers is a subgroup of $(\mathbb{Z}, +)$. More generally, for every $n \in \mathbb{N}$ the set $n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\}$ is a subgroup of $(\mathbb{Z}, +)$.

(e) If H is a subgroup of G and K is a subgroup of H then K is also a subgroup of G. If K and H are subgroups of G and if K is contained in H then K is also a subgroup of H. The subgroups of a group G are often depicted in a diagram. The subgroups are points and an edge between one subgroup K and another subgroup H indicates that K is contained in H. For instance, the diagrams of subgroups of $(\mathbb{Z}_4, +_4)$ and of $\mathbb{Z}_2 \times \mathbb{Z}_2$ are given by



where $e := (0, 0)$, $x := (1, 0)$, $y := (0, 1)$ and $z := (1, 1)$.

4.4 Proposition *Let G be a group and let a be an element of G. Then the subset*

$$H := \{a^n \mid n \in \mathbb{Z}\}$$

is a subgroup of G which contains a. Moreover, if K is a subgroup of G which contains a then K contains H.

Proof We first prove that H is a subgroup. Obviously, H contains $a^0 = 1$. Moreover, with two elements of H, say a^m and a^n, also their product $a^m a^n = a^{m+n}$ belongs to H. Finally, for every element in H, say a^n, also its inverse $(a^n)^{-1} = a^{-n}$ belongs to H.

Next, assume that K is a subgroup of G and that $a \in K$. We want to show that $H \subseteq K$. Clearly, $a^0 = 1_G \in K$ and $a^1 = a \in K$. By induction on $n \in \mathbb{N}$ we can show that $a^n \in K$. In fact, if $a^n \in K$ then also $a^{n+1} = a^n a \in K$. Also, $a \in K$ implies $a^{-1} \in K$. Now, by induction on $n \in \mathbb{N}$, one can show in a similar way that $a^{-n} \in K$. □

4.5 Definition Let G be a group.

(a) For every element a of G, the subgroup $\{a^n \mid n \in \mathbb{Z}\}$ from the previous proposition is called the *subgroup generated by* a and it is denoted by $\langle a \rangle$.

(b) The group G is called *cyclic* if there exists an element $a \in G$ such that $G = \langle a \rangle$. In this case a is called a *generator* of G.

With this notation we can reformulate Proposition 4.4 as follows: For every $a \in G$ one has $\langle a \rangle \leqslant G$. Moreover, if $a \in K \leqslant G$ then $\langle a \rangle \leqslant K$. In other words, $\langle a \rangle$ is the smallest subgroup of G (with respect to inclusion) which contains a as an element.

We will study cyclic groups in more detail in the next section. One immediate property of cyclic groups we establish already here.

4.6 Proposition *Every cyclic group is abelian.*

Proof If G is a cyclic group then $G = \langle a \rangle$ for some $a \in G$. For arbitrary elements $x = a^m$ and $y = a^n$ of G ($m, n \in \mathbb{Z}$), one has $xy = a^m a^n = a^{m+n}$ and $yx = a^n a^m = a^{n+m}$. Since $m + n = n + m$, we have $xy = yx$. Thus, G is abelian. □

4.7 Example For every $n \in \mathbb{N}$, the group $(\mathbb{Z}_n, +_n)$ is cyclic. In fact we have $\mathbb{Z}_n = \langle 1 \rangle$. Similarly, $(\mathbb{Z}, +)$ is a cyclic group, since it is generated by the element 1.

We return to the study of subgroups.

4.8 Proposition *Let G be a group and let H_i, $i \in I$, be a collection of subgroups of G. Then their intersection, $H := \bigcap_{i \in I} H_i$, is again a subgroup of G.*

Proof Since $1_G \in H_i$ for all $i \in I$, we have $1_G \in H$. To show that H is closed assume that a, b are elements in H. Then, for every $i \in I$, the elements a and b belong to H_i. Since H_i is a subgroup of H, also ab lies in H_i. But this holds for all $i \in I$. Therefore, $ab \in H$. Similarly, to show that H contains inverses, let $a \in H$. Then $a \in H_i$ for all $i \in I$. Since H_i is a subgroup of G, also $a^{-1} \in H_i$. Since this holds for all $i \in I$, we have $a^{-1} \in H$. Thus, $H \leqslant G$. □

4.9 Remark Let G be a group and let $a \in G$. By the second part of Proposition 4.4, the group $\langle a \rangle$ is contained in the intersection of all subgroups K of G which contain a. But, since $\langle a \rangle$ is one of these groups K, we obtain

$$\langle a \rangle = \bigcap_{a \in K \leqslant G} K \, .$$

The next definition generalizes the concept of a subgroup generated by one element a to the concept of a subgroup generated by an arbitrary subset X of G.

4.10 Definition Let G be a group.

(a) For any non-empty subset X of G we define $\langle X \rangle$ as the set of all elements of G of the form

$$x_1^{\epsilon_1} x_2^{\epsilon_2} \cdots x_n^{\epsilon_n}$$

where $n \in \mathbb{N}$, $x_1, \ldots, x_n \in X$ and $\epsilon_1, \ldots, \epsilon_n \in \{1, -1\}$. We extend this definition to the empty subset of G by setting $\langle \emptyset \rangle := \{1_G\}$. Note that one always has $X \subseteq \langle X \rangle$. In fact, for every $x \in X$ we can choose $n = 1$, $x_1 = x$, and $\epsilon_1 = 1$. In the following proposition we will prove that $\langle X \rangle$ is a subgroup of G. It is called the *subgroup generated by* X.

(b) If X is a subset of G such that $\langle X \rangle = G$, then we call X a *generating set* of G.

4.11 Proposition *Let X be a subset of a group G. Then the following hold:*

(a) *$\langle X \rangle$ is a subgroup of G which contains X.*

(b) *Every subgroup K of G which contains X also contains $\langle X \rangle$.*

(c) $\langle X \rangle = \bigcap_{X \subseteq K \leqslant G} K$.

Proof All Parts (a)–(c) are easy to verify when $X = \emptyset$. So we assume from now on that $X \neq \emptyset$.

(a) We already saw in Definition 4.10 that $X \subseteq \langle X \rangle$. Next we show that $H := \langle X \rangle$ is a subgroup of G. Since X is non-empty, here exists an element $x \in X$ and we have $1_G = xx^{-1} \in H$. Also, if a and b are two elements of $\langle X \rangle$ then clearly ab is again a product

of elements which are either in X or inverses of elements in X. Similarly, if $a \in \langle X \rangle$ then $a = x_1^{\epsilon_1} \cdots x_n^{\epsilon_n}$ and its inverse, $a^{-1} = x_n^{-\epsilon_n} \cdots x_1^{-\epsilon_1}$, is of the same form and therefore an element of $\langle X \rangle$.

(b) Assume that K is a subgroup of G which contains X. Then K contains every element of X and also the inverse of every element of X. Since K is closed, it also contains all products of such elements. Thus, $\langle X \rangle \subseteq K$.

(c) It follows from Part (a) that $\langle X \rangle$ is one of the subgroups K occurring in the intersection. This shows that the right hand side is contained in the left hand side. On the other hand, Part (b) implies that every subgroup K occurring in the intersection also contains $\langle X \rangle$. This shows that the left hand side is contained in the right hand side. □

4.12 Example Let $G = \mathrm{Sym}(3)$. By Proposition 4.6, we can easily see that Sym(3) is not cyclic (i.e., not generated by a single element). In fact if we set

$$\sigma := \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \quad \text{and} \quad \tau := \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}.$$

then

$$\sigma\tau = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \quad \text{and} \quad \tau\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

which shows that Sym(3) is not abelian.

But Sym(3) can be generated by two elements. For example, $\mathrm{Sym}(3) = \langle \sigma, \tau \rangle$. (This notation is not quite correct, but a standard abbreviation for $\langle \{\sigma, \tau\} \rangle$.) In fact, we can produce all six elements of Sym(3) as iterated products of the elements σ and τ:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad \sigma^2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \quad \sigma^3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix},$$
$$\tau = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \quad \sigma\tau = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \quad \sigma^2\tau = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}.$$

4.13 Remark The following statement is proved very easily, using the definitions: If $f\colon G \to H$ is a homomorphism between groups G and H and if $X \subseteq G$ then $f(\langle X \rangle) = \langle f(X) \rangle$. In particular, if f is surjective and X is a generating set of G then $f(X)$ is a generating set of H.

We close this section with the statement that images and preimages of subgroups (with respect to a homomorphism) are again subgroups. The easy proof is left as an exercise.

4.14 Proposition *Let $f\colon G \to H$ be a homomorphisms between groups G and H.*

(a) *If U is a subgroup of G then $f(U)$ is a subgroup of H.*

(b) *If V is a subgroup of H then $f^{-1}(V)$ is a subgroup of G.*

Exercises for §4

1. Let G be a group and let H be a non-empty subset of G.

(a) Show that H is a subgroup of G if and only if for all $a, b \in H$ one has $ab^{-1} \in H$.

(b) Assume that H is finite. Show that H is a a subgroup of G if and only if for all $a, b \in H$ one has $ab \in H$. (Hint: Consider the set $\{a, a^2, a^3, \ldots\}$ for an element $a \in H$ to see that $1 \in H$ and $a^{-1} \in H$.)

2. Find all subgroups of the symmetric group Sym(3). What are their orders. (Hint: Start with subgroups generated by one element. Show that these together with Sym(3) are all the subgroups.)

3. (a) Show that $(\mathbb{Q}, +)$ is not cyclic. (This is only a warm-up problem for part (b))

(b) Show that $(\mathbb{Q}, +)$ has no finite generating set.

4. Find all generators of $\mathbb{Z}_{12}$. What do you observe? Formulate a general statement about the set of generators of $(\mathbb{Z}_n, +_n)$ (without proving it).

5. Denote by Q_8 the subgroup of the group of invertible 2×2-matrices with complex coefficients generated by the elements

$$a = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \quad \text{and} \quad b = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

This group is called the *quaternion group* of order 8.

(a) Show that $a^4 = 1$, $b^4 = 1$, $a^2 = b^2$, and $ba = ab^3$.

(b) Show that Q_8 has order 8, give a list of all its elements, and show that Q_8 is not abelian. (Hint: Use the relations in (a) to reduce any element of $\langle a, b \rangle$ to the form $a^i b^j$ with $i \in \{0, 1, 2, 3\}$ and $j \in \{0, 1\}$.)

6. Consider the elements $\sigma, \tau \in \mathrm{Sym}(4)$ defined by

$$\sigma := \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} \quad \text{and} \quad \tau := \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}.$$

(a) Show that $\sigma^4 = 1$, $\tau^2 = 1$, and $\tau\sigma = \sigma^3\tau$.

(b) Show that the subgroup $D_8 := \langle \sigma, \tau \rangle$ of Sym(4) has order 8 and write down all its elements. Show that D_8 is not abelian. The group D_8 is called the *dihedral group* of order 8.

7. Prove the statements in Remark 4.13.

8. Prove the statements in Proposition 4.14.

5 Cyclic groups

5.1 Theorem *Every subgroup of a cyclic group is cyclic.*

Proof Let $G = \langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$ and let H be a subgroup of G. If $H = \{1\}$ then H is cyclic ($H = \langle 1 \rangle$) and we are done. So assume from now on that $H \neq \{1\}$. Since $H \neq \{1\}$, there must exist an element $n \in \mathbb{Z}$, $n \neq 0$, such that $1 \neq a^n \in H$. With a^n also its inverse, a^{-n} is an element of H and $a^{-n} \neq 1$. Therefore, there must exist a positive integer n such that $1 \neq a^n \in H$. Thus, we can choose $n \in \mathbb{N}$ minimal such that $1 \neq a^n \in H$. We will show that $H = \langle a^n \rangle$. First note that $a^n \in H$, and therefore, by Proposition 4.4, we obtain $\langle a^n \rangle \leqslant H$. Conversely, assume that $h \in H$. Then $h = a^m$ for some $m \in \mathbb{Z}$. We can divide m by n with remainder and obtain an integer q and a remainder $r \in \{0, \ldots, n-1\}$ such that $m = nq + r$. Now we have $a^m = a^{nq+r} = a^{nq}a^r$. Since $a^m \in H$ and $a^n \in H$, we have $a^{nq} = (a^n)^q \in H$ and $a^{-nq} = (a^{nq})^{-1} \in H$. This implies that $a^r = a^{-nq}a^m \in H$. By the minimal choice of $n \in \mathbb{N}$ such that $1 \neq a^n \in H$, we must have $a^r = 1$. But this implies $h = a^m = (a^n)^q \in \langle a^n \rangle$, and the theorem is proven. □

5.2 Corollary *The subgroups of $(\mathbb{Z}, +)$ are the groups $\langle n \rangle = n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\}$ with $n \in \mathbb{N}_0$. Moreover, if $m\mathbb{Z} = n\mathbb{Z}$ for $m, n \in \mathbb{N}_0$, then $m = n$.*

Proof Let H be a subgroup of $(\mathbb{Z}, +)$. Since $\mathbb{Z}$ is cyclic ($\mathbb{Z} = \langle 1 \rangle$), H is again cyclic by Theorem 5.1. Therefore $H =< n >= n\mathbb{Z}$ for some element $n \in \mathbb{Z}$. Since $n\mathbb{Z} = (-n)\mathbb{Z}$, there exists $n \in \mathbb{N}_0$ such that $H = n\mathbb{Z}$. Conversely, $n\mathbb{Z} = \langle n \rangle$ is obviously a cyclic subgroup of $\mathbb{Z}$, for every $n \in \mathbb{N}_0$.

Assume that m and n are in $\mathbb{N}_0$ such that $m\mathbb{Z} = n\mathbb{Z}$. If $m = 0$ then $m\mathbb{Z} = \{0\}$ and $n\mathbb{Z} = m\mathbb{Z} = \{0\}$ implies that also $n = 0$. Similarly, $n = 0$ implies $m = 0$. So we may assume that both m and n are positive. Then, m is the smallest positive element in $m\mathbb{Z}$ and n is the smallest positive element in $n\mathbb{Z}$. Since $m\mathbb{Z} = n\mathbb{Z}$, we obtain $m = n$. □

5.3 Theorem *Let $a, b \in \mathbb{N}$. Then, in $(\mathbb{Z}, +)$, one has*

$$\langle a, b \rangle = \langle \gcd(a, b) \rangle$$

and there exist $m, n \in \mathbb{Z}$ such that

$$\gcd(a, b) = ma + nb\,.$$

Proof First note that $\langle a, b \rangle = \{ma + nb \mid m, n \in \mathbb{Z}\}$. In fact, by definition, $\langle a, b \rangle$ is the set of arbitrary sums of the elements a, $-a$, b and $-b$.

Next, since $\langle a, b \rangle$ is a subgroup of $\mathbb{Z}$, Corollary 5.2 implies that there exists a unique element $d \in \mathbb{N}_0$ such that $\langle d \rangle = \langle a, b \rangle$. Since $0 \neq a \in \langle a, b \rangle = \langle d \rangle$, we obtain that $d > 0$. By the first part

of the proof there exist $m, n \in \mathbb{Z}$ such that $d = ma+nb$. It suffices now to show that $d = \gcd(a, b)$. First we show that d is a common divisor of a and b. In fact, since $a \in \langle a, b\rangle = \langle d\rangle = d\mathbb{Z}$, we see that a is a multiple of d, and since $b \in \langle a, b\rangle = \langle d\rangle = d\mathbb{Z}$, we see that also b is a multiple of d. Next assume that $e \in \mathbb{N}$ is a common divisor of a and b. Then we can write $a = re$ and $b = se$ for some elements $r, s \in \mathbb{N}$. This implies that $d = ma + nb = mre + nse = (mr + ns)e$. Thus, e is a divisor of d. This show that d is the greatest common divisor of a and b. □

5.4 Example $\gcd(11, 14) = 1$ and one can write $1 = (-5) \cdot 11 + 4 \cdot 14$.

5.5 Lemma *Let G be a group, let a be an element in G and assume that n is a positive integer such that $a^n = 1$. Then $\langle a\rangle = \{1, a, a^2, \ldots, a^{n-1}\}$. In particular, $\langle a\rangle$ has at most n elements.*

Proof Clearly, $\{1, a, a^2, \ldots, a^{n-1}\} \subseteq \langle a\rangle$, by the definition of $\langle a\rangle$. Conversely, let $b \in \langle a\rangle$. Then there exists $m \in \mathbb{Z}$ such that $b = a^m$. We divide m by n with remainder and can write $m = qn + r$ with $q \in \mathbb{Z}$ and $r \in \{0, 1, \ldots, n-1\}$. We have

$$b = a^m = a^{nq+r} = (a^n)^q a^r = 1^q a^r = a^r \in \{1, \ldots . a^{n-1}\}\,.$$

□

5.6 Theorem *Let $G = \langle a\rangle$ be an infinite cyclic group.*

(a) *If k and l are distinct integers then $a^k \neq a^l$.*

(b) *The function*

$$f\colon \mathbb{Z} \to G\,, \quad k \mapsto a^k\,,$$

is an isomorphism between $(\mathbb{Z}, +)$ and G. Thus, every infinite cyclic group is isomorphic to $(\mathbb{Z}, +)$.

Proof (a) Assume that $k \neq l$ are integers and that $a^k = a^l$. Then $a^{k-l} = a^k a^{-l} = a^l a^{-l} = 1$. Therefore, there exists an integer $n \in \mathbb{Z}$, $n \neq 0$, such that $a^n = 1$. Replacing n by $-n$ if necessary, we see that there also exists $n \in \mathbb{N}$ such that $a^n = 1$. Now Lemma 5.5 implies that $G = \langle a\rangle$ is finite. This is a contradiction.

(b) The function f is a homomorphism, since $f(k + l) = a^{k+l} = a^k a^l = f(k)f(l)$, for all $k, l \in \mathbb{Z}$. It is surjective, because every element of $G = \langle a\rangle$ is of the form $a^k = f(k)$ for some $k \in \mathbb{Z}$. Finally, f is injective by part (a). □

5.7 Definition Let G be a group and let a be an element of G. The *order* of a is defined as the smallest $n \in \mathbb{N}$ such that $a^n = 1$. If no such n exists, we define the order of a to be ∞. We denote the order of a by $o(a)$.

5.8 Example (a) Let a be an element in a group. Then $o(a) = 1$ if and only if $a = 1$.

(b) The element $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ in Sym(3) has order 3, since $\sigma^1 = \sigma \neq 1$, $\sigma^2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \neq 1$ and $\sigma^3 = 1$. The element $\tau = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$ has order 2, since $\tau \neq 1$ and $\tau^2 = 1$.

(c) The element 3 in the group $(\mathbb{Z}_{12}, +_{12})$ has order 4, since $3 \neq 0$, $3 +_{12} 3 = 6 \neq 0$, $3 +_{12} +3 +_{12} 3 = 9 \neq 0$ and $3 +_{12} +3 +_{12} 3 +_{12} 3 = 0$.

> Orders of elements are preserved under isomorphisms in the following sense. Assume that $f\colon G \to H$ is an isomorphism between groups G and H and that a is an element of G. Then $o(f(a)) = o(a)$. The proof is left as an exercise.

5.9 Theorem *Let $G = \langle a \rangle$ be a finite cyclic group of order n.*

(a) *One has $G = \{1, a, \ldots, a^{n-1}\}$, the elements $1, a, a^2, \ldots, a^{n-1}$ are pairwise distinct, and $o(a) = n = |G|$.*

(b) *For all integers k and l one has: $a^k = a^l$ if and only if $k \equiv l \mod n$.*

(c) *The function*

$$f\colon \mathbb{Z}_n \to G\,, \quad k \mapsto a^k\,,$$

is an isomorphism between $(\mathbb{Z}_n, +_n)$ and G. Therefore, every cyclic group of order n is isomorphic to $(\mathbb{Z}_n, +_n)$.

Proof (a) Since G has order n, the $n+1$ elements $1, a, a^2, \ldots, a^n$ cannot be pairwise distinct. Therefore, there exists $0 \leqslant k < l \leqslant n$ such that $a^k = a^l$. But then $a^{l-k} = a^l a^{-k} = a^k a^{-k} = 1$. If $l - k \leqslant n - 1$, then, by Lemma 5.5, we obtain $G = \{1, a, \ldots, a^{l-k-1}\} \subseteq \{1, a, \ldots, a^{n-2}\}$ and G has at most $n-1$ elements. This is a contradiction. Thus, $k = 0$ and $l = n$ and $a^n = 1$. Again by Lemma 5.5 we see that $G = \{1, a, \ldots, a^{n-1}\}$. Since G has order n, there cannot be any repetition in the the n elements $1, a, a^2, \ldots, a^{n-1}$ and therefore, $a^k \neq 1$ for every $1 \leqslant k \leqslant n-1$. Together with $a^n = 1$ this implies that a has order n.

(b) Divide k and l by n with remainder and write $k = qn + r$ and $l = q'n + s$ with $q, q' \in \mathbb{Z}$ and $r, s \in \{0, \ldots, n-1\}$. Then, $a^k = a^{qn+r} = (a^n)^q a^r = a^r$ and similarly, $a^l = a^s$. Now we have the following chain of equivalences:

$$k \equiv l \mod n \iff r = s \iff a^r = a^s \iff a^k = a^l\,.$$

In fact, the middle equivalence follows from Part (a).

