Chapter I: Groups

1 Semigroups and Monoids

1.1 Definition Let S be a set.

(a) A *binary operation* on S is a map $b : S \times S \to S$. Usually, $b(x, y)$ is abbreviated by xy, $x \cdot y$, $x * y$, $x \bullet y$, $x \circ y$, $x + y$, etc.

(b) Let $(x, y) \mapsto x * y$ be a binary operation on S.

(i) $*$ is called *associative*, if $(x * y) * z = x * (y * z)$ for all $x, y, z \in S$.

(ii) $*$ is called *commutative*, if $x * y = y * x$ for all $x, y \in S$.

(iii) An element $e \in S$ is called a *left* (resp. *right*) identity, if $e * x = x$ (resp. $x * e = x$) for all $x \in S$. It is called an *identity element* if it is a left and right identity.

(c) The set S together with a binary operation $*$ is called a *semigroup* if $*$ is associative. A semigroup $(S, *)$ is called a *monoid* if it has an identity element.

1.2 Examples (a) Addition (resp. multiplication) on $\mathbb{N}_0 = \{0, 1, 2, \ldots\}$ is a binary operation which is associative and commutative. The element 0 (resp. 1) is an identity element. Hence $(\mathbb{N}_0, +)$ and $(\mathbb{N}_0, \cdot)$ are commutative monoids. $\mathbb{N} := \{1, 2, \ldots\}$ together with addition is a commutative semigroup, but not a monoid. $(\mathbb{N}, \cdot)$ is a commutative monoid.

(b) Let X be a set and denote by $\mathcal{P}(X)$ the set of its subsets (its *power set*). Then, $(\mathcal{P}(X), \cup)$ and $(\mathcal{P}(X), \cap)$ are commutative monoids with respective identities $\emptyset$ and X.

(c) $x*y := (x+y)/2$ defines a binary operation on $\mathbb{Q}$ which is commutative but not associative. (Verify!)

(d) Let X be a set. Then, composition $(f, g) \mapsto f \circ g$ is a binary operation on the set $F(X, X)$ of all functions $X \to X$. $(F(X, X), \circ)$ is a monoid with the identity map $\mathrm{id}_X \colon X \to X$, $x \mapsto x$, as identity element. In general it is not commutative. (Verify!)

1.3 Remark Sometimes a binary operation $*$ is given by a table of the form

$$\begin{array}{c|ccc} * & \cdots & y & \cdots \\ \hline \vdots & & \vdots & \\ x & \cdots & x*y & \\ \vdots & & \vdots & \end{array}$$

For instance, the binary operation "and" on the set $\{\text{true}, \text{false}\}$ can be depicted as

$\wedge$	true	false
true	true	false
false	false	false

Thus, $(\{\text{true}, \text{false}\}, \wedge)$ is a commutative monoid with identity element true.

1.4 Remark Let $(S, *)$ be a semigroup and let $x_1, \ldots, x_n \in S$. One defines $x_1 * x_2 * \cdots * x_n := x_1 * (x_2 * (\cdots * x_n) \cdots)$. Using induction on $n \geqslant 3$, one can prove that this element equals the element that one obtains by any other choice of setting the parentheses. We omit the proof.

1.5 Proposition *Let S be a set with a binary operation $*$. If $e \in S$ is a left identity and $f \in S$ is a right identity, then $e = f$. In particular, there exists at most one identity element in S.*

Proof Since e is a left identity, we have $e * f = f$. And since f is a right identity, we also have $e * f = e$. Thus, $e = e * f = f$. □

1.6 Remark Identity elements are usually denoted by 1 (resp. 0), if the binary operation is denoted by $*$, $\cdot$, $\bullet$, $\circ$ (resp. $+$).

1.7 Definition Let $(M, *)$ be a monoid and let $x \in M$. An element $y \in M$ is called a *left* (resp. *right*) *inverse* of x if $y * x = 1$ (resp. $x * y = 1$). If y is a left and right inverse of x, then y is called an *inverse* of x. If x has an inverse, we call x an *invertible* element of M.

1.8 Proposition *Let $(M, *)$ be a monoid and let $x \in M$. If $y \in M$ is a left inverse of x and $z \in M$ is a right inverse of x, then $y = z$. In particular, every element of M has at most one inverse.*

Proof We have $y = y * 1 = y * (x * z) = (y * x) * z = 1 * z = z$. $\square$

1.9 Remark If x is an invertible element in a monoid, then we denote its (unique) inverse by x^{-1} (resp. $-x$), if the binary operation is denoted by $*$, $\cdot$, $\bullet$, $\circ$ (resp. $+$).

1.10 Example Let

$$M := \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \,\middle|\, a, b, c \in \mathbb{Z} \right\}.$$

M is a non-commutative monoid under matrix multiplication. The element $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$ has an inverse if and only if $a, c \in \{\pm 1\}$. In this case, one has

$$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}^{-1} = \begin{pmatrix} a & -abc \\ 0 & c \end{pmatrix}.$$

(Verify!)

1.11 Proposition *Let $(M, *)$ be a monoid and let $x, y \in M$.*

(a) *If x is invertible, then also x^{-1} is invertible with $(x^{-1})^{-1} = x$.*

(b) *If x and y are invertible, then also $x * y$ is invertible with inverse $y^{-1} * x^{-1}$.*

(c) *The identity element 1 is invertible with $1^{-1} = 1$.*

Proof (a) Since $x * x^{-1} = 1 = x^{-1} * x$, the element x is a left and right inverse of x^{-1}.

(b) We have $(x*y)*(y^{-1}*x