(c) The function f is surjective, since $G = \langle a \rangle$. Moreover, it is injective by Part (a). It remains to be shown that f is a homomorphism. So let $k, l \in \{0, 1, \ldots, n-1\}$ and write $k + l = qn + r$ with $q \in \mathbb{Z}$ and $r \in \{0, 1, \ldots, n-1\}$. Then, $k +_n l = r$ and we have

$$f(k +_n l) = f(r) = a^r = (a^n)^q a^r = a^{qn+r} = a^{k+l} = a^k a^l = f(k) f(l)\,.$$

This completes the proof. □

5.10 Corollary *Let G be a group and let a be an element of G. Then $o(a) = |\langle a \rangle|$.*

Proof If $\langle a \rangle$ is a group of infinite order then also $o(a) = \infty$ by Theorem 5.6(a) applied to the group $\langle a \rangle$. If $\langle a \rangle$ is a group of finite order n then, by Theorem 5.9(a) applied to the group $\langle a \rangle$, we also have $o(a) = n = |\langle a \rangle|$. □

5.11 Corollary *Let G be a group and let $a \in G$ be an element of finite order n. For every $k \in \mathbb{Z}$ one has:*

$$a^k = 1 \iff n \text{ divides } k.$$

Proof Write $k = qn + r$ with $q \in \mathbb{Z}$ and $r \in \{0, 1, \ldots, n-1\}$. Then, by Theorem 5.9(b), we have $a^k = a^r$. Moreover, by Theorem 5.9(a), we have $a^r = 1$ if and only if $r = 0$. But this is equivalent to n dividing k. □

5.12 Proposition *Let G be a group, let $a \in G$ be an element of finite order n, and let $k \in \mathbb{N}$. Then*

$$o(a^k) = \frac{n}{\gcd(k, n)}\,.$$

Proof We write $d := \gcd(k, n)$. For every $m \in \mathbb{N}$ we have $(a^k)^m = 1$ if and only if $a^{km} = a^0$. By Theorem 5.9(b), the latter statement is equivalent to $km \equiv 0 \mod n$. This holds if and only if n divides km. This in turn holds if and only if $\frac{n}{d}$ divides $\frac{k}{d}m$. Since $\frac{k}{d}$ and $\frac{n}{d}$ have no common prime divisor, the latter holds if and only if $\frac{n}{d}$ divides m. Thus, the smallest m with this property is $\frac{n}{d}$, and the proof is complete. □

5.13 Corollary *Let $G = \langle a \rangle$ be a finite group of order n. For $k \in \{1, \ldots, n-1\}$ one has*

$$G = \langle a^k \rangle \iff \gcd(k, n) = 1\,.$$

Proof By Corollary 5.10 we have: a^k is a generator of G if and only if $o(a^k) = n$. By Proposition 5.12, the latter condition is equivalent to $\gcd(k, n) = 1$. □

5.14 Example (a) If $G = \langle a \rangle$ is a group of order 20, then each of the elements

$$a, a^3, a^7, a^9, a^{11}, a^{13}, a^{17}, a^{19}$$

is a generator of G, and there are no other generators of G.

(b) The subgroup $\langle 12 \rangle$ of $(\mathbb{Z}_{20}, +_{20})$, generated by the element 12, has order 5. In fact, 1 is a generator of $\mathbb{Z}_{20}$, $12 = 12 \cdot 1$, $\gcd(12, 20) = 4$ and $20/4 = 5$. We can also compute $\langle 12 \rangle$ explicitly: $\langle 12 \rangle = \{0, 12, 4, 16, 8\}$.

Exercises for §5

1. Let $f\colon G \to H$ be an isomorphism between groups G and H.

(a) Show that for every $a \in G$ one has $o(f(a)) = o(a)$.

(b) Show that G is cyclic if and only if H is cyclic.

2. Show that the groups Q_8, D_8, $\mathbb{Z}_8$, $\mathbb{Z}_4 \times \mathbb{Z}_2$, $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ are pairwise non-isomorphic.

3. Compute the order of the element 34 in $(\mathbb{Z}_{200}, +_{200})$.

4. (a) Let a and b be elements of a group G. Assume that $m := o(a)$ and $n := o(b)$ satisfy $\gcd(m, n) = 1$ and that $ab = ba$. Show that $o(ab) = mn$.

(b) Is the statement in (a) still true if one drops the hypothesis $\gcd(m, n) = 1$ or the hypothesis $ab = ba$?

(c) Let G be a cyclic group of order m and let H be a cyclic group of order n. Assume that $\gcd(m, n) = 1$. Show that $G \times H$ is cyclic.

5. Let $G = \langle a \rangle$ be a cyclic group of order n. Show that, for every divisor d of n, there exists a subgroup of G whose order is d.

6. Let $f\colon G \to H$ be a homomorphism between two groups G and H. Assume that $a \in G$ is an element of finite order $n \in \mathbb{N}$. Show that the order of $f(a)$ divides n.

6 Symmetric groups

Recall that for any set X, the group $\mathrm{Sym}(X)$, the symmetric group on X consists of all permutations of X, i.e., all bijective functions from X to X. The binary operation is given by composition of functions. If $X = \{1, \ldots, n\}$ we also used the notation $\mathrm{Sym}(n)$. To distinguish between the element 1 of $\{1, \ldots, n\}$ from the identity element of $\mathrm{Sym}(n)$, we will denote the latter by id.

6.1 Proposition *If X and Y are sets with the same cardinality (i.e., if there exists a bijection between X and Y) then $\mathrm{Sym}(X)$ and $\mathrm{Sym}(Y)$ are isomorphic.*

Proof Let $f\colon X \to Y$ be a bijective function. Consider the functions

$$\varphi\colon \mathrm{Sym}(X) \to \mathrm{Sym}(Y)\,, \quad \sigma \mapsto f \circ \sigma \circ f^{-1}$$

and

$$\psi\colon \mathrm{Sym}(Y) \to \mathrm{Sym}(X)\,, \quad \tau \mapsto f^{-1} \circ \tau \circ f\,.$$

They satisfy $(\psi \circ \varphi)(\sigma) = \sigma$ and $(\varphi \circ \psi)(\tau) = \tau$ for all $\sigma \in \mathrm{Sym}(X)$ and all $\tau \in \mathrm{Sym}(Y)$. Thus, φ is bijective (with inverse ψ). Moreover, φ is a homomorphism, since

$$\varphi(\sigma \circ \tau) = f \circ \sigma \circ \tau \circ f^{-1} = f \circ \sigma \circ f^{-1} \circ f \circ \tau \circ f^{-1} = \varphi(\sigma) \circ \varphi(\tau)\,.$$

Therefore $\varphi\colon \mathrm{Sym}(X) \to \mathrm{Sym}(Y)$ is an isomorphism. □

> The previous proposition shows that if X is a finite set with n elements then $\mathrm{Sym}(X)$ is isomorphic to $\mathrm{Sym}(n)$. Therefore, it suffices to investigate the group $\mathrm{Sym}(n)$. Everything we will prove about $\mathrm{Sym}(n)$ will also be true for $\mathrm{Sym}(X)$ after translating the statement via an isomorphism.

6.2 Definition Let $n \in \mathbb{N}$ and let $a_1, a_2, \ldots, a_k$ be k distinct elements of $\{1, \ldots, n\}$. We define

$$(a_1, a_2, \ldots, a_k) \in \mathrm{Sym}(n)$$

as the permutation that maps a_1 to a_2, a_2 to a_3, …, a_{k-1} to a_k, and a_k to a_1. Every element in $\{1, \ldots, n\} \smallsetminus \{a_1, \ldots, a_k\}$ is mapped to itself. An element as above is called a *k-cycle* and k is called its *length*. Note that every 1-cycle (a) is equal to the identity. 2-cycles are also called *transpositions*. Two cycles $(a_1, \ldots, a_k)$ and $(b_1, \ldots, b_l)$ are called *disjoint* if $\{a_1, \ldots, a_k\} \cap \{b_1, \ldots, b_l\} = \emptyset$.

6.3 Example The element

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 2 & 4 & 1 \end{pmatrix} = (1,3,2,5) = (3,2,5,1) = (2,5,1,3) = (5,1,3,2)$$

is a 4-cycle in Sym(5). Usually it is clear from the context if $(1,3,2,5)$ is viewed as an element in Sym(5), or Sym(6), or Sym(7), etc.

6.4 Proposition *Let $n \in \mathbb{N}$ and let γ and δ be two disjoint cycles in* Sym(n)*. Then γ and δ* commute*, i.e., $\gamma\delta = \delta\gamma$.*

Proof We can write $\gamma = (a_1, \ldots, a_k)$ and $\delta = (b_1, \ldots, b_l)$. If $c \in \{a_1, \ldots, a_k\}$ then

$$(\gamma\delta)(c) = \gamma(\delta(c)) = \gamma(c) = \delta(\gamma(c)) = (\delta\gamma)(c)\,,$$

since c and $\gamma(c)$ are not in $\{b_1, \ldots, b_l\}$. Similarly, if $c \in \{b_1, \ldots, b_l\}$ then

$$(\gamma\delta)(c) = \gamma(\delta(c)) = \delta(c) = \delta(\gamma(c)) = (\delta\gamma)(c)\,,$$

since $\delta(c)$ and c are not in $\{a_1, \ldots, a_k\}$. Finally, if $c \in \{1, \ldots, n\}$ is neither contained in $\{a_1, \ldots, a_k\}$ nor in $\{b_1, \ldots, b_l\}$ then we obtain for similar reasons that $(\gamma\delta)(c) = \gamma(c) = c = \delta(c) = (\delta\gamma)(c)$. Altogether, this implies that $\gamma\delta = \delta\gamma$. □

6.5 Example Let's pick a random permutation, say

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 5 & 8 & 4 & 9 & 3 & 1 & 6 & 7 \end{pmatrix} \in \text{Sym}(9)$$

Note that we can write

$$\sigma = (1,2,5,9,7)(3,8,6)(4) = (1,2,5,9,7)(3,8,6)\,,$$

a product of pairwise disjoint cycles (of length $\geqslant 2$ if we want). The next theorem shows that this is no coincidence. This can be done for every element σ in Sym(n).

> Sometimes we will talk about the empty product in a group. This means a product with 0 factors. Our convention is that such a product is always equal to the identity element. Thus, an expression $g_1 g_2 \cdots g_r$ is interpreted as the identity of the group if $r = 0$.

6.6 Theorem *Let $n \in \mathbb{N}$. Every element $\sigma \in$ Sym(n) can be written as a product $\gamma_1 \cdots \gamma_r$ of pairwise disjoint cycles $\gamma_1, \ldots, \gamma_r$ of lengths $\geqslant 2$.*

Proof For $\sigma \in \mathrm{Sym}(n)$ denote by $M(\sigma)$ the set of elements $a \in \{1, \dots, n\}$ which are moved by σ, i.e., such that $\sigma(a) \neq a$. Note that $M(\sigma\tau) \subseteq M(\sigma) \cup M(\tau)$, that $M(\sigma) = M(\sigma^{-1})$, and that $M(\sigma) = \emptyset$ if and only if $\sigma = \mathrm{id}$. Also, if $\sigma = (a_1, \dots, a_k)$ is a k-cycle with $k \geqslant 2$ then $M(\sigma) = \{a_1, \dots, a_k\}$. Finally, note that there exists no permutation σ with $|M(\sigma)| = 1$.

If $\sigma = \mathrm{id}$ then we can write σ as the empty product.

We will prove by induction on m the following assertion: If $\sigma \neq \mathrm{id}$ and $|M(\sigma)| = m$ then σ can be written as a product $\gamma_1 \cdots \gamma_r$ of pairwise disjoint cycles of lengths $\geqslant 2$ such that $M(\sigma) = M(\gamma_1) \cup \cdots \cup M(\gamma_r)$. This assertion then clearly implies the one in the theorem.

By the above, we need to start the induction with $m = 2$. So assume that σ is an element of $\mathrm{Sym}(n)$ such that $M(\sigma) = \{a_1, a_2\}$ has two elements. This means that $\sigma(a) = a$ for all $a \in \{1, \dots, n\} \smallsetminus \{a_1, a_2\}$ and $\sigma(a_1) = a_2$ and $\sigma(a_2) = a_1$. Thus, $\sigma = (a_1, a_2)$ is a transposition and the statement is proved.

Next let $\sigma \in \mathrm{Sym}(n)$ with $|M(\sigma)| = m > 2$ and assume that the assertion of the theorem holds for all $\mathrm{id} \neq \tau \in \mathrm{Sym}(n)$ with $|M(\tau)| < m$. Pick an element $a \in M(\sigma)$ and consider the sequence $a, \sigma(a), \sigma^2(a), \sigma^3(a), \dots$ of elements in $\{1, \dots, n\}$. Let k be the smallest natural number such that $a, \sigma(a), \dots, \sigma^k(a)$ contains a repetition. Then $k \geqslant 2$ and $a, \sigma(a), \dots, \sigma^{k-1}(a)$ contains no repetition. We claim that $\sigma^k(a) = a$. In fact, if $\sigma^k(a) = \sigma^i(a)$ for some $i = 1, \dots, k-1$ then applying the inverse of σ^i we obtain $\sigma^{k-i}(a) = a$ and we would already have had a repetition in $a, \sigma(a), \dots, \sigma^{k-i}(a)$, contradicting the minimality of k. Set $\gamma := (a, \sigma(a), \sigma^2(a), \dots, \sigma^{k-1}(a))$ and $\tau := \sigma\gamma^{-1}$. Note that $M(\gamma) = \{a, \sigma(a), \dots, \sigma^{k-1}(a)\} \subseteq M(\sigma)$ and that $M(\tau) \cap M(\gamma) = \emptyset$. Moreover, we have $M(\sigma) = M(\tau\gamma) \subseteq M(\tau) \cup M(\gamma) = M(\sigma\gamma^{-1}) \cup M(\gamma) \subseteq M(\sigma) \cup M(\gamma^{-1}) \cup M(\gamma) = M(\sigma)$. Thus, $M(\sigma) = M(\tau) \cup M(\gamma)$ and this union is disjoint. If $\tau = 1$ then $\sigma = \gamma$ and we are done. If $\tau \neq \mathrm{id}$ then, by induction (note that $|M(\tau)| = m - k$) we can write τ as $\tau = \gamma_1 \cdots \gamma_r$ with pairwise disjoint cycles $\gamma_1, \dots, \gamma_r$ of lengths $\geqslant 2$ such that $M(\tau) = M(\gamma_1) \cup \cdots M(\gamma_r)$. This implies that $\sigma = \gamma_1 \cdots \gamma_r\gamma$ can be written as a product of cycles of lengths $\geqslant 2$. They are disjoint, since $(M(\gamma_1) \cup \cdots \cup M(\gamma_r)) \cap M(\gamma) = M(\tau) \cap M(\gamma) = \emptyset$. We also have $M(\sigma) = M(\tau) \cup M(\gamma) = M(\gamma_1) \cup \cdots \cup M(\gamma_r) \cup M(\gamma)$. This completes the proof. □

6.7 Proposition *Let $n \in \mathbb{N}$. Every element in $\mathrm{Sym}(n)$ can be written as a product of transpositions.*

Proof Let σ be an element in $\mathrm{Sym}(n)$. By Theorem 6.6, σ can be written as a product of cycles of length $\geqslant 2$. Therefore it suffices to show that we can write every k-cycle with $k \geqslant 2$ as a product of transpositions. So let $\gamma = (a_1, \dots, a_k)$ be a k-cycle with $k \geqslant 2$. Then, by inspection, we see that

$$(a_1, \dots, a_k) = (a_1, a_k)(a_1, a_{k-1})(a_1, a_{k-2}) \cdots (a_1, a_3)(a_1, a_2)\,.$$

In fact, if $a \in \{1, \dots, n\} \smallsetminus \{a_1, \dots, a_k\}$ then both sides map a to a. And also if $a \in \{a_1, \dots, a_k\}$ then both sides map a to the same element. This completes the proof. □

6.8 Definition A transposition in $\mathrm{Sym}(n)$ of the form $(i, i+1)$ with $i \in \{1, \ldots, n-1\}$ is called a *simple transposition*.

6.9 Proposition *Let $n \in \mathbb{N}$. Every transposition in $\mathrm{Sym}(n)$ is a product of an odd number of simple transpositions. In particular, by Proposition 6.7, $\mathrm{Sym}(n)$ is generated by the set $\{(1,2), (2,3), \ldots, (n-1, n)\}$ of simple transpositions.*

Proof Let $1 \leqslant k < l \leqslant n$. We will show by induction on $l-k$ that (k,l) is a product of an odd number of simple transpositions. If $l-k = 1$ then (k,l) is a simple transposition and a product of such with 1 factor. Next assume that $l-k \geqslant 2$. One can check by inspection that

$$(k,l) = (k,k+1)(k+1,l)(k,k+1)\,.$$

Since $l-(k+1) < l-k$, we can apply the induction hypothesis and write $(k+1,l)$ as a product of an odd number of simple transpositions. This completes the proof. □

6.10 Definition Let n be a positive integer and let σ be an element in $\mathrm{Sym}(n)$. A pair (i,j) with $1 \leqslant i < j \leqslant n$ is called an *inversion* of σ if $\sigma(i) > \sigma(j)$. The number of inversions of σ will be denoted by $N(\sigma)$. The permutation σ is called *even* if $N(\sigma)$ is even and *odd* if $N(\sigma)$ is odd. We also define the *sign* function

$$\mathrm{sgn}\colon \mathrm{Sym}(n) \to \{1, -1\}\,, \quad \sigma \mapsto (-1)^{N(\sigma)}\,.$$

Thus, an even permutation has sign 1 and and an odd permutation has sign -1.

> Note that the symbol (i,j) can mean two different things: First it can be a transposition, i.e., an element of $\mathrm{Sym}(n)$; secondly it can be just a pair of elements for which one wants to decide if it is an inversion for σ. It should be clear from the context which of the two one is talking about. To avoid confusion we can also say "the transposition (i,j)", or in the other cast "the pair (i,j)".
> It is clear that, for every $\sigma \in \mathrm{Sym}(n)$, the number of inversions $N(\sigma)$ satisfies $0 \leqslant N(\sigma) \leqslant n(n-1)/2$. Exercise 4 shows that the upper bound $n(n-1)/2$ actually occurs, and only for one choice of σ.

6.11 Example Let

$$\sigma := \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix} \in \mathrm{Sym}(4)\,.$$

The inversions of σ are $(2,3)$ and $(2,4)$. Thus, $\mathrm{sgn}(\sigma) = 1$ and σ is an even permutation.

6.12 Lemma *Let $n \in \mathbb{N}$ and let $\sigma \in \mathrm{Sym}(n)$.*

(a) *One has $N(\sigma) = 0$ if and only if $\sigma = \mathrm{id}$.*

(b) *If $1 \leqslant k < l \leqslant n$ and $\sigma = (k, l)$ then $N(\sigma) = 2(l - k) - 1$. Thus, every transposition is an odd permutation.*

(c) *Let $1 \leqslant k < n$. If $\sigma(k) < \sigma(k+1)$ then $N(\sigma(k, k+1)) = N(\sigma) + 1$ and if $\sigma(k) > \sigma(k+1)$ then $N(\sigma(k, k+1)) = N(\sigma) - 1$*

(d) *Assume that $\sigma = \tau_1 \cdots \tau_s$ is a product of s simple transpositions $\tau_1, \ldots, \tau_s$. Then $N(\sigma) \equiv s \mod 2$.*

Proof (a) If $\sigma = \mathrm{id}$ then σ has no inversions. Conversely, if σ has no inversion then $\sigma(1) < \sigma(2) < \cdots < \sigma(n)$. This implies that $\sigma = \mathrm{id}$.

(b) Let $1 \leqslant i < j \leqslant n$. If both i and j are not contained in $\{k, l\}$ then (i, j) is not an inversion. If $i = k$ and $j \in \{k + 1, \ldots, l - 1\}$ then (i, j) is an inversion and if $j > l$ then (i, j) is not an inversion. Similarly, if $j = l$ and $i \in \{k+1, \ldots, l-1\}$ then (i, j) is an inversion and if $i < k$ then (i, j) is not an inversion. Finally, the only remaining pair, namely (k, l), is an inversion. Altogether we have found that the permutation (k, l) has $(l-k-1)+(l-k-1)+1 = 2(l-k)-1$ inversions.

(c) Let $1 \leqslant i < j \leqslant n$. If i and j are not in $\{k, k + 1\}$ then $(\sigma(k, k + 1))(i) = \sigma(i)$ and $(\sigma(k, k + 1))(j) = \sigma(j)$. Thus, (i, j) is an inversion for σ if and only if (i, j) is an inversion for $\sigma(k, k + 1)$. Next assume that $j > k + 1$. Then (k, j) is an inversion of $\sigma(k, k + 1)$ if and only if $(k + 1, j)$ is an inversion of σ and $(k + 1, j)$ is an inversion of $\sigma(k, k + 1)$ if and only if (k, j) is an inversion of σ. Also if $i < k$ then (i, k) is an inversion of $\sigma(k, k + 1)$ if and only if $(i, k + 1)$ is an inversion of σ and $(i, k + 1)$ is an inversion of $\sigma(k, k + 1)$ if and only if (i, k) is an inversion of σ. Finally, we see that $(k, k + 1)$ is an inversion of $\sigma(k, k + 1)$ if an only if $(k, k + 1)$ is not an inversion of σ. This proves the statement in (c).

(d) We prove the statement by induction on s. If $s = 0$ then $\sigma = \mathrm{id}$ and $s = 0 = N(\sigma)$ by Part (a). Similarly, if $s = 1$ then $s = 1 = N(\sigma)$ by Part (b). Now assume that $s > 1$ and set $\sigma' := \tau_1 \cdots \tau_{s-1}$. Then $\sigma = \sigma'\tau_s$ and, by Part (c) and the induction hypothesis applied to σ', we have $N(\sigma) \equiv N(\sigma') + 1 \equiv (s - 1) + 1 = s \mod 2$. □

6.13 Theorem *Let $n \in \mathbb{N}$ and let $\sigma \in \mathrm{Sym}(n)$. Assume that $\sigma = \tau_1 \cdots \tau_r$ is a product of r transpositions. Then $N(\sigma) \equiv r \mod 2$.*

The theorem states that if σ is even then also r must be even, and if σ is odd then also r must be odd. This shows that if σ can be written as a product of an even number of transpositions then every other product of transpositions that equals σ must also have an even number of factors. Similarly, if σ can be written as a product of an odd number of transpositions then every other product of transpositions that equals σ must also have an odd number of factors. For instance, it cannot happen that σ can be expressed as a product of 3 transpositions and also as a product of 4 transpositions.
Another consequence of the theorem is that a permutation is even (resp. odd) if and only if it can be written as a product of an even (resp. odd) number of transpositions. This property is often used in textbooks as a definition for even (resp. odd) permutations.

Proof By Proposition 6.9 we can write every transposition τ_i as a product of s_i simple transpositions, such that $s_i \in \mathbb{N}$ is odd. Substituting each τ_i by such a product yields an expression of σ as a product of $s = s_1 + \ldots + s_r$ simple transpositions. Since each s_i is odd, we have $s_i \equiv 1 \mod 2$. Adding these r congruences yields $s \equiv r \mod 2$. Further, by Lemma 6.12(d), we have $N(\sigma) \equiv s \mod 2$. Thus $N(\sigma) \equiv s \equiv r \mod 2$. □

6.14 Definition Let $n \in \mathbb{N}$. We denote the set of even permutations in $\mathrm{Sym}(n)$ by $\mathrm{Alt}(n)$. By the following corollary, this is a subgroup of $\mathrm{Sym}(n)$, called the *alternating group* on $\{1, \ldots, n\}$.

6.15 Corollary *The product of two even permutations is even, the product of two odd permutations is even, and the product of two permutations of mixed signs is odd. The inverse of an even permutation is even and the inverse of an odd permutation is odd. In particular,* $\mathrm{Alt}(n)$ *is a subgroup of* $\mathrm{Sym}(n)$ *and the function* $\mathrm{sgn}\colon \mathrm{Sym}(n) \to \{1, -1\}$ *is a homomorphism.*

Proof Let σ and τ be elements of $\mathrm{Sym}(n)$. Write σ and τ as products of s and t transpositions, respectively, then $\sigma\tau$ can be written as a product of $s + t$ transpositions. Now the first sentence in the corollary follows from Theorem 6.13. Since transpositions are their own inverses, the inverse of σ is again a product of s transpositions and the second sentence follows. Finally, Theorem 6.13 implies

$$\mathrm{sgn}(\sigma\tau) = (-1)^{N(\sigma\tau)} = (-1)^{s+t} = (-1)^s(-1)^t = (-1)^{N(\sigma)}(-1)^{N(\tau)} = \mathrm{sgn}(\sigma)\mathrm{sgn}(\tau)\,.$$

□

6.16 Remark Let n be a positive integer and let σ be a permutation in $\mathrm{Sym}(n)$. The number $N(\sigma)$, of inversions of σ, has the following interesting property: $N(\sigma)$ is the smallest possible number of factors that are needed to express σ as a product of simple transposition. This can be proved using Lemma 6.12(c). The proof is left as an exercise (see Exercise 5).

Exercises for §6

1. (a) Show that the order of a k-cycle in $\mathrm{Sym}(n)$ is equal to k.

(b) Compute the order of $(1,2,3)(4,5,6,7)$ in $\mathrm{Sym}(7)$.

2. Let $n \in \mathbb{N}$, let $\sigma \in \mathrm{Sym}(n)$ and let $(a_1, \ldots, a_k)$ be a k-cycle in $\mathrm{Sym}(n)$. Show that $\sigma \circ (a_1, a_2, \ldots, a_k) \circ \sigma^{-1} = (\sigma(a_1), \ldots, \sigma(a_k))$.

3. Let $2 \leqslant n \in \mathbb{N}$ and set $\sigma := (1, 2, 3, \ldots, n)$ and $\tau := (1, 2)$. Show that $\mathrm{Sym}(n) = \langle \sigma, \tau \rangle$.

4. Let $2 \leqslant n \in \mathbb{N}$. Show that there exists precisely one element ω in $\mathrm{Sym}(n)$ such that every pair (i, j) with $1 \leqslant i < j \leqslant n$ is an inversion of ω. Show that ω has order 2.

5. Let $n \geqslant 2$. For $\sigma \in \mathrm{Sym}(n)$, define the *length* of σ (notation $l(\sigma)$) as the smallest $l \in \mathbb{N}_0$ such that σ can be written as a product of l simple transpositions. Show that $l(\sigma) = N(\sigma)$.

6. In the tableau

2	1	3	4
5	6	7	8
9	10	11	12
13	14	15	

one is allowed to shift any square bordering the empty slot to the empty slot. Find out if it is possible to obtain the constellation

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	

from the first one by a sequence of the above moves.

7. Assume that σ is a k-cycle. Show that if k is even then σ is odd and if k is odd then σ is even.

7 Symmetry groups

7.1 Remark (a) Recall that an *orthogonal transformation* of $\mathbb{R}^n$ is a linear function $f\colon \mathbb{R}^n \to \mathbb{R}^n$ with the property

$$\langle f(x), f(y)\rangle = \langle x, y\rangle \text{ for all } x, y \in \mathbb{R}^n. \tag{7.1.a}$$

Here $\langle x, y\rangle = x_1y_1 + \cdots + x_ny_n$ is the standard euclidean inner product. Thus, an orthogonal transformation is a linear map that preserves angles and lengths. Recall also that every linear function $f\colon \mathbb{R}^n \to \mathbb{R}^n$ is of the form $x \mapsto Ax$ for a uniquely determined $n \times n$-matrix A. An $n \times n$-matrix A is called *orthogonal* if it has the property corresponding to (7.1.a):

$$\langle Ax, Ay\rangle = \langle x, y\rangle \text{ for all } x, y \in \mathbb{R}^n. \tag{7.1.b}$$

The equation in (7.1.b) is equivalent to requiring $A^tA = I_n$, where A^t denotes the transposed of A and I_n denotes the identity matrix. Thus, every orthogonal matrix A is invertible and its inverse is A^t. The orthogonal matrices form a subgroup of $\mathrm{GL}_n(\mathbb{R})$, called the *orthogonal group*. It is denoted by $\mathrm{O}_n(\mathbb{R})$. Note that since $\det(A) = \det(A^t)$, the equation $A^tA = I_n$ implies that $\det(A)^2 = 1$. Thus, every orthogonal matrix has determinant ± 1. An orthogonal matrix with determinant $+1$ is called a *special orthogonal matrix*. The special orthogonal matrices form a subgroup of $\mathrm{O}_n(\mathbb{R})$, called the *special orthogonal group*. It is denoted by $\mathrm{SO}_n(\mathbb{R})$.

(b) If $n = 2$, then every orthogonal transformation is either a reflection about a line through 0 or a rotation about 0. The rotations are the ones with determinant 1 and the reflections have determinant -1. For example,

$$\begin{pmatrix} \cos(\phi) & -\sin(\phi) \\ \sin(\phi) & \cos(\phi) \end{pmatrix}$$

is a counterclockwise rotation with angle ϕ and

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

is a reflection about the diagonal of the first and third quadrants.

(c) If $n = 3$ then every special orthogonal transformation is a rotation about an axis through the origin with some angle ϕ. For instance,

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos(\phi) & -\sin(\phi) \\ 0 & \sin(\phi) & \cos(\phi) \end{pmatrix}$$

is such a rotation about the x-axis. Every reflection about a two-dimensional subspace is again an orthogonal transformation with determinant -1, but there are more orthogonal transformations with determinant -1. This is why, in $\mathbb{R}^n$, for $n \geqslant 3$, we will later only consider special orthogonal transformations.

7.2 Definition (a) Let $S \subset \mathbb{R}^2$ be a subset of $\mathbb{R}^2$. The *symmetry group* of S, $\Sigma(S)$, is the set of orthogonal transformations, i.e., rotations and reflections, which map S onto itself. This is clearly a group under composition.

(b) Let $S \subset \mathbb{R}^3$ be a subset of $\mathbb{R}^3$. The *rotational symmetry group* of S, $\Sigma^r(S)$, is the set of all special orthogonal transformations (i.e., rotations) which map S onto itself. This is clearly a group under composition.

7.3 Example (a) Consider a square with its center in the origin. It has 8 symmetries: The four counterclockwise rotations with angles 0°, 90°, 180°, and 270°, and the four reflections. We number the vertices of the square in counterclockwise orientation by 1, 2, 3 and 4. We denote the counterclockwise rotation with angle 90° by σ and the reflection about the line that passes through the mid point of the edge connecting 1 and 4 by τ. Then the four rotations are given by $\mathrm{id}, \sigma, \sigma^2, \sigma^3$ and the four reflections are given by $\tau, \sigma\tau, \sigma^2\tau, \sigma^3\tau$. Clearly one has $\sigma^4 = \mathrm{id}$ and $\tau^2 = \mathrm{id}$. But one also has $\tau\sigma = \sigma^3\tau$, which allows one to bring products of arbitrary length into the form of the above 8 elements. For instance, $\sigma\sigma\tau\sigma\sigma\tau\sigma = \sigma\sigma\tau\sigma\sigma\sigma^3\tau = \sigma\sigma\tau\sigma\tau = \sigma\sigma\sigma^3\tau\tau = \sigma$.

(b) More generally, one can consider a regular n-gon P_n (for $n \geqslant 3$) with center located in the origin. Again we number the vertices in counterclockwise orientation by 1, 2, ..., n and denote the counterclockwise rotation with angle $360°/n$ by σ and the reflection about the line that passes through the midpoint of the edge connecting 1 and n by τ. The symmetry group of the n-gon consists of n rotations, namely id, σ, σ^2, ..., σ^{n-1}, and n reflections, namely τ, $\sigma\tau$, $\sigma^2\tau$, ..., $\sigma^{n-1}\tau$. In particular, $\{\sigma, \tau\}$ is a generating set of the symmetry group of the regular n-gon. One can again easily verify that these elements satisfy the relations $\sigma^n = 1$, $\tau^2 = 1$ and $\tau\sigma = \sigma^{n-1}\tau = \sigma^{-1}\tau$ which allow us to carry out any computation in this group. The symmetry group of the regular n-gon is called the *dihedral group* of order $2n$. It is denoted by D_{2n}.

7.4 Proposition *Assume the notation from Example 7.3(b). There exists an injective group homomorphism* $\alpha\colon \Sigma(P_n) \to \mathrm{Sym}(n)$ *with*

$$\alpha(\sigma) = (1, 2, \ldots, n) \quad \textit{and} \quad \alpha(\tau) = (1, n)(2, n-1)(3, n-2)\cdots .$$

In particular, $D_{2n} = \Sigma(P_n)$ *is isomorphic to the subgroup* $\langle (1, 2, \ldots, n), (1, n)(2, n-1)\cdots \rangle$ *of* $\mathrm{Sym}(n)$.

Proof We number the vertices of P_n the same way as in Example 7.3(b). Then we define the function

$$\alpha\colon \Sigma(P_n) \to \mathrm{Sym}(n)\,, f \mapsto f|_{\{1,\ldots,n\}}\,.$$

Since every vertex of P_n is mapped under a symmetry to a vertex, the map $f|_{\{1,\ldots,n\}}$ (the restriction of f to $\{1, \ldots, n\}$) is a function from $\{1, \ldots, n\}$ to $\{1, \ldots, n\}$. Since f is injective, also $f|_{\{1,\ldots,n\}}$ is injective. But this implies that $f|_{\{1,\ldots,n\}}$ is an element of $\mathrm{Sym}(n)$. Also, for $f, g \in \Sigma(P_n)$ one has $(g \circ f)|_{\{1,\ldots,n\}} = (g|_{\{1,\ldots,n\}}) \circ (f|_{\{1,\ldots,n\}})$. Thus, α is a group homomorphism. Moreover, α is injective. In fact, assume that f and g are elements of $\Sigma(P_n)$ whose restrictions

to $\{1, \ldots, n\}$ coincide. Then $f(1) = g(1)$ and $f(2) = g(2)$. Since the vectors 1 and 2 generate the vector space $\mathbb{R}^2$, this implies $f = g$. Thus, α is injective and defines an isomorphism $\alpha\colon \Sigma(P_n) \to \alpha(\Sigma(P_n))$. Clearly, $\alpha(\sigma) = (1, \ldots, n)$ and $\alpha(\tau) = (1, n)(2, n-1)\cdots$. Since $\Sigma(P_n) = \langle \sigma, \tau \rangle$, we have $\alpha(\Sigma(P_n)) = \langle (1, 2, \ldots, n), (1, n)(2, n-1)\cdots \rangle$. □

7.5 Example (a) The rotational symmetry group of the tetrahedron is isomorphic to Alt(4) (left as exercise).

(b) The rotational symmetry group of the cube consists of

- 9 rotations about an axis through the centers of opposite squares (6 of them have order 4, and 3 of them have order 2),
- 6 rotations of order 2 about an axis through the centers of opposite edges,
- 8 rotations of order 3 about an axis through opposite vertices, and
- the identity.

Compare this to the 24 elements of Sym(4): 6 4-cycles, 3 double transpositions, 6 transpositions, 8 3-cycles, and the identity. In fact, one can show that the rotational symmetry group of the cube is isomorphic to Sym(4), see Exercise 3.

(c) The rotational symmetry group of the dodecahedron consists of

- 24 rotations of order 5 about an axis that passes through the centers of opposite pentagons,
- 30 rotations of order 3 about an axis that passes through opposite vertices,
- 15 rotations of order 2 about an axis that passes through the centers of opposite edges,
- and the identity element.

Note that also the group Alt(5) has, besides the identity, 24 elements of order 5 (the 5-cycles), 30 elements of order 3 (the 3-cycles), and 15 elements of order 2 (the double transpositions). And in fact, one can prove that the rotational symmetry group of the dodecahedron is isomorphic to Alt(5).

Exercises for §7

1. (a) Let σ be the elements of the dihedral group D_{2n} given as the rotation with $360°/n$, and let $\rho \in D_{2n}$ be any reflection. Show that $\rho\sigma = \sigma^{-1}\rho$, and show that $\sigma\rho$ and ρ are elements of order 2 which generate D_{2n}.

(b) Assume that $G = \langle t_1, t_2 \rangle$ is a finite group which is generated by two *involutions* t_1, t_2, i.e., elements of order 2 and assume that $n := o(t_1 t_2) \geqslant 3$. Show that $G \cong D_{2n}$.

2. Show that the rotational symmetry group of a tetrahedron is isomorphic to Alt(4), by considering the four vertices of the tetrahedron.

3. Show that the rotational symmetry group of a cube is isomorphic to Sym(4), by considering the four diagonals of the cube.

8 Cosets and Lagrange's Theorem

8.1 Notation For a group G and subsets X and Y of G we set

$$XY := \{xy \mid x \in X, y \in Y\}\,.$$

Note that if also Z is a subset of G then $(XY)Z = X(YZ)$.

8.2 Definition Let G be a group and let H be a subgroup of G. A *left coset* of H in G is a subset of G of the form $aH = \{ah \mid h \in H\}$ for some $a \in G$. Similarly, a *right coset* of H in G is a subset of G of the form $Ha = \{ha \mid h \in H\}$ for some $a \in G$. Note that $a \in aH$ and $a \in Ha$.

8.3 Proposition *Let G be a group and let H be a subgroup of G. Furthermore, let a and b be element of G.*

(a) *One has $aH = H$ if and only if $a \in H$.*

(b) *One has either $aH = bH$ or $aH \cap bH = \emptyset$. Moreover,*

$$aH = bH \iff b^{-1}a \in H \iff a^{-1}b \in H\,.$$

(c) *One has $Ha = H$ if and only if $a \in H$.*

(d) *One has either $Ha = Hb$ or $Ha \cap Hb = \emptyset$. Moreover,*

$$Ha = Hb \iff ab^{-1} \in H \iff ba^{-1} \in H\,.$$

Proof (a) If $aH = H$ then $a = a \cdot 1_G \in aH = H$. Conversely, if $a \in H$ then $aH \subseteq H$, since H is closed. Moreover, $H = 1_G \cdot H = (aa^{-1})H = a(a^{-1}H) \subseteq aH$, since also $a^{-1}H \subseteq H$.

(b) For the first statement it suffices to show that if aH and bH have an element in common then $aH = bH$. So assume that $ah = bh'$ for some elements $h, h' \in H$. Then $aH = bh'h^{-1}H = bH$, since $h'h^{-1}H = H$ by Part (a). For the second statement note that $aH = bH$ if and only if $b^{-1}aH = H$ and also if and only if $H = a^{-1}bH$. Now the second statement follows from Part (a).

(c) This is proved in the same way as Part (a).

(d) This is proved in the same way as Part (b). □

Proposition 8.3(b) implies that G is the disjoint union of the left cosets of H. The corresponding equivalence relation of this partitioning of G is given by

$$a \sim_L b : \Longleftrightarrow\ a^{-1}b \in H\,.$$

Similarly, G is the disjoint union of the right cosets of H, and the corresponding equivalence relation is given by

$$a \sim_R b : \Longleftrightarrow\ ab^{-1} \in H\,.$$

In general, the partitioning of G into left cosets of H is different from the partitioning of G into right cosets of H, as the following example shows.

8.4 Example Let $G = \mathrm{Sym}(3)$.

(a) Let $H = \{1, (1,2)\} \leqslant G$ then the left cosets of H are the three subsets

$$\begin{aligned} H &= \{1, (1,2)\} \\ (1,2,3)H &= \{(1,2,3), (1,3)\} \\ (1,3,2)H &= \{(1,3,2), (2,3)\}\,, \end{aligned}$$

and the right cosets of H are the three subsets

$$\begin{aligned} H &= \{1, (1,2)\} \\ H(1,2,3) &= \{(1,2,3), (2,3)\} \\ H(1,3,2) &= \{(1,3,2), (1,3)\}\,. \end{aligned}$$

The left coset $(1,2,3)H$ that contains $(1,2,3)$ is different from the right coset $H(1,2,3)$ that contains $(1,2,3)$. Thus, the left coset $(1,2,3)H$ of H is not equal to a right coset of H.

(b) Let $K = \langle (1,2,3) \rangle = \{1, (1,2,3), (1,3,2)\} \leqslant G$. Then the left cosets of K are given by

$$\begin{aligned} K &= \{1, (1,2,3), (1,3,2)\} \\ (1,2)K &= \{(1,2), (2,3), (1,3)\}\,. \end{aligned}$$

The right cosets of K are given by

$$\begin{aligned} K &= \{1, (1,2,3), (1,3,2)\} \\ K(1,2) &= \{(1,2), (1,3), (2,3)\}\,. \end{aligned}$$

Therefore, the left cosets of K are also right cosets.

8.5 Definition Let G be a group and let H be a subgroup of G. We denote the set of left cosets of H in G by G/H and the set of right cosets of H in G by $H\backslash G$.

8.6 Example With the notation in Example 8.4, we have

$$G/H = \{H, (1,2,3)H, (1,3,2)H\}, \quad H\backslash G = \{H, H(1,2,3), H(1,3,2)\}$$

and

$$G/K = \{K, (1,2)K\}, \quad K\backslash G = \{K, K(1,2)\}.$$

Therefore, $G/H \neq H\backslash G$, but $G/K = K\backslash G$, cf. Example 8.4

8.7 Notation If X is a subset of a group G we define

$$X^{-1} := \{x^{-1} \mid x \in X\}.$$

Note that if also Y is a subset of G then $(XY)^{-1} = Y^{-1}X^{-1}$. Moreover note that if H is a subgroup of G then $H^{-1} = H$. In particular, if aH is a left coset of H in G then $(aH)^{-1} = H^{-1}a^{-1} = Ha^{-1}$ is a right coset of H in G. Similarly, if Ha is a right coset of H in G then $(Ha)^{-1} = a^{-1}H$ is a left coset of H in G.

8.8 Proposition *Let G be a group and let $H \leqslant G$.*

(a) *For every $a \in G$, the function $l_a \colon H \to aH$, $h \mapsto ah$, is bijective.*

(b) *For every $a \in G$ the function $r_a \colon H \to Ha$, $h \mapsto ha$, is bijective.*

(c) *The function $G/H \to H\backslash G$, $aH \mapsto (aH)^{-1} = Ha^{-1}$, is a bijection. In particular $|G/H| = |H\backslash G|$.*

Proof (a) Clearly, l_a is surjective. To see that l_a is injective, note that $ah_1 = ah_2$ implies $h_1 = h_2$ for all $h_1, h_2 \in H$.

(b) This is proved in a similar way as Part (a).

(c) The function is bijective, since $H\backslash G \to G/H$, $Ha \mapsto (Ha)^{-1} = a^{-1}H$, is an inverse to the given function. □

> Assume that G is a finite group and that $H \leqslant G$. Part (a) (resp. Part (b)) of Proposition 8.8 shows that all the left cosets (reps. right cosets) of H in G have the same cardinality, namely the order of H.

8.9 Definition Let G be a group and let H be a subgroup of G. By Proposition 8.8(c), the number of left cosets of H in G is equal to the number of right cosets of H in G. This number, $|G/H| = |H\backslash G|$, is called the *index* of H in G and it is denoted by $[G : H]$. It can be equal to infinity.

8.10 Theorem (Lagrange) *Let G be a group and let H be a subgroup of G. Then*

$$|G| = |H| \cdot [G : H]$$

(with the usual rules of arithmetic for ∞). In particular, if G is a finite group then $|H|$ divides $|G|$.

Proof By Proposition 8.3(b), the set G is the disjoint union of the left cosets of G. By Proposition 8.8(a), each left coset of H has the same number of elements as H. Thus, $|G| = |G/H| \cdot |H| = [G : H] \cdot |H|$. This equation is even true when one allows the values ∞ for $|G|$, $|H|$, or $[G : H]$. □

8.11 Corollary *Let G be a finite group and let $a \in G$. Then $o(a)$ divides $|G|$.*

Proof By Corollary 5.10 we have $o(a) = |\langle a \rangle|$. By Lagrange's Theorem, $|\langle a \rangle|$ divides $|G|$. This proves the corollary. □

8.12 Corollary *Let p be a prime number. Every group G of order p is cyclic. In particular, $G \cong (\mathbb{Z}_p, +_p)$, and there exists only one group of order p (up to isomorphism).*

Proof Let $a \in G$ be an element that is different from the identity element. Then $o(a) \neq 1$, and $o(a)$ divides $|G| = p$ by Corollary 8.11. Thus $o(a) = p$, and $|\langle a \rangle| = o(a) = p$ by Corollary 5.10. This implies that $\langle a \rangle = G$. □

8.13 Examples (a) For $n \geqslant 2$, he subgroup $\mathrm{Alt}(n)$ of $\mathrm{Sym}(n)$ has two left cosets and two right cosets in Sym, namely $\mathrm{Alt}(n)$ and $\tau\mathrm{Alt}(n) = \mathrm{Alt}(n)\tau$, where τ is any odd permutation. In fact the even permutations form the left and right coset $\mathrm{Alt}(n)$. Moreover, any two odd permutations α and β lie in the same left coset and also in the same right coset, since $\alpha^{-1}\beta \in \mathrm{Alt}(n)$ and $\alpha\beta^{-1} \in \mathrm{Alt}(n)$. Thus, $\tau\mathrm{Alt}(n)$ and $\mathrm{Alt}(n)\tau$ is the set of odd permutations. We obtain, that $|\mathrm{Alt}(n)|$ has index 2 in $\mathrm{Sym}(n)$ and by Lagrange we obtain that $|\mathrm{Alt}(n)| = n!/2$. Proposition 8.8 implies that $|\mathrm{Alt}(n)| = |\tau\mathrm{Alt}(n)|$, so that there are as many even permutations as odd permutations.

(b) Let $n \in \mathbb{N}$ and consider the subgroup $n\mathbb{Z}$ of $(\mathbb{Z}, +)$. Since $\mathbb{Z}$ is abelian, one has $a + n\mathbb{Z} = n\mathbb{Z} + a$, i.e., left and right cosets coincide. For arbitrary $a, b \in \mathbb{Z}$ one has

$$a + n\mathbb{Z} = b + n\mathbb{Z} \iff a - b \in n\mathbb{Z} \iff a \equiv b \mod n\,.$$

Thus, $n\mathbb{Z}$ has precisely n cosets in $\mathbb{Z}$, namely

$$0 + n\mathbb{Z}, 1 + n\mathbb{Z}, 2 + n\mathbb{Z}, \ldots, (n-1) + n\mathbb{Z}$$

and therefore $[\mathbb{Z} : n\mathbb{Z}] = n$, i.e., $n\mathbb{Z}$ has index n in $\mathbb{Z}$.

Exercises for §8

1. Show that $V := \{1, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}$ is a subgroup of Alt(4) and compute its left and right cosets. Do the left and right cosets of V yield the same partitioning of Alt(4)?

2. Let p be prime and let G be a group of order p^n for some $n \in \mathbb{N}$. Show that G has an element of order p. (Hint: Choose an element $1 \neq a \in G$ and consider the group $\langle a \rangle$. Then find an element of order p in this group.)

3. Let H and K be subgroups of a group G and assume that $\gcd(|H|, |K|) = 1$. Show that $H \cap K = \{1_G\}$.

4. Find all the subgroups of Alt(4) of order 1, 2, 3, and 4. Does Alt(4) have a subgroup of order 6?

5. Let G be a finite group and let H be a subgroups of G. Elements $a_1, \ldots, a_n$ of G are called *left coset representatives* of H in G if each left coset of H in G can be written as $a_i H$ for a unique $i = 1, \ldots, n$ (in other words, if G is the disjoint union of the subsets $a_i H$, $i = 1, \ldots, n$). Note that in this case $n = [G\colon H]$.

(a) Show that if $a_1, \ldots, a_n$ are left coset representatives of H in G then a_i^{-1} are right coset representatives of H in G.

(b) Assume that H and K are subgroups of G with $H \cap K = \{1\}$ and $HK = G$. Show that K is a set of left and right coset representatives of H in G.

(c) Let $K \leqslant H \leqslant G$, let $a_1, \ldots, a_n \in G$ be left coset representatives of H in G and let $b_1, \ldots, b_m \in H$ be left coset representatives of K in H. Show that $a_i b_j$ $(i = 1, \ldots, n,\ j = 1, \ldots, m)$ are left coset representatives of K in G. Conclude that $[G : K] = [G : H] \cdot [H : K]$. Can the last statement be shown in a shorter way?

9 Normal subgroups and factor groups

9.1 Definition Let $f\colon G \to H$ be a homomorphism between groups. The *kernel* of f is defined as the set of all $a \in G$ with $f(a) = 1_H$. We denote the kernel of f by $\ker(f)$. In other words, $\ker(f) = f^{-1}(1_H)$. Since $\{1_H\}$ is a subgroup of H, Proposition 4.14(b) implies that $\ker(f)$ is a subgroup of G.

9.2 Proposition *Let $f\colon G \to H$ be a homomorphism between groups G and H, let a be an element of G and set $b := f(a)$. Then*

$$f^{-1}(b) = a\ker(f) = \ker(f)a\,.$$

Proof First assume that $a' \in f^{-1}(b)$. Then $f(a') = b$ and $f(a^{-1}a') = f(a^{-1})f(a') = f(a)^{-1}f(a') = b^{-1}b = 1_H$. Thus, $a^{-1}a' \in \ker(f)$ and $a' = (aa^{-1})a' = a(a^{-1}a') \in a\ker(f)$. Conversely, let $ax \in a\ker(f)$ with an element $x \in \ker(f)$. Then $f(ax) = f(a)f(x) = b1_H = b$ and therefore, $ax \in f^{-1}(b)$. This shows that $f^{-1}(b) = a\ker(f)$.

Similarly one shows that $f^{-1}(b) = \ker(f)a$. □

9.3 Corollary *A group homomorphisms $f\colon G \to H$ is injective if and only if* $\ker(f) = \{1_G\}$.

Proof If f is injective then $\ker(f) = \{1_G\}$. In fact, if $\ker(f)$ has more than one element then these elements are all mapped to 1_H, contradicting the injectivity of f. Conversely, assume that $\ker(f) = \{1_G\}$. In order to show that f is injective let $a, a' \in G$ with $f(a) = f(a')$ and set $b := f(a) = f(a')$. Then $a, a' \in f^{-1}(b)$ and, by Propositions 9.2 and 8.8, we have $|f^{-1}(b)| = |\ker(f)| = 1$. Thus, $a = a'$, and f is injective. □

9.4 Definition A subgroup N of a group G is called a *normal* subgroup of G if $aN = Na$ for every $a \in G$. If N is a normal subgroup of G we write $N \trianglelefteq G$. If N is a normal subgroup of G and $N \neq G$ we write $N \triangleleft G$.

> One always has $\{1_G\} \trianglelefteq G$ and $G \trianglelefteq G$. Moreover, if G is abelian then every subgroup of G is normal in G. Proposition 9.2 shows that for every group homomorphism $f\colon G \to H$ one has $\ker(f) \trianglelefteq G$.

9.5 Proposition *Let G be a group and let N be a subgroup of G. The following are equivalent:*
(i) *$aN = Na$ for all $a \in G$, i.e. N is normal in G.*
(ii) *$aNa^{-1} = N$ for all $a \in G$.*
(iii) *$aNa^{-1} \subseteq N$ for all $a \in G$.*

Proof (i)⇒(ii): Let $a \in G$. By (i) we have $aN = Na$. We multiply this equation from the right with a^{-1} and obtain $aNa^{-1} = N$.

(ii)⇒(iii): This is trivial.

(iii)⇒(i): Let $a \in G$. We will show that $aN = Na$. By (iii) we have $aNa^{-1} \subseteq N$ and $a^{-1}Na \subseteq N$. Multiplying the first inclusion with a from the right yields $aN \subseteq Na$ and multiplying the second inclusion from the left with a yields $Na \subseteq aN$. □

9.6 Theorem *Assume that N is a normal subgroup of G.*

(a) *For any $a, b \in G$ one has (with the multiplication of subsets of G defined in 8.1):*

$$(aN)(bN) = (ab)N = N(ab) = (Na)(Nb)\,.$$

(b) *The set of left (or right) cosets G/N is a group under the binary operation in (a). The element $1_GN = N$ is the identity element. For each $a \in G$, the inverse of aN is equal to $a^{-1}N$.*

(c) *The function $\nu\colon G \to G/N$, $a \mapsto aN$, is a surjective group homomorphism with* $\ker(\nu) = N$.

Proof (a) Since N is normal in G one has $bN = Nb$. Thus,

$$(aN)(bN) = a(Nb)N = a(bN)N = (ab)(NN) = (ab)N\,,$$

since $NN = N$. Similiarly one obtains $(Na)(Nb) = N(ab)$. Since N is normal one has $(ab)N = N(ab)$.

(b) By Part (a), the multiplication of left cosets of N defines a binary operation on G/N. This binary operation is associative, since $(XY)Z = X(YZ)$ for any three subsets X, Y, Z of G. The multiplication formula in Part (a) gives $(1_GN)(aN) = (1_Ga)N = aN = (a1_G)N = (aN)(1_GN)$. Thus, $N = 1_GN$ is an identity element. The multiplication rule in Part (a) also implies that $(aN)(a^{-1}N) = (aa^{-1})N = 1_GN = (a^{-1}a)N = (a^{-1}N)(aN)$. Therefore, the element $a^{-1}N$ is an inverse of the element aN.

(c) For $a, b \in G$ we have $\nu(ab) = abN$ and $\nu(a)\nu(b) = (aN)(bN) = abN$. This shows that ν is a homomorphism. For $a \in G$ we have

$$a \in \ker(\nu) \iff aN = N \iff a \in N\,.$$

Thus, $\ker(\nu) = N$. Finally, ν is clearly surjective, since every left coset of N in G is of the form $aN = \nu(a)$ for some $a \in G$. □

9.7 Definition Let N be a normal subgroup of G. The group G/N from Theorem 9.6 is called the *factor group* of G with respect to N, or short G *modulo* N. Its order is equal to $[G : N]$. If G is finite, this is equal to $|G|/|N|$, by Lagrange's Theorem. The epimorphism $\nu\colon G \to G/N$, $g \mapsto gN$, is called the *natural epimorphism.*

9.8 Proposition *If N is a subgroup of G of index 2 then N is normal in G.*

Proof Let $a \in G$. If $a \in N$ then $aN = N = Na$. If $a \notin N$ then $aN = G \setminus N$, since G has precisely two left cosets and since G is the disjoint union of the two left cosets of N, N being one of them. But similarly, if $a \notin N$, one sees that $Na = G \setminus N$. Therefore, $aN = Na$ also in this case. □

9.9 Examples (a) For any group G, one has $\{1_G\} \trianglelefteq G$ and $G \trianglelefteq G$. The natural epimorphism $\nu\colon G \mapsto G/\{1_G\}$ is an isomorphism, since $\ker(\nu) = \{1_G\}$. The factor group G/G is a trivial group.

(b) If G is an abelian group then every subgroup N of G is normal in G, since $aN = Na$ for all $a \in G$.

(c) If $f\colon G \to H$ is a group homomorphism then $\ker(f)$ is a normal subgroup of G. In fact, by Proposition 9.2 we have $a\ker(f) = f^{-1}(f(a)) = \ker(f)a$ for all $a \in G$. On the other hand, every normal subgroup N of G is the kernel of the corresponding natural epimorphism $\nu\colon G \to G/N$ by Theorem 9.6(c). Thus, the normal subgroups of G are precisely the kernels of all homomorphisms from G to H, where H can be any group.

(d) For every $n \geqslant 2$ one has $[\mathrm{Sym}(n)\colon \mathrm{Alt}(n)] = 2$, cf. Examples 8.13(a). Therefore, $\mathrm{Sym}(n)/\mathrm{Alt}(n)$ is a group of order 2. Its two elements are given by the set of even permutations and the set of odd permutations.

(e) For every $n \in \mathbb{N}$ we obtain a factor group $\mathbb{Z}/n\mathbb{Z}$ of $\mathbb{Z}$. By Example 8.13(b) it has the n elements $0 + n\mathbb{Z}, 1 + n\mathbb{Z}, \ldots, (n-1) + n\mathbb{Z}$. It is now clear that the function

$$f\colon \mathbb{Z}_n \to \mathbb{Z}/n\mathbb{Z}\,, \quad i \mapsto i + n\mathbb{Z}\,,$$

is bijective. It is also a group homomorphism. In fact, for $i, j \in \{0, 1, \ldots, n-1\}$ one has: $i +_n j$ is the unique element $r \in \{0, 1, \ldots, n-1\}$ such that $i + j \equiv r \mod n$, and $f(i +_n j) = r + n\mathbb{Z}$. On the other hand we have $f(i) + f(j) = (i + n\mathbb{Z}) + (j + n\mathbb{Z}) = (i + j) + n\mathbb{Z} = r + n\mathbb{Z}$. Altogether, f is an isomorphism.

(f) The *center* of a group G is defined by

$$Z(G) := \{a \in G \mid ax = xa \text{ for all } x \in G\}\,.$$

It is easy to see that $Z(G)$ is a normal subgroup of G.

(g) The *normalizer* of a subgroup H of a group G is defined as

$$N_G(H) := \{a \in G \mid aHa^{-1} = H\}\,.$$

It is easy to see that $H \trianglelefteq N_G(H) \leqslant G$.

(h) The *centralizer* of a subset X of a group G is defined by

$$C_G(X) := \{a \in G \mid ax = xa \text{ for all } x \in X\}\,.$$

It is straightforward to prove that $C_G(X)$ is a subgroup of G. It is also an easy exercise to show that if H is a subgroup of G then $C_G(H) \trianglelefteq N_G(H)$.

9.10 Definition A group G ia called *simple* if $|G| > 1$ and if G has no normal subgroups other than G and $\{1_G\}$.

9.11 Remark (a) If $1 < N \triangleleft G$ we think of G being constructed from the two groups N and G/N. We also can think of G/N as an approximation of G such that N describes the error terms that are allowed. The smaller N is, the better is the approximation.

(b) For every prime p the group $(\mathbb{Z}_p, +_p)$ is a finite abelian simple group. In fact, by Lagrange's Theorem, $\mathbb{Z}_p$ has no normal subgroups other than $\{0\}$ and $\mathbb{Z}_p$. It is not difficult to see that every finite simple group which is abelian is isomorphic to one of the groups $\mathbb{Z}_p$, for a prime p, see Exercise 7.

(c) The finite simple groups are known. They consist of a finite number of infinite families together with a finite number of groups which do not belong to any of these families. One of the families is the family of alternating groups $\mathrm{Alt}(n)$, $n \geqslant 5$. There are 26 groups that do not belong to any of the infinite families. They are called the *sporadic simple groups*. The largest one among them is called the *Monster* group M. Its order is equal to

$$\begin{aligned} |M| &= 808,017,424,794,512,875,886,459,904,961,710,757,005,754,368,000,000,000 \\ &= 2^{46} \cdot 3^{20} \cdot 5^9 \cdot 7^6 \cdot 11^2 \cdot 13^3 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71\,, \end{aligned}$$

a number with 54 digits. It is mysterious that only very small primes occur in the factorization of this order. This phenomenon also occurs for the other 25 sporadic simple groups.

Exercises for §9

1. Let N be a subgroup of a group G. Show that the following are equivalent:

(i) Every left coset of N in G is equal to a right coset of N in G.

(ii) Every right coset of N in G is equal to a left coset of N in G.

(iii) N is normal in G.

2. Assume that M and N are normal subgroups of a group G.

(a) Show that $M \cap N$ is a normal subgroup of G.

(b) Show that MN is a normal subgroup of G.

3. Let G be a group.

(a) Show that $Z(G)$ is an abelian and normal subgroup of G.

(b) Show that G is abelian if and only if $Z(G) = G$.

(c) Show that if $f\colon G \to H$ is a group isomorphism then $f(Z(G)) = Z(H)$.

4. Let H be a subgroup of a group G.

(a) Show that $H \trianglelefteq N_G(H) \leqslant G$.

(b) Show that $C_G(H)$ is a subgroup of G and that $C_G(H) \trianglelefteq N_G(H)$.

(c) Let $V := \langle (1,2)(3,4), (1,3)(2,4) \rangle \leqslant \mathrm{Sym}(4) =: G$. Compute $N_G(V)$ and $C_G(V)$.

5. (a) Compute $Z(D_8)$ and $Z(D_{10})$.

(b) Compute $Z(Q_8)$.

6. Show that $Z(\mathrm{Sym}(n)) = 1$ for all $n \geqslant 3$.

7. Assume that G is a simple abelian group. Show that G is cyclic and that the order of G is a prime.

8. Show again that $\mathrm{Alt}(4)$ has no subgroup of order 6, see also Exercise 8.4. (Hint: Assume H is a subgroup of order 6. Show first that H is normal in $\mathrm{Alt}(4)$. Then show that for every $\sigma \in \mathrm{Alt}(4)$, the element σ^2 must be contained in H, by using the factor group $\mathrm{Alt}(4)/H$. Finally, check how many elements are of the form σ^2.)

10 Isomorphism Theorems

If $f\colon G \to H$ is a group homomorphism, we denote by $\mathrm{im}(f)$ its *image*, i.e., the subset $f(G)$ of H. By Proposition 4.14(a), this is a subgroup of H.

10.1 Theorem (Fundamental Theorem of Homomorphisms (FTH)) *Let $f\colon G \to H$ be a group homomorphism and let N be a normal subgroup of G which is contained in $\ker(f)$. Then there exists a unique group homomorphism $\overline{f}\colon G/N \to H$ such that $\overline{f} \circ \nu = f$. Here $\nu\colon G \to G/N$ denotes the natural epimorphism. In other words, $\overline{f}(aN) = f(a)$ for all $a \in G$. Moreover, $\mathrm{im}(\overline{f}) = \mathrm{im}(f)$ and $\ker(\overline{f}) = \{aN \in G/N \mid a \in \ker(f)\} = \ker(f)/N$.*

Proof Note that if $aN = bN$ for $a, b \in G$ then $a^{-1}b \in N \leqslant \ker(f)$, $f(a)^{-1}f(b) = f(a^{-1}b) = 1_H$ and therefore $f(a) = f(b)$. Thus, we can define a function $\overline{f}\colon G/N \to H$ by $\overline{f}(aN) := f(a)$. This is a homomorphism, since

$$\overline{f}((aN)(bN)) = \overline{f}(abN) = f(ab) = f(a)f(b) = \overline{f}(aN)\overline{f}(bN)\,,$$

and it clearly satisfies $\overline{f}(\nu(a)) = \overline{f}(aN) = f(a)$ for all $a \in G$. Thus, $\overline{f} \circ \nu = f$. If $g\colon G/N \to H$ is also a homomorphism with $g \circ \nu = f$ then $g(aN) = g(\nu(a)) = f(a) = \overline{f}(aN)$ for all $a \in G$. Thus, $g = \overline{f}$. Next we determine $\mathrm{im}(\overline{f})$ and $\ker(\overline{f})$. Since $\overline{f}(aN) = f(a)$ for all $a \in G$, we obtain $\mathrm{im}(\overline{f}) = \mathrm{im}(f)$. Moreover, for $a \in G$ we have $\overline{f}(aN) = 1_H$ if and only if $f(a) = 1_H$. This in turn is equivalent to $a \in \ker(f)$. Thus, $\ker(\overline{f}) = \{aN \in G/N \mid a \in \ker(f)\} = \ker(f)/N$. □

10.2 Corollary (1^{st} Isomorphism Theorem) *Let $f\colon G \to H$ be a group homomorphism. Then $G/\ker(f)$ is isomorphic to $\mathrm{im}(f)$.*

Proof We apply the FTH to $f\colon G \to H$ and $N := \ker(f)$. This yields a homomorphism $\overline{f}\colon G/\ker(f) \to H$ with $\ker(\overline{f}) = \{a\ker(f) \in G/\ker(f) \mid a \in \ker(f)\} = \{\ker(f)\} = \{1_{G/\ker(f)}\}$. Thus, $\overline{f}$ is injective. Moreover, we know from the FTH that $\mathrm{im}(\overline{f}) = \mathrm{im}(f)$. Therefore, $\overline{f}$ defines an injective and surjective homomorphism from $G/\ker(f)$ to $\mathrm{im}(\overline{f}) = \mathrm{im}(f)$. □

10.3 Examples In this example we try to determine factor groups G/N in various situations.

(a) For $n \geqslant 2$, the sign homomorphism $\mathrm{sgn}\colon \mathrm{Sym}(n) \to \{1, -1\}$ is a surjective group homomorphism with $\ker(\mathrm{sgn}) = \mathrm{Alt}(n)$. The Fundamental Theorem of Homomorphims induces an isomorphism $\mathrm{Sym}(n)/\mathrm{Alt}(n) \cong \{1, -1\}$.

(b) The set $\mathbb{R}^\times := \mathbb{R} \setminus \{0\}$ is a group under multiplication and $\det\colon \mathrm{GL}_n(\mathbb{R}) \to \mathbb{R}^\times$ is a surjective homomorphism with $\ker(\det) = \mathrm{SL}_n(\mathbb{R})$. Thus, $\mathrm{SL}_n(\mathbb{R})$ is a normal subgroup of $\mathrm{GL}_n(\mathbb{R})$ and, by the 1^{st} Isomorphism Theorem, we have $\mathrm{GL}_n(\mathbb{R})/\mathrm{SL}_n(\mathbb{R}) \cong \mathbb{R}^\times$.

(c) The center of D_8 is equal to $\{1, \sigma^2\} =: Z$, where σ denotes the counterclockwise rotation of $90°$. Therefore, D_8/Z is a group of order 4, and it must be isomorphic to the cyclic group of

order 4, $\mathbb{Z}_4$, or to the Klein Four-Group, $\mathbb{Z}_2 \times \mathbb{Z}_2$. Which one is it? This time we don't have a homomorphism $f\colon D_8 \to H$ at hand that has kernel $\{1, \sigma^2\}$, and we will have to determine the factor group D_8/Z differently. Recall that a cyclic group of order 4 has an element of order 4, but the Klein 4-group doesn't. We compute the elements of D_8/Z. If $\tau \in D_8$ denotes a reflection then $\tau\sigma = \sigma^{-1}\tau$ and we obtain $D_8/Z = \{Z, \sigma Z, \tau Z, \sigma\tau Z\}$. It follows that $(aZ)^2 = a^2 Z = Z$ for each of the 4 cosets $aZ \in D_8/Z$. Therefore D_8/Z is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$.

10.4 Theorem (Correspondence Theorem) *Let G be a group, let N be a normal subgroup of G and let $\nu\colon G \to G/N$, $a \mapsto aN$, denote the natural epimorphism. Then the function*

$$\Phi\colon \{N \leqslant H \leqslant G\} \to \{X \leqslant G/N\}\,, \quad H \mapsto \nu(H) = H/N\,,$$

is a bijection between the set of all subgroups H of G which contain N and the set of all subgroups X of G/N. Its inverse is given by

$$\Psi\colon \{X \leqslant G/N\} \to \{N \leqslant H \leqslant G\}\,, \quad X \mapsto \nu^{-1}(X)\,.$$

Moreover, the bijection Φ preserves inclusion and normality. That is, for subgroups $N \leqslant H \leqslant G$ and $N \leqslant K \leqslant G$ one has

$$H \leqslant K \iff H/N \leqslant K/N$$

and

$$H \trianglelefteq G \iff H/N \trianglelefteq G/N\,.$$

Proof If H is a subgroup of G with $N \leqslant H$ then $\nu(H) = \{aN \mid a \in H\} = H/N$ is a subgroup of G/N by Proposition 4.14(a). Also, if X is a subgroup of G/N then $\nu^{-1}(X)$ is a subgroup of G by Proposition 4.14(b). Moreover, since $1_{G/N} \in X$, we have $N = \ker(\nu) = \nu^{-1}(\{1_{G/N}\}) \leqslant \nu^{-1}(X)$. Thus, the maps Φ and Ψ take their values in the indicated sets.

Next we show that $\Psi \circ \Phi$ is the identity, i.e., that $\nu^{-1}(\nu(H)) = H$. Clearly, H is contained in $\nu^{-1}(\nu(H))$ by the definition of the preimage of $\nu(H)$. Conversely, if $g \in \nu^{-1}(\nu(H))$ then $\nu(g) \in \nu(H)$. Thus, there exists $h \in H$ such that $\nu(g) = \nu(h)$. This implies that $\nu(gh^{-1}) = \nu(g)\nu(h)^{-1} = 1_{G/N}$ and $gh^{-1} \in \ker(\nu) = N$. Thus, $g \in Nh \subseteq H$, since $N \leqslant H$.

Next we show that $\Phi \circ \Psi$ is the identity, i.e., that $\nu(\nu^{-1}(X)) = X$. But this holds in general for every surjective function ν as one easily verifies.

If $N \leqslant H \leqslant K \leqslant G$ then clearly $\nu(H) \leqslant \nu(K)$ and if $X \leqslant Y \leqslant G/N$ then clearly $\nu^{-1}(X) \leqslant \nu^{-1}(Y)$. This shows the second to last statement (monotonicity).

Finally, if H is normal in G then $gHg^{-1} \subseteq H$ for all $g \in G$. Applying ν to this containment and using that ν is a homomorphism, we obtain that $\nu(g)\nu(H)\nu(g)^{-1} \subseteq \nu(H)$ for all $g \in G$. Since ν is surjective, this implies that $\nu(H)$ is normal in G/N. Conversely, if X is normal in G/N and $X = \nu(H)$ then $\nu(gHg^{-1}) = \nu(g)\nu(H)\nu(g)^{-1} \subseteq \nu(H)$ for all $g \in G$. Applying ν^{-1} to this inclusion, we obtain $gHg^{-1} \leqslant H$ by the monotonicity statement and since Φ and Ψ are inverses. This shows that H is normal in G, and the proof is complete. □

In general, if H and K are subgroups of a group G, the subset HK is not necessarily a subgroup of G. We will investigate under what additional conditions HK is a subgroup of G. It is easy to see that if H and K are normal then HK is again a normal subgroup, see Exercise 9.2(b). The next proposition gives a formula for the number of elements in HK, and the subsequent proposition gives conditions under which HK is again a subgroup.

The proof of the next proposition uses the following useful counting principle: If $f\colon A \to B$ is a surjective function between finite sets A and B then $|A| = \sum_{b\in B} |f^{-1}(b)|$.

10.5 Proposition *Let G be a group and let H and K be finite subgroups of G. Then*

$$|HK| = \frac{|H|\cdot|K|}{|H\cap K|} = |KH|\,.$$

Proof Consider the function $f\colon H\times K \to HK$, $(h,k)\mapsto hk$. This is a surjective function. Therefore,

$$|H\times K| = \sum_{b\in HK} |f^{-1}(b)|\,. \tag{10.5.a}$$

Next we fix $b\in HK$ and determine $|f^{-1}(b)|$. We can write $b=hk$ with some $h\in H$ and $k\in K$ which we fix. Then every element of the form $(hx, x^{-1}k)$, with $x\in H\cap K$, is contained in $f^{-1}(b)$, since $(hx,x^{-1}k)\in H\times K$ and $f(hx,x^{-1}k) = hxx^{-1}k = hk = b$. On the other hand, if $(h',k')\in H\times K$ and $f(h',k') = b$ then $h'k' = hk$ and $x := h^{-1}h' = kk'^{-1} \in H\cap K$. This implies that $(h',k') = (hx,x^{-1}k)$. Therefore, we have proved that $f^{-1}(b) = \{(hx,x^{-1}k) \mid x\in H\cap K\}$. But the latter set has precisely $|H\cap K|$ elements, since $(hx,x^{-1}k) = (hy,y^{-1}k)$ implies $x=y$ for $x,y\in H\cap K$. Substituting this in Equation (10.5.a) yields

$$|H|\cdot|K| = |H\times K| = \sum_{b\in HK} |f^{-1}(b)| = \sum_{b\in HK} |H\cap K| = |HK|\cdot|H\cap K|\,,$$

and the first equation in the proposition follows. The second equation can be shown in a similar way, or by noting that $HK\to KH$, $b\mapsto b^{-1}$, is a bijective function with inverse $KH\to HK$, $a\mapsto a^{-1}$. □

10.6 Example Let $G = \mathrm{Sym}(3)$, $H = \{\mathrm{id}, (1,2)\}$ and $K = \{\mathrm{id},(2,3)\}$. Then $|HK| = |H|\cdot|K|/|H\cap K| = 4$. By Lagrange's Theorem, HK cannot be a subgroup of G. Note that $HK = \{1,(1,2),(2,3),(1,2,3)\}$ and $KH = \{1,(1,2),(2,3),(1,3,2)\}$. Thus, $HK\neq KH$, in accordance with the statement of the next proposition.

10.7 Proposition *Let G be a group and let H and K be subgroups of G.*

(a) *The following are equivalent:*

(i) *HK is a subgroup of G.*

(ii) *KH is a subgroup of G.*

(iii) *$HK = KH$.*

(b) *If $K \leqslant N_G(H)$ or $H \leqslant N_G(K)$ then $HK = KH$ and HK is a subgroup of G. In particular, if one of the subgroups H and K is normal then $HK = KH$ and HK is a subgroup of G.*

Proof (a) Assume that HK is a subgroup of G. Then $HK = (HK)^{-1} = K^{-1}H^{-1} = KH$. So (i) implies (iii). Similarly, (ii) implies (iii). Next assume that $HK = KH$. We will show that HK is a subgroup of G. First we have $1_G = 1_G 1_G \in HK$. Secondly, if $a \in HK$ then $a = hk$ for some $h \in H$ and $k \in K$ and $a^{-1} = k^{-1}h^{-1} \in KH = HK$. Finally, if $a \in HK$ and $b \in HK$ then $ab \in HKHK = HHKK = HK$. Thus, $HK \leqslant G$ and also $KH = HK \leqslant G$. This shows that (iii) implies (i) and (ii).

(b) Assume first that $K \leqslant N_G(H)$. By Part (a) it suffices to show that $HK = KH$. Let $h \in H$ and $k \in K$. Then $khk^{-1} \in H$ and $k^{-1}hk \in H$, since $K \leqslant N_G(H)$. Therefore, $hk = kk^{-1}hk \in KH$ and $kh = khk^{-1}k \in HK$. This shows that $HK = KH$. By symmetry, also the condition $H \leqslant N_G(K)$ implies that $HK = KH$. □

10.8 Theorem (2^{nd} Isomorphism Theorem) *Let G be a group, let $H \leqslant G$ and $N \trianglelefteq G$. Then N is normal in $HN = NH$, $H \cap N$ is normal in H, and there exists an isomorphism*

$$\phi\colon H/(H \cap N) \to HN/N$$

with the property that $\phi(a(H \cap N)) = aN$ for all $a \in H$.

Proof First, $NH = HN$ is a subgroup of G by Proposition 10.7(b). Moreover, since N is normal in G, N is also normal in HN.

Next let f denote the composition of the group homomorphisms $H \to NH$, $a \mapsto a$, and $NH \mapsto NH/N$, $a \mapsto aN$. Then $f\colon H \to HN/N$ is a homomorphism and $f(a) = aN$. We show that f is surjective. In fact, let $a \in H$ and $n \in N$ then $anN = aN = f(a)$.

Finally we show that $\ker(f) = H \cap N$. This will also imply that $H \cap N$ is normal in H. Clearly, if $a \in H \cap N$ then $f(a) = aN = N$ and if $a \in H$ such that $f(a) = 1_{HN/N} = N$ then $aN = N$ and $a \in N$, so that $a \in H \cap N$.

Now, by the Fundamental Theorem of Homomorphisms, there exists a group homomorphism $\overline{f}\colon H/H \cap N \to HN/N$ with $\overline{f}(a(H \cap N)) = f(a) = aN$. This homomorphism is injective, since $\ker(f) = H \cap N$ and it is surjective, since f was surjective. □

The following theorem is often used to simplify expressions that involve factor groups of factor groups. By the Correspondence Theorem, a normal subgroup of a factor group G/N is of the form H/N with $N \leqslant H \trianglelefteq G$. In this situation one can consider the factor group $(G/N)/(H/N)$ of G/N. As for fractions of numbers, the two "denominators" N can be "canceled" by the following theorem.

10.9 Theorem (3^{rd} Isomorphism Theorem) *Let G be a group, let N and H be normal subgroups of G and assume that N is contained in H . Then*

$$(G/N)/(H/N) \cong G/H\,.$$

Proof By the Correspondence Theorem, the subgroup H/N is normal in G/N. Let $\nu_N\colon G \to G/N$ and $\nu_{H/N}\colon G/N \to (G/N)/(H/N)$ denote the canonical epimorphisms. Then their composition $f\colon G \to (G/N)/(H/N)$ is a surjective group homomorphism with $\ker(f) = \nu_N^{-1}(\ker(\nu_{H/N}))$. But $\ker(\nu_{H/N}) = H/N$ and $\nu_N^{-1}(H/N) = H$, again by the Correspondence Theorem. By the First Isomorphism Theorem we obtain $G/H \cong (G/N)/(H/N)$. □

Exercises for §10

1. Assume that G is a group.

(a) Let $N \trianglelefteq G$ and let $N \leqslant H \leqslant G$. Show that $N \trianglelefteq H$.

(b) Let $N \trianglelefteq G$, let $\nu_N \colon G \to G/N$ denote the natural epimorphism, and let $H \leqslant G$. Show that $\nu_N(H) = HN/N = NH/N$.

(c) Let H and K be subgroups of G and assume that $HK \subseteq H$. Show that $K \leqslant H$.

2. Normality is not transitive: Find an example of a group G and subgroups K and H of G such that $K \triangleleft H \triangleleft G$ but K is not normal in G.

3. Let M and N be normal subgroups of a group G and assume that $M \cap N = 1$.

(a) Show that $ab = ba$ for all $a \in N$ and all $b \in M$.

(b) Assume additionally that $MN = G$. Show that the function $f \colon M \times N \to G$, $(a, b) \mapsto ab$, is an isomorphism. Here $M \times N$ denotes the direct product group formed from the groups M and N.

4. (a) Show that a factor group of an abelian group is abelian.

(b) Show that a factor group of a cyclic group is cyclic.

5. Let $V := \langle (1,2)(3,4), (1,3)(2,4) \rangle$. Then V is normal in Sym(4) according to Exercise 9.4(c). What is the isomorphism type of Sym(4)$/V$? (Hint: Consider Sym(3) as a subgroup of Sym(4) and use the 2^{nd} Isomorphism Theorem.)

6. Find an example of two finite groups G and H with normal subgroups $N \triangleleft G$ and $M \triangleleft H$ such that $N \cong M$ and $G/N \cong H/M$, but $G \ncong H$.

7. Let G be a group and assume that $\{1\} < N \triangleleft G$ such that N and G/N are simple (we think of G being made up as a molecule from the atoms N and G/N). Assume that also M is a normal subgroup of G such that M and G/M are simple. Show that

(i) $M \cong N$ and $G/M \cong G/N$

or

(ii) $M \cong G/N$ and $G/M \cong N$.

(Hint: Start by distinguishing the cases $M = N$ and $M \neq N$. The first case should lead to (i) and the second case to (ii). Use appropriate isomorphism theorems.)

8. Let M and N be normal subgroups of a group G such that G/M and G/N are abelian. Show that $G/(M \cap N)$ is abelian. (Hint: Show that $f \colon G \to G/M \times G/N$, $a \mapsto (aM, aN)$, is a homomorphism. Determine its kernel and use the first Isomorphism Theorem.)

11 Group action on a set

One often thinks of a group G as a group of movements of the elements of some set X. This was the case with symmetry groups, where every group element moves the points of a geometric object. The axiomatic mathematical notion covering this point of view is the notion of a group action on a set. A group G can act on any set X. However, it can also act on sets that arise internally from G: For instance, on G itself, or the set of subgroups of G, or on the set G/H of cosets for a subgroup $H \leqslant G$. In this section we introduce the necessary terminology and basic results on group actions, see Theorem 11.10 and Corollary 11.12 on Burnside's orbit equation and its consequence for a group G of prime power order. We apply this to obtain two fundamental results in group theory: Theorem 11.15 stating that a non-trivial group of prime power order has non-trivial center, and Cauchy's Theorem (Theorem 11.18) stating that if a prime p divides the order of a finite group G then G has an element of order p. In the following section we will continue to apply the notion of group actions to prove Sylow's Theorems on subgroups of p-power order in a group G.

11.1 Definition An *action* of a group G on a set X is a function

$$*\colon G \times X \to X\,, \quad (g,x) \mapsto g * x\,,$$

satisfying the following two conditions:

(i) $1_G * x = x$ for all $x \in X$.

(ii) $g * (h * x) = (gh) * x$ for all $g, h \in G$ and all $x \in X$.

In this case one says that G *acts on* X via $*$, or that X is a G*-set* via $*$.

11.2 Examples (a) Every group G acts on itself by left-multiplication: $G \times G \to G$, $(g,x) \mapsto gx$.

(b) The group $G = \mathrm{GL}_2(\mathbb{R})$ acts on the set $X = \mathbb{R}^2$ of column vectors of length 2 by the usual matrix multiplication:

$$A * \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = A \begin{pmatrix} x_2 \\ x_2 \end{pmatrix} = \begin{pmatrix} ax_1 + bx_2 \\ cx_1 + dx_2 \end{pmatrix}\,, \text{ if } A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

In fact, for all $x \in \mathbb{R}^2$ and all $A, B \in \mathrm{GL}_2(\mathbb{R})$, one has

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} x = x \quad \text{and} \quad (AB)x = A(Bx)\,.$$

(c) Let X be any set, and let $G \leqslant \mathrm{Sym}(X)$ be a subgroup. Then G acts on X via $\sigma * x := \sigma(x)$. In fact, $\mathrm{id}_X(x) = x$ and $(\sigma\tau) * x = (\sigma \circ \tau)(x) = \sigma(\tau(x)) = \sigma * (\tau * x)$ for all $x \in X$ and all $\sigma, \tau \in \mathrm{Sym}(X)$.

(d) The dihedral group D_8 (symmetry group of a square, viewed as subgroup of $\mathrm{O}_2(\mathbb{R})$) acts on the 4 vertices (numbered v_1, v_2, v_3, v_4) of the square with center in the origin by $f * v_i := f(v_i)$, for $f \in D_8$ and $i \in \{1, 2, 3, 4\}$. In fact, $\mathrm{id}_{O_2(\mathbb{R})}(v_i) = v_i$ and $(f \circ g) * v_i = (f \circ g)(v_i) = f(g(v_i)) = f * (g * v_i)$ for all $i \in \{1, 2, 3, 4\}$ and all $f, g \in D_8$.

11.3 Proposition *Assume that G acts on the set X via $*$. For every $g \in G$, the function*

$$\sigma_g \colon X \to X\,, \quad x \mapsto g * x\,,$$

is bijective. The resulting function

$$\rho \colon G \to \mathrm{Sym}(X)\,, \quad g \mapsto \sigma_g\,,$$

is a group homomorphism and it is called the permutation representation *of the action of G on X.*

Proof First let $g \in G$. We want to show that σ_g is bijective. For the injectivity part assume that $\sigma_g(x) = \sigma_g(y)$ for elements $x, y \in X$. This means that $g * x = g * y$ and it implies that $g^{-1} * (g * x) = g^{-1} * (g * y)$. But by the second axiom for group actions this means $(g^{-1}g) * x = (g^{-1}g) * y$ or equivalently $1_G * x = 1_G * y$. Now by the first axiom of group actions we obtain $x = y$, and σ_g is injective. In order to see that σ_g is surjective, let $x \in X$. Then $\sigma_g(g^{-1} * x) = g * (g^{-1} * x) = (gg^{-1}) * x = 1_G * x = x$ and x is contained in the image of σ_g. Thus, σ_g is surjective. Altogether, σ_g is bijective.

Next we show that $\rho \colon G \to \mathrm{Sym}(X)$, $g \mapsto \sigma_g$, is a group homomorphism. So let $g, h \in G$. We need to show that $\rho(gh) = \rho(g) \circ \rho(h)$, or in other words that $\sigma_{gh} = \sigma_g \circ \sigma_h$. To show the latter equality, let $x \in X$. We need to show that $\sigma_{gh}(x) = \sigma_g(\sigma_h(x))$. But this is equivalent to the equation $(gh) * x = g * (h * x)$, which holds by the second axiom for group actions. □

11.4 Proposition *Let G be a group and let X be a set. Furthermore, let $\rho \colon G \to \mathrm{Sym}(X)$ be a group homomorphism. Then the function*

$$* \colon G \times X \to X\,, \quad (g, x) \mapsto (\rho(g))(x)$$

defines an action of G on X.

Proof In order to verify the first group action axiom we need to show that $(\rho(1_G))(x) = x$ for all $x \in X$. But, since ρ is a homomorphism, we have $\rho(1_G) = \mathrm{id}_X$ and the first axiom is verified. Next we verify the second axiom. So let $g, h \in G$ and let $x \in X$. Then $g * (h * x) = g * (\rho(h)(x)) = \rho(g)(\rho(h)(x)) = (\rho(g) \circ \rho(h))(x) = \rho(gh)(x) = (gh) * x$. □

11.5 Remark It is straightforward to verify that the two constructions in Propositiions 11.3 and 11.4 are inverse to each other.

11.6 Proposition *Assume that the group G acts on the set X via $*$. The relation on X defined by*

$$x \sim y :\Longleftrightarrow \text{ There exists } g \in G \text{ such that } g * x = y$$

is an equivalence relation. Its equivalence classes are called the orbits of G on X *or the* G-orbits of X.

Proof To verify reflexivity, let $x \in X$. Then $x \sim x$, since $1_G * x = x$. To verify symmetry, let x, y be elements in X such that $x \sim y$. Then there exists $g \in G$ such that $g*x = y$. This implies that $g^{-1}*(g*x) = g^{-1}*y$ and further that $1_G*x = g^{-1}*y$ and $g^{-1}*y = x$. Thus $y \sim x$. Finally, to verify transitivity, let x, y, z be elements of X and assume that $x \sim y$ and $y \sim z$. Then there exist $g, h \in G$ such that $g*x = y$ and $h*y = z$. This implies that $(hg)*x = h*(g*x) = h*y = z$ and therefore $x \sim z$. □

11.7 Remark/Definition Assume that X is a G-set via $*$.

(a) For every $x \in X$ we denote the G-orbit of X which contains x by O_x. Thus,

$$O_x = \{g * x \mid g \in G\}\,.$$

Since $\sim$ is an equivalence relation on X, cf. Proposition 11.6, X is the disjoint union of its G-orbits. Every G-orbit of X is again a G-set in its own right. The G-set X is called *transitive* if X has only one orbit, i.e., if for any two elements $x, y \in X$ there exists $g \in G$ such that $g * x = y$. In general, every G-orbit of X is a transitive G-set, and this way, X is a disjoint union of transitive G-sets.

(b) For $x \in X$ we define the *stabilizer* of x in G by

$$\mathrm{stab}_G(x) := \{g \in G \mid g * x = x\}\,.$$

It is easy to see that $\mathrm{stab}_G(x)$ is a subgroup of G. It is not difficult to verify that, for $g \in G$, one has $\mathrm{stab}(g * x) = g\,\mathrm{stab}_G(x)g^{-1}$ and that the kernel of the permutation representation $\rho\colon G \to \mathrm{Sym}(X)$ associated to the G-set X is given by

$$\ker(\rho) = \bigcap_{x \in X} \mathrm{stab}_G(x)\,.$$

(c) An element $x \in X$ is called a *G-fixed point* if $g * x = x$, for all $g \in G$. The set of G-fixed points of X is denoted by X^G. Note that for every $x \in X$ one has:

$$x \in X^G \iff \mathrm{stab}_G(x) = G \iff O_x = \{x\}\,.$$

11.8 Example (a) G acts on $X = G$ *via left multiplication*: $g * x = gx$ for $g \in G$ and $x \in G$.

(b) More generally, let H be a subgroup of G. Then $X := G/H$, the set of left cosets of H in G, is a G-set via left multiplication

$$g * (aH) = gaH\,.$$

(Note that if $H = \{1_G\}$ then we recover the example in part (a) if we identify $a\{1_G\}$ with a.) This action is transitive, since for every $a, b \in G$, one has $(ba^{-1})*(aH) = bH$. The stabilizer of H in G is $\mathrm{stab}_G(H) = H$ and, by Remark 11.7(b), $\mathrm{stab}_G(aH) = \mathrm{stab}_G(a * H) = a\,\mathrm{stab}_G(H)a^{-1} = aHa^{-1}$. In particular, aHa^{-1} is again a subgroup of G. The kernel of the corresponding permutation representation ρ is equal to $\bigcap_{a\in G} aHa^{-1}$. This group is also called the *core* of H in G and it is denoted by $\mathrm{core}_G(H)$. As the kernel of the homomorphism $\rho\colon G \to \mathrm{Sym}(G/H)$, the subgroup $\mathrm{core}_G(H)$ is normal in G.

> The following theorem seems striking at first, but it does not have as many applications as one might think.

11.9 Theorem (Cayley's Theorem) *Let G be a finite group of order n. Then G is isomorphic to a subgroup of* $\mathrm{Sym}(n)$.

Proof Let $\rho\colon G \to \mathrm{Sym}(G)$ denote the permutation representation associated to the left multiplication action of G on itself. Then ρ is injective. In fact, if g and h are elements of G such that $ga = ha$ for all $a \in G$ then $g = h$. Moreover $\mathrm{Sym}(G)$ is isomorphic to $\mathrm{Sym}(n)$ by Proposition 6.1. Composing ρ with such an isomorphism, we obtain an injective homomorphism $\rho'\colon G \to \mathrm{Sym}(n)$. Thus, G is isomorphic to the subgroup $\rho'(G)$ of $\mathrm{Sym}(n)$. □

> The following theorem will give an important counting principle. If a finite group G acts on a finite set X then one can count the number of elements in X from knowledge of the orbits and stabilizers. A *set of representatives* of the G-orbits of X is a subset $\mathcal{R}$ of X such that $\mathcal{R}$ contains precisely one element from each G-orbit of X.

11.10 Theorem (Burnside's orbit equation) *Assume that X is a G-set.*

(a) *If G acts transitively on X and $x \in X$ then* $[G : \mathrm{stab}_G(x)] = |X|$.

(b) *If $\mathcal{R} \subseteq X$ is a set of representatives of the G-orbits of X then*

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

Proof (a) Set $H := \mathrm{stab}_G(x)$ and consider the function $f\colon G/H \to X$ defined by $gH \mapsto g * x$. This function is well-defined, since if $gH = g'H$ then there exists $h \in H$ such that $g' = gh$ and we obtain $g' * x = (gh) * x = g * (h * x) = g * x$. It is surjective, since G acts transitively on X: For any $y \in X$ there exists $g \in G$ such that $y = g * x = f(gH)$. The function f is also injective: Assume that $f(gH) = f(g'H)$ for $g, g' \in G$. Then $g * x = g' * x$, which implies $x = g^{-1} * (g' * x) = (g^{-1}g') * x$. This further implies $g^{-1}g' \in \mathrm{stab}_G(x) = H$ and $gH = g'H$. Altogether, we have proved that f is bijective and the result follows.

(b) We know that X is the disjoint union of its G-orbits, which implies $|X| = \sum_{x \in \mathcal{R}} |O_x|$. By Part (a), and since O_x is a transitive G-set containing x, we obtain $|O_x| = [G : \mathrm{stab}_G(x)]$. Now the result follows. □

> Assume that G is finite. From the proof of Burnside's orbit equation we see that $|O_x| = [G : \mathrm{stab}_G(x)]$, for every element $x \in X$. This implies $|G| = |O_x| \cdot |\mathrm{stab}_G(x)|$. Therefore, the *orbit length* $|O_x|$ divides $|G|$.

11.11 Definition Let p be a prime. A *p-group* is a finite group G whose order is a power of p: $|G| = p^a$ for some $a \in \mathbb{N}_0$. Note that every subgroup and every factor group of a p-group G is again a p-group and that every element of G has an order of the form p^b with $0 \leqslant b \leqslant a$.

11.12 Corollary *Let G be a p-group and let X be a finite G-set. Then*

$$|X^G| \equiv |X| \mod p\,.$$

Proof Let $\mathcal{R} \subseteq X$ be a set of representatives of the G-orbits of X. By Burnside's orbit equation we have

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

If $x \in \mathcal{R}$ satisfies $x \in X^G$ then $\mathrm{stab}_G(x) = G$, $O_x = \{x\}$ and the corresponding summand $[G : \mathrm{stab}_G(x)]$ is equal to 1. On the other hand if $x \in \mathcal{R}$ satisfies $x \notin X^G$ then $\mathrm{stab}_G(x) < G$, and the corresponding summand $[G : \mathrm{stab}_G(x)]$ is a power of p which is greater than 1. In this case we have $[G : \mathrm{stab}_G(x)] \equiv 0 \mod p$. Altogether we obtain

$$|X| = \sum_{x \in \mathcal{R}} [G : \mathrm{stab}_G(x)] \equiv \sum_{\substack{x \in \mathcal{R} \\ x \in X^G}} 1 = \sum_{x \in X^G} 1 = |X^G|$$

and the theorem is proven. □

11.13 Remark/Definition (Conjugation) Let G be a group and let $a \in G$. The function

$$c_a \colon G \to G\,, \quad x \mapsto axa^{-1}\,,$$

is called *conjugation with* a. It is a homomorphism, since $c_a(x)c_a(y) = axa^{-1}aya^{-1} = axya^{-1} = c_a(xy)$, for all $x, y \in G$. Moreover, for $a, b, x \in G$, one has $c_a(c_b(x)) = c_a(bxb^{-1}) = c_a(bxb^{-1}) = abxb^{-1}a^{-1} = abx(ab)^{-1} = c_{ab}(x)$. Thus,

$$c_a \circ c_b = c_{ab}\,. \tag{11.13.a}$$

Note also that $c_1(x) = x$ so that

$$c_1 = \mathrm{id}_G\,. \tag{11.13.b}$$

This implies that c_a is an isomorphism for all $a \in G$ with inverse $c_{a^{-1}}$, since $c_a \circ c_{a^{-1}} = \mathrm{id}_G = c_{a^{-1}} \circ c_a$ by Equations (11.13.a) and (11.13.b).

An isomorphism $f \colon G \to G$ is also called an *automorphism* of G. The set $\mathrm{Aut}(G)$ of automorphisms of G is a group under composition, the *automorphism group* of G. Note that $\mathrm{Aut}(G)$ is a subgroup of $\mathrm{Sym}(G)$. An automorphism f of G is called *inner* if $f = c_a$ for some $a \in G$. By Equation (11.13.a), the function

$$c \colon G \to \mathrm{Aut}(G)\,, \quad a \mapsto c_a\,,$$

is a homomorphim. Its kernel is equal to $Z(G)$ and its image is equal to the set $\mathrm{Inn}(G)$ of inner automorphims of G. In particular, $\mathrm{Inn}(G)$ is a subgroup of $\mathrm{Aut}(G)$, called the *inner automorphism group* of G. By the 1st Isomorphism Theorem we have

$$\mathrm{Inn}(G) \cong G/Z(G)\,.$$

It is easy to verify that, for $f \in \mathrm{Aut}(G)$ and $a \in G$, one has

$$f \circ c_a \circ f^{-1} = c_{f(a)}\,.$$

This shows that $\mathrm{Inn}(G)$ is a normal subgroup of $\mathrm{Aut}(G)$. The factor group $\mathrm{Aut}(G)/\mathrm{Inn}(G)$ is denoted by $\mathrm{Out}(G)$ and it is called the *outer automorphism group* of G.

11.14 Examples Let G be a group.

(a) G acts on itself, i.e., on $X = G$, by conjugation: $a * x := c_a(x) = axa^{-1}$ for $a \in G$ and $x \in G$. In fact, $1*x = c_1(x) = x$, and $a*(b*x) = c_a(c_b(x)) = (c_a \circ c_b)(x) = c_{ab}(x) = (ab)*x$ for all $x, a, b \in G$. The orbits under this action are called the *conjugacy classes* of G, and two elements x and y of G are called *conjugate* if they belong to the same orbit, i.e., if there exists $a \in G$ such that $y = axa^{-1}$. Under this action we have $\mathrm{stab}_G(x) = \{a \in G \mid axa^{-1} = x\} = C_G(x)$. The fixed points under this action are precisely the elements of $Z(G)$.

(b) G also acts by conjugation on the set $\mathcal{S}(G)$ of subgroups of G: $a * H := c_a(H) = aHa^{-1}$. In fact, we already observed in Example 11.8(b) that aHa^{-1} is again a subgroup of G. Moreover, $1 * H = c_1(H) = H$ and $a * (b * H) = c_a(c_b(H)) = abHb^{-1}a^{-1} = (ab) * H$. The orbits under the conjugation action are called the *conjugacy classes of subgroups* of G and two subgroups H and K of G are called *conjugate* in G if they belong to the same orbit, i.e., if there exists $a \in G$ such that $H = aKa^{-1}$. For $H \leqslant G$ we have $\mathrm{stab}_G(H) = \{a \in G \mid aHa^{-1} = H\} = N_G(H)$. Moreover, the set of fixed points, $\mathcal{S}(G)^G$, consists precisely of the normal subgroups of G.

(c) Let $G = \mathrm{Sym}(3)$. Then the conjugacy classes of elements are given by

$$\{1_G\}\,,\ \{(1,2),(2,3),(1,3)\}\,,\ \{(1,2,3),(1,3,2)\}$$

as a quick computation shows. In fact, 1_G is not conjugate to any other element. To compute the conjugacy class of $(1,2)$, note that $c_{(2,3)}((1,2)) = (1,3)$ and $c_{(1,3)}((1,2)) = (2,3)$, showing that the conjugacy class of $(1,2)$ has at least 3 elements. On the other hand, $\langle(1,2)\rangle \leqslant C_G((1,2))$, showing that $C_G(x)$ has at least 2 elements. By Burnside's orbit equation, the conjugacy class of $(1,2)$ has $|G|/|C_G(x)| \leqslant 3$ elements. Thus, we have found the conjugacy class of $(1,2)$. To compute the conjugacy class of $(1,2,3)$, note that $C_G((1,2,3))$ contains at least the 3 elements in $\langle(1,2,3)\rangle$. Thus, by Burnside orbit equation, the conjugacy class of $(1,2,3)$ has at most 2 elements. On the other hand $c_{(1,2)}((1,2,3)) = (1,2,3)$ and therefore we have computed the conjugacy class of $(1,2,3)$.

Next we determine the conjugacy classes of subgroups of $G = \mathrm{Sym}(3)$. We already know that

$$\mathcal{S}(G) = \{\{1_G\}, \langle(1,2)\rangle, \langle(2,3)\rangle, \langle(1,3)\rangle, \langle(1,2,3)\rangle, G\}\,.$$

Since $\{1_G\}$, G, and $\langle(1,2,3)\rangle$ are normal in G (the latter because it has index 2 in G), they are alone in their respective conjugacy class. Moreover, by the computations above we also see that the three subgroups $\langle(1,2)\rangle$, $\langle(2,3)\rangle$, and $\langle(1,3)\rangle$ are conjugate in G. Thus the conjugacy classes of subgroups of G are

$$\{\{1_G\}\}\,,\quad \{\langle(1,2)\rangle, \langle(2,3)\rangle, \langle(1,3)\rangle\}\,,\quad \{\langle(1,2,3)\rangle\}\,,\quad \{G\}\,.$$

11.15 Theorem *Let G be a non-trivial p-group for a prime p. Then $Z(G) > \{1\}$.*

Proof We use the action of G on itself, i.e., on $X = G$, by conjugation (as in Example 11.14(a)) and apply Corollary 11.12. Note that $X^G = Z(G)$. Thus, we obtain $|Z(G)| \equiv |X| = |G| \equiv 0 \mod p$. This implies that p divides $|Z(G)|$ and therefore $|Z(G)| \geqslant p$. □

11.16 Lemma *If G is a group such that $G/Z(G)$ is cyclic then G is abelian.*

Proof Since $G/Z(G)$ is cyclic, there exists $x \in G$ such that $\langle xZ(G)\rangle = G/Z(G)$. If $g \in G$ is an arbitrary element then $gZ(G) = (xZ(G))^i = x^iZ(G)$ for some $i \in \mathbb{Z}$. This implies that

$g = x^i z$ for some $i \in \mathbb{Z}$ and some $z \in Z(G)$. If also h is an element of G then for the same reason it can be written as $h = x^j y$ with $j \in \mathbb{Z}$ and $y \in Z(G)$. Altogether we obtain $gh = x^i z x^j y = x^i x^j z y = x^{i+j} yz$ and $hg = x^j y x^i z = x^j x^i yz = x^{i+j} yz$. Therefore, $gh = hg$ for all $g, h \in G$ and G is abelian. □

11.17 Corollary *Assume that p is a prime and that G is a group of order p^2. Then G is abelian.*

Proof By Theorem 11.15 we have $Z(G) > \{1\}$. This implies that $|Z(G)| = p$ or $|Z(G)| = p^2$. But then $G/Z(G)$ has order p or 1. In either case, $G/Z(G)$ is cyclic (by Corollary 8.12), and Lemma 11.16 implies that G is abelian. □

11.18 Theorem (Cauchy's Theorem) *Let G be a finite group and let p be a prime which divides $|G|$. Then G has an element of order p and a subgroup of order p.*

Proof It suffices to show that G has an element of order p. Then the subgroup generated by this element has order p as well. Consider the set

$$X := \{(x_1, \ldots, x_p) \in G \times \cdots \times G \mid x_1 x_2 \cdots x_p = 1\}.$$

The group $A := (\mathbb{Z}_p, +_p)$ acts on X by

$$i * (x_1, \ldots, x_p) := (x_{i+1}, \ldots, x_p, x_1, \ldots, x_i).$$

In fact, the last element is in X, since

$$\begin{aligned} x_{i+1} \cdots x_p x_1 \cdots x_i &= (x_1 \cdots x_i)^{-1} (x_1 \cdots x_i x_{i+1} \cdots x_p)(x_1 \cdots x_i) \\ &= (x_1 \cdots x_i)^{-1} 1_G (x_1 \cdots x_i) = 1. \end{aligned}$$

It is also easy to verify the two axioms of group actions. Now Corollary 11.12 implies that $|X^A| \equiv |X| \mod p$. But $|X| = |G|^{p-1} \equiv 0 \mod p$ and $X^A = \{(x, x, \ldots, x) \mid x \in G \text{ and } x^p = 1\}$. Thus, $|X^A|$ is equal to the number of elements $x \in G$ with $x^p = 1$. Since $x = 1$ has this property, this number is at least 1. On the other hand, by the above, this number is also divisible by p. Therefore, there exists an element $x \neq 1$ such that $x^p = 1$. This implies that $o(x) = p$. □

Exercises for §11

1. Let X be a G-set via $*$.

(a) Show that $\mathrm{stab}_G(x) := \{g \in G \mid g * x = x\}$, the stabilizer of x in G, is a subgroup of G.

(b) Show that for $g \in G$ and $x \in X$ one has $\mathrm{stab}_G(g * x) = g\,\mathrm{stab}_G(x)g^{-1}$.

(c) Let $\rho\colon G \to \mathrm{Sym}(X)$ denote the permutation representation of the G-set X. Show that $\ker(\rho) = \bigcap_{x\in X} \mathrm{stab}_G(x)$.

(d) Show that for every $x \in X$ one has: $x \in X^G \iff \mathrm{stab}_G(x) = G$.

2. Let $H \leqslant G$ and set $C := \mathrm{core}_G(H) = \bigcap_{a\in G} aHa^{-1}$.

(a) Show that C is normal in G and $C \leqslant H$.

(b) Assume that also $N \trianglelefteq G$ and $N \leqslant H$. Show that $N \leqslant C$. (In other words, $\mathrm{core}_G(H)$ is the largest normal subgroup of G that is contained in H).

3. Show that $\mathrm{Inn}(G)$ is normal in $\mathrm{Aut}(G)$.

4. Let G be a non-trivial p-group and let N be a non-trivial normal subgroup of G. Show that $|N \cap Z(G)| > 1$. (Hint: Show that G acts on N via conjugation and use the congruence corollary to Burnside's orbit equation.)

5. (a) Compute the conjugacy classes of elements of $\mathrm{Alt}(4)$.

(b) Compute the conjugacy classes of subgroups of $\mathrm{Alt}(4)$.

6. Let $n \in \mathbb{N}$. The *cycle type* of a permutation $\sigma \in \mathrm{Sym}(n)$ is defined as follows: Write $\sigma = \gamma_1 \cdots \gamma_l$ with disjoint cycles γ_i, including the cycles of length 1 (so that every element from $\{1, \ldots, n\}$ occurs in precisely one of the cycles γ_i) and assume that the elements γ_i are already ordered according to their cycle lengths k_i, i.e., $k_1 \geqslant k_2 \geqslant \cdots \geqslant k_l$ and $k_1 + \cdots + k_l = n$. For instance, $(1,3,7)(2,8)(4,6)(5) \in \mathrm{Sym}(8)$ has cycle type $(3,2,2,1)$.

(a) Show that two permutations in $\mathrm{Sym}(n)$ are conjugate if and only if they have the same cycle type.

(b) How may conjugacy classes are there in $\mathrm{Sym}(5)$? What are their sizes?

7. The goal of this problems is to show that $\mathrm{Alt}(5)$ is a simple group. This is done in four steps:

(a) Show that $\mathrm{Alt}(5)$ has 24 elements of cycle type (5), 20 elements of cycle type $(3,1,1)$, 15 elements of cycle type $(2,2,1)$, and 1 element of cycle type $(1,1,1,1,1)$. (For instance, the elements $(1,2,3,4,5)$, $(1,2,3)$, $(1,2)(3,4)$ and id have these cycle types.)

(b) Show that the 20 3-cycles form a conjugacy class and that the 15 double transpositions form a conjugacy class in Alt(5). (Hint: Any two 3-cycles π_1 and π_2 are conjugate by an element $\sigma \in \mathrm{Sym}(5)$, by Exercise 6. If σ happens to be in Alt(5) you are done, if not, multiply σ by an appropriate odd permutation τ such that $\tau\pi_1\tau^{-1} = \pi_1$.)

(c) Show that the 24 5-cycles in Alt(5) form 2 conjugacy classes, each of size 12. (Hint: First show that for every 5-cycle σ one has $|C_{\mathrm{Sym}(5)}(\sigma)| = 5$ (use Exercise 6 and the orbit equation) and conclude that $C_{\mathrm{Sym}(5)}(\sigma) = \langle\sigma\rangle$. From there conclude that $C_{\mathrm{Alt}(5)}(\sigma) = \langle\sigma\rangle$ and that the Alt(5)-conjugacy class of σ has size 12.)

(d) Assume that G is a group of order 60 and that its conjugacy classes have size 1, 12, 12, 15 and 20. Show that G is a simple group. (Hint: Use that every normal subgroup is a union of conjugacy classes of elements of G.)

12 The Sylow Theorems

In this section we will apply the notion of group actions to prove the Sylow Theorems. By Lagrange, we know that if H is a subgroup of a finite group G then $|H|$ divides $|G|$. One can ask if a kind of converse is true: if G is a finite group and d is a divisor of $|G|$, does there always exist a subgroup H of G with $|H| = d$. The answer in general is "no". For instance, we have seen in a homework problem that Alt(4), a group of order 12, does not have a subgroup of order 6. However, for certain types of divisors d of $|G|$, the answer is always "yes". For instance if d is a prime (see Cauchy's Theorem). Part of the content of the Sylow Theorems is that if d is a prime power, then the answer is always "yes". The Sylow Theorems shed much more light on such p-subgroups than just saying that they exist.

Throughout this section p denotes a prime number.

12.1 Remark Assume that the group G acts on the set X via $*\colon G\times X \to X$. If H is a subgroup of G, one can restrict this function to the subset $H \times X$ to obtain a function $*\colon H \times X \to X$. This function satisfies clearly the axioms of an action of H on X. This action is called the *restriction to H* of the action of G on X. For every $x \in X$ one has $\mathrm{stab}_H(x) = \mathrm{stab}_G(x) \cap H$. Every G-orbit decomposes into a union of H-orbits.

12.2 Lemma *Let G be a finite group and let P be a p-subgroup of G, i.e., a subgroup of G which is a p-group. Then*

$$[N_G(P) : P] \equiv [G : P] \mod p\,.$$

Proof Consider the action of G on $X = G/P$ by left multiplication: $a * gP = agP$. We restrict this action to an action of P on G/P. For this action we have $(G/P)^P = N_G(P)/P$. In fact, for $gP \in G/P$ one has

$$\begin{aligned} gP \in (G/P)^P &\iff agP = gP \text{ for all } a \in P \iff g^{-1}ag \in P \text{ for all } a \in P \\ &\iff a \in gPg^{-1} \text{ for all } a \in P \iff P \leqslant gPg^{-1} \iff P = gPg^{-1} \\ &\iff g \in N_G(P) \iff gP \in N_G(P)/P\,. \end{aligned}$$

Now, Corollary 11.12 implies the result. □

12.3 Corollary *Let G be a finite group and let P be a p-subgroup of G such that p divides $[G : P]$. Then p divides $[N_G(P) : P]$.*

Proof This follows immediately from Lemma 12.2. □

12.4 Theorem (Sylow's First Theorem) *Let G be a finite group of order n and let p be a prime. Write $n = p^a m$ with $a \in \mathbb{N}_0$ and $m \in \mathbb{N}$ such that p does not divide m.*

(a) *If P is a subgroup of G of order p^b with $0 \leqslant b < a$ then there exists a subgroup $\tilde{P}$ of G of order p^{b+1} such that $P \triangleleft \tilde{P}$.*

(b) *For every $b \in \{0, \ldots, a\}$ there exists a subgroup P of G with $|P| = p^b$.*

Proof (a) Assume that P is a subgroup of G of order p^b with $1 \leqslant b < a$. Then p divides $[G : P]$ and, by Corollary 12.3, p also divides $[N_G(P) : P] = |N_G(P)/P|$. By Cauchy's Theorem, the group $N_G(P)/P$ has a subgroup of order p. By the Correspondence Theorem this subgroup must be of the form $\tilde{P}/P$ with $P \leqslant \tilde{P} \leqslant N_G(P)$. This implies that $P \trianglelefteq \tilde{P}$ and that $|\tilde{P}| = |P| \cdot |\tilde{P}/P| = p^b \cdot p = p^{b+1}$ as desired.

(b) This follows immediately from Part (a) by induction on b. □

12.5 Definition Let G be a group of order n and let p be a prime. Write $n = p^a m$ with $a \in \mathbb{N}_0$ and $m \in \mathbb{N}$ such that p does not divide m. Every subgroup of G of order p^a is called a *Sylow p-subgroup* of G. The set of Sylow p-subgroups of G is denoted by $\mathrm{Syl}_p(G)$. By the First Sylow Theorem, the set $\mathrm{Syl}_p(G)$ is not empty, i.e., G has at least one Sylow p-subgroup. Note that G acts on $\mathrm{Syl}_p(G)$ by conjugation. In fact, if $S \in \mathrm{Syl}_p(G)$ and $g \in G$ then $|gSg^{-1}| = |S|$ and therefore $gSg^{-1} \in \mathrm{Syl}_p(G)$.

Note: If $a = 0$, i.e., if p does not divide $|G|$, then $\{1_G\} \in \mathrm{Syl}_p(G)$ and the trivial subgroup is the only Sylow p-subgroup of G.

For instance, for $G = \mathrm{Sym}(3)$ we have

$$\begin{aligned}
\mathrm{Syl}_2(G) &= \{\langle(1,2)\rangle, \langle(2,3)\rangle, \langle(1,3)\rangle\}, \\
\mathrm{Syl}_3(G) &= \{\langle(1,2,3)\rangle\}, \\
\mathrm{Syl}_p(G) &= \{\ \{1_G\}\ \} \quad \text{if } p \geqslant 5.
\end{aligned}$$

12.6 Theorem (Sylow's Second Theorem) *Let G be a finite group.*

(a) *Every p-subgroup of G is contained in a Sylow p-subgroup of G.*

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

Proof (a) This follows immediately by repeated application of Part (a) of Sylow's First Theorem.

(b) Assume that $S_1, S_2 \in \mathrm{Syl}_p(G)$. Consider the action of S_2 on $X = G/S_1$ by left multiplication. By Corollary 11.12 we have $|X^{S_2}| \equiv |X| = [G : S_1] \mod p$. Since $[G : S_1]$ is not divisible by p, the set X^{S_2} is not empty. So let $gS_1 \in X^{S_2}$. Then $agS_1 = gS_1$ for all $a \in S_2$. This implies that $g^{-1}agS_1 = S_1$ and that $g^{-1}ag \in S_1$ for all $a \in S_2$. Consequently, $a \in gS_1g^{-1}$

for all $a \in S_2$, i.e., $S_2 \leqslant gS_1g^{-1}$. But S_2 and gS_1g^{-1} have the same order. This implies that $S_2 = gS_1g^{-1}$ so that S_1 and S_2 are conjugate subgroups of G. □

Part (b) of Sylow's Second Theorem implies that any two Sylow p-subgroups of a finite group G are isomorphic. Sylow's Third Theorem will say something about the number $|\mathrm{Syl}_p(G)|$.

12.7 Theorem (Sylow's Third Theorem) *Let G be a finite group of order n and let p be a prime. Write $n = p^a m$ with $a \in \mathbb{N}_0$ and $m \in \mathbb{N}$ such that p does not divide m. Then the number $n_p(G) = |\mathrm{Syl}_p(G)|$ of Sylow p-subgroups of G satisfies:*

$$n_p(G) \equiv 1 \mod p \qquad \text{and} \qquad n_p(G) \mid m.$$

Proof Let $S \in \mathrm{Syl}_p(G)$.

By Sylow's Second Theorem, the conjugation action of G on $\mathrm{Syl}_p(G)$ is transitive. This implies that $n_p(G) = |\mathrm{Syl}_p(G)| = [G : \mathrm{stab}_G(S)] = [G : N_G(S)]$. But $[G : N_G(S)] \cdot [N_G(S) : S] = [G : S] = m$. Thus, $n_p(G)$ divides m.

In order to show that $n_p(G) \equiv 1 \mod p$, we consider the conjugation action of S on $X = \mathrm{Syl}_p(G)$. By Corollary 11.12 we have $n_p(G) = |X| \equiv |X^S| \mod p$. So it suffices to show that $|X^S| = \{S\}$. So let $T \in \mathrm{Syl}_p(G)^S$. Then $aTa^{-1} = T$ for all $a \in S$. This implies that $S \leqslant N_G(T)$, and by Proposition 10.7(b) the subset ST of G is a subgroup of G. By Proposition 10.5 we have $|ST| = |S| \cdot |T|/|S \cap T|$. This implies that $|ST|$ is a power of p. Since $S \leqslant ST \leqslant G$, p^a divides $|ST|$ and $|ST|$ divides $p^a m$. This implies $|ST| = p^a$ and $S = ST$. Thus, $T \leqslant S$. But since $|S| = |T|$, we obtain $S = T$. This shows that $\mathrm{Syl}_p(G)^S = \{S\}$ and the congruence is proved. □

12.8 Remark Let G be a finite group and let S be a Sylow p-subgroup of G. Then

$$\mathrm{Syl}_p(G) = \{S\} \iff S \trianglelefteq G\,.$$

In fact, if S is the only Sylow p-subgroup of G then $aSa^{-1} = S$ for all $a \in G$, since $|aSa^{-1}| = |S|$. Thus, S is normal in G. Conversely, if S is normal in G then, by Sylow's Second Theorem, S is the only Sylow p-subgroup of G.

12.9 Example Let G be a group of order 100 and let S be a Sylow 5-subgroup of G. Then S has order 25. We will show that S is normal. By the above remark it suffices to show that $n_5(G) = 1$. By Sylow's Third Theorem we know that $n_5(G)$ divides 4 and that $n_5(G) \equiv 1 \mod p$. This implies $n_5(G) = 1$ and $S \triangleleft G$. Since S is a group of order 5^2 and G/S is a group of order 2^2, both groups are abelian by Corollary 11.17. Thus, G is "composed" of the two abelian group S and G/S. Thus, with the vocabulary from the next section, G is *solvable*.

Exercises for §12

1. Let p be a prime, let P be a p-group and let $Q < P$.

(a) Show that $N_P(Q) > Q$.

(b) Show that if $[P : Q] = p$ then $Q \lhd P$.

2. Let G be a group of order 1000. Show that G is not simple.

3. (a) For $G = \mathrm{Alt}(4)$ and $p = 2, 3$, determine a Sylow p-subgroup S of G, the normalizer of S in G and the number $|\mathrm{Syl}_p(G)|$.

(b) For $G = \mathrm{Alt}(5)$ and $p = 2, 3, 5$, do the same as in Part (a).

4. Assume that G is a finite group of order $n = p_1 \cdots p_r$ for pairwise distinct prime numbers. Assume further that, for each prime p_i, G has only one Sylow p_i-subgroup S_i. Show that G is cyclic.
(Hint: Let a_i be a generator of S_i, and set $a := a_1 \cdots a_r$. First show that $a_i a_j = a_j a_i$ for all $i, j \in \{1, \ldots, r\}$. Then show that $G = \langle a \rangle$ by showing that $S_i \leqslant \langle a \rangle$ for every $i = 1, \ldots, r$.)

5. (a) Show that every group of order 15 is cyclic.

(b) Show that every group of order 1001 is cyclic.

6. (a) Find a Sylow 2-subgroup of Sym(4). How many Sylow 2-subgroups are there?

(b) Find a Sylow 2-subgroup of Sym(5). How many Sylow 2-subgroups are there?
(Hint: Consider the conjugation action of Sym(5) on its Sylow 2-subgroups. Show that $\mathrm{Syl}_2(\mathrm{Sym}(4)) \subseteq \mathrm{Syl}_2(\mathrm{Sym}(5))$, choose $S \in \mathrm{Syl}_2(\mathrm{Sym}(4))$, and show that $N_{\mathrm{Sym}(5)}(S) \leqslant \mathrm{Sym}(4)$. Then use Part (a) and the orbit equation.)

13 Solvable groups

In this section we introduce the notion of a solvable group and show, often by applying the Sylow Theorems, that groups of certain orders are always solvable. Vaguely speaking, solvable groups are groups that are built from abelian groups. For this reason their structure is less complicated than that of arbitrary groups. The class of solvable groups contains the class of abelian groups and also the class of p-groups. The class of solvable groups has also the convenient property that it is closed under taking subgroups and forming factor groups. The name "solvable" has to do with a connection to solving polynomial equations. This connection is explained using Galois Theory (but not in these notes).

13.1 Definition Let G be a group.

(a) A *subnormal series* of G is a finite sequence of subgroups of the form

$$1 = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_n = G\,,$$

i.e., every subgroup is normal in the following one. It is not required that G_i is normal in G. The factor groups G_i/G_{i-1}, $i = 1, \ldots, n$, are called the *factors* of the subnormal series.

(b) The group G is called *solvable* if it has a subnormal series with abelian factors.

> This definition is motivated by the following. Let $f(x)$ denote a polynomial of degree n with coefficients in $\mathbb{Q}$. Galois associated (through a complex process) to this polynomial a finite group $G_{f(x)}$, called the Galois group of the polynomial. This group is isomorphic to a subgroup of $\mathrm{Sym}(n)$. In fact, if one picks a "random" polynomial $f(x)$ of degree n, chances are very high that $G_{f(x)}$ is isomorphic to $\mathrm{Sym}(n)$. This was probably the first occurrence of the notion of a *group*. Abel proved that the solutions of the equation $f(x) = 0$ can be expressed in terms of the coefficients of $f(x)$ and the usual operations $+$, $-$, $\cdot$, $/$, together with higher roots, if and only if $G_{f(x)}$ is solvable. It was known that such formulas existed for polynomials of degrees 1, 2, 3, and 4. For instance, the solutions of the equation $ax^2 + bx + c = 0$ are $(-b \pm \sqrt{b^2 - 4ac})/2a$. Abel's Theorem therefore explains why nobody was able to find a general formula for solutions of polynomial equations of degree 5 and higher: The groups $\mathrm{Sym}(n)$, for $n \geqslant 5$, are not solvable (see Exercise 5) while $\mathrm{Sym}(n)$, for $n \leqslant 4$, and its subgroups are solvable (as we will see later in this section).

13.2 Remark (a) If G is an abelian group then G is solvable, because the sequence $\{1_G\} \trianglelefteq G$ is a subnormal series with abelian factor.

(b) If G is a p-group then Part (a) of Sylow's First Theorem guarantees a subnormal series

$$\{1\} = G_0 \triangleleft G_1 \triangleleft \cdots \triangleleft G_n = G$$

with factors G_i/G_{i-1} of order p. for $i = 1, \ldots, n$. Since every group of order p is cyclic (and therefore abelian), we have shown that every p-group is solvable.

13.3 Examples (a) Sym(3) is solvable, since $\{\mathrm{id}\} \triangleleft \langle (1,2,3) \rangle \triangleleft \mathrm{Sym}(3)$ is a subnormal series with abelian factors.

(b) Alt(4) is solvable, since $\{\mathrm{id}\} \triangleleft V_4 \triangleleft \mathrm{Alt}(4)$ is a subnormal series with abelian factors, where $V_4 = \langle (1,2)(3,4), (1,3)(2,4) \rangle$.

(c) Sym(4) is solvable, since $\{\mathrm{id}\} \triangleleft V_4 \triangleleft \mathrm{Alt}(4) \triangleleft \mathrm{Sym}(4)$ is a subnormal series with abelian factors.

(d) Alt(5) is not solvable, because Alt(5) is simple (see Exercise 11.7) and non-abelian.

13.4 Proposition *Every group G of order pq, where p and q are primes, is solvable.*

Proof If $p = q$ then G is a p-group and solvable by Remark 13.2(b). So we can assume from now on, without loss of generality, that $p < q$. By Sylow's Third Theorem we know that $n_q(G)$ divides p and that $n_q(G) \equiv 1 \mod q$. This implies that $n_q(G) = 1$ and that G has a normal Sylow q-subgroup S. This leads to a subnormal series $\{1_G\} \triangleleft S \triangleleft G$ with factors of order q and of order p. This implies that the factors are abelian, and that G is solvable. □

13.5 Proposition *Let p and q be primes and let G be a group of order p^2q. Then G is solvable.*

Proof If $p = q$ then G is a p-group and we are done by Remark 13.2(b). So we assume from now on that $p \neq q$. By Sylow's Third Theorem we have $n_p(G) \in \{1, q\}$ and $n_q(G) \in \{1, p, p^2\}$. If $n_p(G) = 1$ or $n_q(G) = 1$ we are done, since then we obtain a subnormal series with factor groups that are of order p^2 and order q and therefore abelian.

So we assume from now on that $n_p(G) = q$ and that $n_q(G) \in \{p, p^2\}$. We will see that this case cannot occur by deriving a contradiction. By Sylow's Third Theorem we have $q = n_p(G) \equiv 1 \mod p$. This implies that $p \leqslant q - 1 < q$ and then that $p \not\equiv 1 \mod q$. Thus, again by Sylow's Third Theorem, $n_q(G) \neq p$, and therefore we have $n_q(G) = p^2$. This means G has p^2 different subgroups of order q. Each of them has precisely $q - 1$ elements of order q, and each element of order q belongs to precisely one subgroup of order q. Thus, the number of elements of G of order q is equal to $p^2(q-1)$, and G has at most $p^2q - p^2(q-1) = p^2$ elements whose order divides p^2. Now let S be a Sylow p-subgroup of G. Then S has p^2 elements whose order divides p^2. If there existed two different Sylow p-subgroups of G, say $S \neq T$, then

$|S \cap T| = |S| + |T| - |S \cap T| \geqslant p^2 + p^2 - p > p^2$ and G would contain more than p^2 elements of order dividing p^2. Thus, G has only one Sylow p-subgroup. This is a contradiction to our assumption that $n_p(G) = q$. □

13.6 Theorem *Let G be a group.*

(a) *If G is solvable and H is a subgroup of G then H is solvable.*

(b) *If G is solvable and N is a normal subgroup of G then G/N is solvable.*

(c) *If N is a normal subgroup of G such that N and G/N are solvable, then G is solvable.*

Proof (a) Let

$$1 = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_n = G$$

be a subnormal series of G with abelian factors. We claim that then

$$1 = G_0 \cap H \trianglelefteq G_1 \cap H \trianglelefteq \cdots \trianglelefteq G_n \cap H = H$$

is again a subnormal series with abelian factors. We set $H_i := G_i \cap H$ for $i = 0, \ldots, n$. First we show that H_{i-1} is normal in H_i for $i = 1, \ldots, n$. This follows from the Second Isomorphism Theorem applied to the group G_i and the subgroups G_{i-1} and $G_i \cap H$. In fact, G_{i-1} is normal in G_i and therefore $H_{i-1} = G_{i-1} \cap (G_i \cap H)$ is normal in $G_i \cap H = H_i$. Next we show that H_i/H_{i-1} is abelian. Again by the Second Isomorphism Theorem, there exists an isomorphism

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

But the latter group is a subgroup of the abelian group G_i/G_{i-1} and therefore abelian. This shows that also H_i/H_{i-1} is abelian.

(b) Again, let

$$1 = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_n = G$$

be a subnormal series of G with abelian factors. We claim that

$$1 = G_0N/N \trianglelefteq G_1N/N \trianglelefteq \cdots \trianglelefteq G_nN/N = G/N$$

is a subnormal series of G/N with abelian factors. First of all, G_iN is a subgroup of G for all $i = 0, \ldots, n$, since N is normal in G. Secondly, G_iN/N is a subgroup of G/N for all $i = 0, \ldots, n$, by the Correspondence Theorem. Also, clearly $G_{i-1}N/N$ is a subgroup of G_iN/N for all $i = 1, \ldots, n$. Next we show that $G_{i-1}N/N$ is normal in G_iN/N for all $i = 1, \ldots, n$. By the Correspondence Theorem applied to the group G_iN and the normal subgroup N, it suffices to show that $G_{i-1}N$ is normal in G_iN, or equivalently that $G_i \leqslant N_G(G_{i-1}N)$ and $N \leqslant N_G(G_{i-1}N)$. But, clearly $N \leqslant N_G(G_{i-1}N)$, since $N \leqslant G_{i-1}N$, and for $a \in G_i$ we have $aG_{i-1}N = G_{i-1}aN = G_{i-1}Na$, since N is normal in G and G_{i-1} is normal in G_i. Finally, we

need to show that the factors $(G_iN/N)/(G_{i-1}N/N)$ are abelian. By the Third Isomorphism Theorem, we have

$$(G_iN/N)/(G_{i-1}N/N) \cong (G_iN)/(G_{i-1}N)\,.$$

By the Second Isomorphism Theorem applied to the group G_iN and the normal subgroup $G_{i-1}N$ and the subgroup G_i we obtain further that

$$G_iN/G_{i-1}N = G_i(G_{i-1}N)/G_{i-1}N \cong G_i/(G_i \cap G_{i-1}N)\,.$$

And finally, using again the Third Isomorphism Theorem, applied to the group G_i and the normal subgroups $G_i \cap G_{i-1}N$ and G_{i-1}, we obtain

$$G_i/(G_i \cap G_{i-1}N) \cong (G_i/G_{i-1})/((G_i \cap G_{i-1}N)/G_{i-1})\,.$$

Altogether we obtain that $(G_iN/N)/(G_{i-1}N/N)$ is isomorphic to a factor group of the abelian group G_i/G_{i-1}. Therefore, $(G_iN/N)/(G_{i-1}N/N)$ is abelian.

(c) Since N is solvable there exists a subnormal series

$$\{1_G\} = N_0 \trianglelefteq N_1 \trianglelefteq \cdots \trianglelefteq N_k = N$$

with abelian factors N_i/N_{i-1}, for $i = 1, \ldots, k$. And since G/N is solvable there exists a subnormal series

$$\{1_{G/N}\} = X_0 \trianglelefteq X_1 \trianglelefteq \cdots \trianglelefteq X_l = G/N$$

with abelian factors. By the Correspondence Theorem, there exist subgroups H_i of G with $N \leqslant H_i$, for $i = 0, \ldots, l$, such that $X_i = H_i/N$. It follows also by the Correspondence Theorem that $H_0 = N$, that $H_l = G$ and that H_{i-1} is normal in H_i (the latter follows from the Correspondence Theorem applied to the group H_i). Therefore, we obtain a subnormal series

$$\{1_G\} = N_0 \trianglelefteq N_1 \trianglelefteq \cdots \trianglelefteq N_k = N = H_0 \trianglelefteq H_1 \trianglelefteq \cdots \trianglelefteq H_l = G\,.$$

We claim that this subnormal series has abelian factors. In fact N_i/N_{i-1} (for $i = 1, \ldots, k$) is abelian by our assumption from the beginning of the proof of Part (c), and H_i/H_{i-1} (for $i = 1, \ldots, l$) is isomorphic to $(H_i/N)/(H_{i-1}/N) = X_i/X_{i-1}$ by the Third Isomorphism Theorem. But the latter groups are also abelian by our assumption. □

13.7 Example Every group G of order 36 is solvable. In fact, if $n_3(G) = 1$ then G has a normal Sylow 3-subgroup S (by Remark 12.8) and we obtain a subnormal series $\{1_G\} \triangleleft P \triangleleft G$. (The factors are abelian, because they have order p^2 for a prime p, cf. Corollary 11.17.) So assume that $n_3(G) > 1$ and let $S \neq T$ be two Sylow 3-subgroups. We claim that $P := S \cap T$ has order 3 and that P is normal in G. Once we have proved this we see from Proposition 13.5 that G/P, which has order 12, is solvable, and together with P being solvable, Theorem 13.6(c)

implies that G is solvable. Next we prove the claim. First, note that, by Proposition 10.5, we have $|ST| = |S| \cdot |T|/|S \cap T| = 81/|S \cap T|$. This implies that $|S \cap T| \neq 1$. But $S \cap T$ is a subgroup of S and not equal to S (since otherwise we obtain $S = T$). Now, by Lagrange, we obtain $|S \cap T| = 3$. Therefore, by the above equation we obtain $|ST| = 27$. Since S and T are abelian (since of order 3^2), $P = S \cap T$ is normal in S and normal in T. In other words, S and T are subgroups of $N_G(P)$. But then also the subset ST is contained in $N_G(P)$. This means that $27 \leqslant |N_G(P)|$. But, by Lagrange's Theorem, $|N_G(P)|$ is a divisor of 36. This implies that $N_G(P) = G$ and P is normal in G.

> The solvability of groups of order 36 would also follow with a shorter proof from the following proposition. However, the arguments in the above example still go through for every group of order p^2q^2 with primes $p \neq q$ (see Exercise 4), while the proposition below cannot be applied in the general case.

13.8 Proposition *Let G be a finite group and let H be a subgroup of index n in G.*

(a) *$G/\mathrm{core}_G(H)$ is isomorphic to a subgroup of $\mathrm{Sym}(n)$.*

(b) *If $n \leqslant 4$ and if $\mathrm{core}_G(H)$ is solvable then G is solvable.*

Proof (a) Consider the action of G on $X = G/H$ by left multiplication. The associated permutation representation is a homomorphism $\rho\colon G \to \mathrm{Sym}(X)$ with kernel $\mathrm{core}_G(H) = \bigcap_{a \in G} aHa^{-1}$, by Example 11.8(b). Now the First Isomorphism Theorem implies that $G/\mathrm{core}_G(H)$ is isomorphic to a subgroup of $\mathrm{Sym}(X)$ and therefore also to a subgroup of $\mathrm{Sym}(n)$, by Proposition 6.1.

(b) We know that $\mathrm{core}_H(G)$ is normal in G. Moreover, by Part (a), we know that $G/\mathrm{core}_H(G)$ is isomorphic to a subgroup of $\mathrm{Sym}(n)$ with $n \leqslant 4$. But $\mathrm{Sym}(n)$ is solvable for $n \leqslant 4$, by Examples 13.3. Theorem 13.6(a) implies that $G/\mathrm{core}_G(H)$ is solvable. Now Theorem 13.6(c) implies that G is solvable. □

13.9 Example Every group of order 48 is solvable. Since $48 = 2^4 \cdot 3$, there exists a subgroup S of order 16 by Sylow's First Theorem. The group $\mathrm{core}_G(S)$ is a subgroup of S. Therefore, it is a 2-group and is solvable. Moreover, the index of S in G is equal to 3. Now Proposition 13.8(b) applies and shows that G is solvable.

13.10 Remark (a) A famous theorem by Feit and Thompson states that every finite group of odd order is solvable. This is usually referred to as the "Odd Order Theorem". It was proved in 1963. The proof is about 250 pages long.

(b) Another famous theorem is "Burnside's p^aq^b-Theorem". It states that every group of order p^aq^b, where p and q are primes and a, b are natural numbers, is solvable. The proof of this theorem is not very long, but it uses methods from *character theory*, which arises from studying how groups can act on vector spaces.

Exercises for §13

1. Let G be a group of order 80.

(a) Show that G has a normal Sylow 5-subgroup or a normal Sylow 2-subgroup.

(b) Show that G is solvable.

2. Show that every group of order 500 is solvable.

3. Show that all groups of order smaller than 60 are solvable.

4. Show that all groups of order p^2q^2 (with primes p and q) are solvable. (Hint: Generalize the proof in Example 13.7, where $p = 2$ and $q = 3$.)

5. Let G be a finite group. Show that the following are equivalent:

(i) G is solvable.

(ii) G has a subnormal series with cyclic factors.

(iii) G has a subnormal series with cyclic factors of prime order.

(Hint: Refine a given subnormal series using the Correspondence Theorem.)

6. Show that $\mathrm{Sym}(n)$, for $n \geqslant 5$, is not solvable. (Hint: Use that $\mathrm{Alt}(5)$ is simple, see Exercise 11.7, and show that $\mathrm{Alt}(5)$ is isomorphic to a subgroup of $\mathrm{Sym}(n)$.)

7. Show that every group of order 72 is solvable. (Hint: Use the third Sylow Theorem to see that $|\mathrm{Syl}_3(G)| \in \{1, 4\}$ and treat these two cases separately.)

14 The structure of finite abelian groups

The goal of this section is to prove the following theorem about finite abelian groups. It says that there are no new surprise finite abelian groups: They are all isomorphic to direct products of cyclic groups of the form $\mathbb{Z}_{p^e}$, where p is a prime and $e \in \mathbb{N}$.

14.1 Theorem *Let G be a non-trivial finite abelian group. Then there exist unique prime powers $p_1^{e_1}, \dots, p_r^{e_r}$ ($e_i \geqslant 1$ for $i = 1, \dots, r$) such that*

$$G \cong \mathbb{Z}_{p_1^{e_1}} \times \cdots \times \mathbb{Z}_{p_r^{e_r}} .$$

The natural numbers $p_1^{e_1}, \dots, p_r^{e_r}$ are called the elementary divisors *of G.*

> In the above theorem, repetitions are allowed. For instance,
> the elementary divisors could be $4, 4, 8, 3, 9$.

14.2 Examples (a) According to the above theorem, there exist precisely 5 isomorphism classes of abelian groups of order 16, represented by the following groups:

$$\mathbb{Z}_{16}\,, \quad \mathbb{Z}_8 \times \mathbb{Z}_2\,, \quad \mathbb{Z}_4 \times \mathbb{Z}_4\,, \quad \mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_2\,, \quad \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2\,.$$

(b) The isomorphism classes of abelian groups of order $36 = 2^2 \cdot 3^2$ are represented by

$$\mathbb{Z}_4 \times \mathbb{Z}_9\,, \quad \mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_3\,, \quad \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_9\,, \quad \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3\,.$$

(c) For every prime p there exist precisely two isomorphism types of groups of order p^2, namely $\mathbb{Z}_{p^2}$ and $\mathbb{Z}_p \times \mathbb{Z}_p$. In fact, by Corollary 11.17, every group of order p^2 is abelian and Theorem 14.1 applies.

For the proof of Theorem 14.1 we need to prove a few auxiliary results.

14.3 Proposition *Let G be a non-trivial finite abelian group and let $p_1, \dots, p_s$ denote the distinct prime divisors of $|G|$. For $i = 1, \dots, s$, let P_i be the Sylow p_i-subgroup. Then the function*

$$f\colon P_1 \times \cdots \times P_s \to G\,, \quad (a_1, \dots, a_s) \mapsto a_1 \cdots a_s\,,$$

is an isomorphism.

Proof The function f is a homomorphism, since

$$\begin{aligned} f((a_1, \dots, a_s)(b_1, \dots, b_s)) &= f((a_1 b_1, \dots, a_s b_s)) = a_1 b_1 a_2 b_2 \cdots a_s b_s \\ &= a_1 \cdots a_s b_1 \cdots b_s = f((a_1, \dots, a_s)) f((b_1, \dots, b_s))\,. \end{aligned}$$

Next we show that f is surjective. For this purpose write $|G| = p_1^{e_1} \cdots p_s^{e_s}$. Then $|P_i| = p_i^{e_i}$ for all $i = 1, \dots, s$. For every $i = 1, \dots, s$, the subgroup P_i of G is contained in the image of f.

Therefore, $|\mathrm{im}(f)|$ is divisible by $p_i^{e_i}$ for all $i = 1, \ldots, s$. But this implies that $|\mathrm{im}(f)|$ is divisible by $p_1^{e_1} \cdots p_s^{e_s} = |G|$. Thus, $|G| = |\mathrm{im}(f)|$ and $\mathrm{im}(f) = G$.

Finally, since $|P_1 \times \cdots \times P_s| = p_1^{e_1} \cdots p_s^{e_s} = |G|$, the function f is also injective. □

14.4 Corollary *Let $n > 1$ be an integer and let $n = p_1^{e_1} \cdots p_r^{e_s}$ be its prime factorization. Then*

$$\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{e_1}} \times \cdots \times \mathbb{Z}_{p_s^{e_s}} .$$

Proof Since every subgroup of a cyclic group is cyclic, the Sylow p_i-subgroup P_i of $\mathbb{Z}_n$ is isomorphic to $\mathbb{Z}_{p_i^{e_i}}$ for all $i = 1, \ldots, s$. This together with Proposition 14.3 yields isomorphisms

$$\mathbb{Z}_{p_1^{e_1}} \times \cdots \times \mathbb{Z}_{p_s^{e_s}} \cong P_1 \times \cdots \times P_s \cong \mathbb{Z}_n .$$

□

14.5 Remark If $f\colon G \to H$ is an isomorphism between two finite groups and if S is a Sylow p-subgroup of G for some prime p then $f(S)$ is a Sylow p-subgroup of H (since $|G| = |H|$ and $|f(S)| = |S|$). Moreover, S is isomorphic to $f(S)$.

Proposition 14.3 and the above remark now show that, in order to prove Theorem 14.1, it suffices to prove it in the special case of a p-group. More precisely, the general existence of an isomorphism as in Theorem 14.1 follows from Proposition 14.3 and the existence statement in Theorem 14.6. And the uniqueness of the prime powers follows from the above remark together with the uniqueness statement in Theorem 14.6.

14.6 Theorem *Let p be a prime and let G be a non-trivial finite abelian p-group. Then there exist unique positive integers $e_1 \geqslant e_2 \geqslant \cdots \geqslant e_r$ such that*

$$G \cong \mathbb{Z}_{p^{e_1}} \times \cdots \times \mathbb{Z}_{p^{e_r}} . \tag{14.6.a}$$

Before we can start proving Theorem 14.6, we need one more lemma.

14.7 Lemma *Assume that G is a finite non-cyclic abelian p-group and that $a \in G$ is an element whose order is maximal among the orders of all elements of G. Then there exists $b \in G$ of order p with $\langle a \rangle \cap \langle b \rangle = \{1_G\}$.*

Proof Since G is not cyclic, the group $G/\langle a \rangle$ is not trivial. By Cauchy's Theorem, there exists an element $c\langle a \rangle \in G/\langle a \rangle$ of order p. This implies that $c^p\langle a \rangle = (c\langle a \rangle)^p = \langle a \rangle$, and therefore $c^p \in \langle a \rangle$. Thus, there exists $k \in \mathbb{Z}$ such that $c^p = a^k$. If p does not divide k, then $\gcd(k, o(a)) = 1$ and therefore $o(a^k) = o(a)$ (by Proposition 5.12). This implies that $o(c) = p \cdot o(a^k) = p \cdot o(a)$ (again by Proposition 5.12, this time applied to c and c^p), contradicting the maximality of $o(a)$

among all elements of G. Thus, p divides k and we can write $k = pl$ for some $l \in \mathbb{Z}$. Now, the element $b := c^{-1}a^l$ satisfies $b^p = c^{-p}a^k = 1$ and $b \neq 1$, since otherwise $c \in \langle a \rangle$, contradicting $o(c\langle a \rangle) = p$. Thus, b has order p. Moreover, $\langle b \rangle \cap \langle a \rangle = \{1\}$, since otherwise this intersection is a non-trivial subgroup of $\langle b \rangle$ and therefore equal to $\langle b \rangle$ (because $|\langle b \rangle| = p$), which implies $b \in \langle a \rangle$ and $c = a^l b^{-1} \in \langle a \rangle$ which we just ruled out. Now the proof is complete. □

Proof of Thm 14.6.

(a) First we prove by induction on $|G|$ that there exist positive integers $e_1 \geqslant e_2 \geqslant \cdots \geqslant e_r$ and an isomorphism as in (14.6.a).

If $|G| = p$, then $G \cong \mathbb{Z}_p$ and we are done. Now assume that $|G| > p$ and that the existence part of the statement in the theorem holds for all finite non-trivial abelian p-groups of order smaller than $|G|$. If G is cyclic, we are done. So asume that G is not cyclic. Let $a \in G$ be an element with maximal order. Among all subgroups H of G satisfying $H \cap \langle a \rangle = \{1\}$ pick one with maximal order.

We claim that $H\langle a \rangle = G$. Assume that $H\langle a \rangle$ is a proper subgroup of G. It is easy to see that the order of the element $aH \in G/H$ is equal to the order of the element $a \in G$. In fact, $(aH)^k = H$ if and only if $a^k \in H$, and this happens if and only if $a^k = 1$, since $\langle a \rangle \cap H = \{1_G\}$. But then $o(aH)$ is the maximal possible order of elements in G/H, since in general $o(gH) \leqslant o(g)$, for $g \in G$. Since $G/H > \langle a \rangle H/H = \langle aH \rangle$, this implies that G/H is not cyclic. By Lemma 14.7, there exists an element $bH \in G/H$ of order p with $bH \notin \langle aH \rangle$. Thus, b is not in H and $\langle b \rangle H > H$. But also $\langle b \rangle H \cap \langle a \rangle = \{1_G\}$. In fact, let $x \in \langle b \rangle H \cap \langle a \rangle$. Then we can write $x = b^i h = a^j$ with $i, j \in \mathbb{Z}$ and $h \in H$. This implies $(bH)^i = b^i H = a^j H \in \langle aH \rangle$. Since bH has order p and is not contained in $\langle aH \rangle$, this implies that p divides i (since otherwise $\langle bH \rangle = \langle b^i H \rangle \subseteq \langle aH \rangle$). But if p divides i then $b^i \in H$, since bH has order p. This implies that $x = a^j = b^i h \in H \cap \langle a \rangle = \{1_G\}$. Thus, we have proved that $\langle b \rangle H \cap \langle a \rangle = \{1_G\}$. But this contradicts the maximality of H with respect to $H \cap \langle a \rangle = \{1_G\}$. Therefore the claim is proved.

Now we have $\langle a \rangle H = G$ and $\langle a \rangle \cap H = \{1_G\}$. This implies that the function

$$\phi \colon \langle a \rangle \times H \to G\,, \quad (a^i, h) \mapsto a^i h\,,$$

is an isomorphism. In fact, it is easy to see that it is a homomorphism, since G is abelian. It is surjective, since $\langle a \rangle H = G$, and it is injective, since

$$|G| = |\langle a \rangle H| = \frac{|\langle a \rangle| \cdot |H|}{|\langle a \rangle \cap H|} = |\langle a \rangle| \cdot |H| = |\langle a \rangle \times H|\,.$$

By induction, there exist positive integers $e_2 \geqslant \cdots \geqslant e_r$ and an isomorphism

$$\psi \colon H \to \mathbb{Z}_{p^{e_2}} \times \cdots \times \mathbb{Z}_{p^{e_r}}\,.$$

If we denote by e_1 the positive integer with $o(a) = p^{e_1}$ then $e_1 \geqslant e_2$, since a has maximal possible order in G. Since $\mathbb{Z}_{p^{e_i}}$ and $\langle a \rangle$ are both cyclic groups of order p^{e_1}, there exists an isomorphism

$\omega\colon \langle a\rangle \to \mathbb{Z}_{p^{e_1}}$ and we obtain an isomorphism

$$\langle a\rangle \times H \cong \mathbb{Z}_{p^{e_1}} \times (\mathbb{Z}_{p^{e_2}} \times \cdots \times \mathbb{Z}_{p^{e_r}})\,, \quad (x,y) \mapsto (\omega(x), \psi(y))\,.$$

Altogether we obtain an isomorphism as in (14.6.a).

(b) Now we prove the uniqueness part of the theorem. Assume that $e_1 \geqslant e_2 \geqslant \cdots \geqslant e_r$ and $f_1 \geqslant f_2 \geqslant \cdots \geqslant f_s$ are positive integers and that

$$\mathbb{Z}_{p^{e_1}} \times \cdots \times \mathbb{Z}_{p^{e_r}} \cong \mathbb{Z}_{p^{f_1}} \times \cdots \times \mathbb{Z}_{p^{f_s}}\,.$$

We will show that $r = s$ and that $e_i = f_i$ for all $i = 1, \ldots, r$.

For every $k \in \mathbb{N}$, let $E(k)$ denote the number of elements $(a_1, \ldots, a_r) \in \mathbb{Z}_{p^{e_1}} \times \cdots \times \mathbb{Z}_{r^{e_r}}$, satisfying $p^k(a_1, \ldots, a_r) = (0, \ldots, 0)$, i.e., $E(k)$ counts the elements whose order divides p^k. Similarly, we define $F(k)$ as the number of elements $(b_1, \ldots, b_s) \in \mathbb{Z}_{p^{e_1}} \times \cdots \times \mathbb{Z}_{p^{e_s}}$, satisfying $p^k(b_1, \ldots, b_s) = (0, \ldots, 0)$. Since f is an isomorphism, we clearly have $E(k) = F(k)$, for all $k \in \mathbb{N}$. But, $p^k(a_1, \ldots, a_r) = (0, \ldots, 0)$ if and only if $p^k a_i = 0$ in $\mathbb{Z}_{p^{e_i}}$ for every $i = 1, \ldots, r$. If $e_i \geqslant k$ then $\mathbb{Z}_{p^{e_i}}$ has precisely p^k elements with this property, namely the subgroup generated by $p^{e_i - k}$. If $e_i < k$ then every element of $\mathbb{Z}_{p^{e_i}}$ has this property. Let $t := \max\{e_1, f_1\}$. Then, if we denote by m_k $(k = 1, \ldots, t)$ the number of exponents e_i with $e_i = k$, and by n_k $(k = 1, \ldots, t)$ the number of exponents f_j with $f_j = k$, we obtain

$$E(k) = p^{m_1 + 2m_2 + 3m_3 + \cdots + k(m_k + m_{k+1} + \cdots + m_t)}$$

and

$$F(k) = p^{n_1 + 2n_2 + 3n_3 + \cdots + k(n_k + n_{k+1} + \cdots + n_t)}$$

Since $F(1) = E(1)$, we obtain

$$r = m_1 + m_2 + \cdots + m_t = n_1 + n_2 + \cdots + n_t = s\,.$$

Since $F(2) = E(2)$, we obtain

$$m_1 + 2(m_2 + \cdots + m_t) = n_1 + 2(n_2 + \cdots + n_t)\,.$$

Together with the previous equation this implies $m_1 = n_1$ and $m_2 + \cdots + m_t = n_2 + \cdots + n_t$. Since $F(3) = E(3)$, we obtain

$$m_1 + 2m_2 + 3(m_3 + \cdots + m_t) = n_1 + 2n_2 + 3(n_3 + \cdots + n_t)\,.$$

Using $m_1 = n_1$ and $m_2 + \cdots + m_t = n_2 + \cdots + n_t$, we obtain $m_2 = n_2$ and $m_3 + \cdots + m_t = n_3 + \cdots + n_t$. Continuing in this way we obtain $m_i = n_i$ for all $i = 1, \ldots, t$. This implies that $e_i = f_i$ for all $i = 1, \ldots, r$. □

By the paragraph preceding Theorem 14.6 now also Theorem 14.1 is proved.

Exercises for §14

1. Write down a set of representatives of the isomorphism classes of all abelian groups of order up to 20.

2. How many isomorphism types of abelian groups of order $10,000$ are there?

3. Let G be a group and let H and K be subgroups of G. Show that the following are equivalent:

(i) $H \cap K = 1$, $HK = G$ and for every $h \in H$ and $k \in K$ one has $hk = kh$.

(ii) $H \trianglelefteq G$, $K \trianglelefteq G$, $H \cap K = 1$, and $HK = G$.

(iii) For every $h \in H$ and $k \in K$ one has $hk = kh$ and for every element $g \in G$ there exist unique elements $h \in H$ and $k \in K$ such that $g = hk$.

(iv) The function $H \times K \to G$, $(h, k) \mapsto hk$, from the direct product group $H \times K$ to G is an isomorphism.

If the above conditions are satisfied then G is called the *internal direct product* of the subgroups H and K, and one writes $G = H \times K$. By (iv), this notation is justified.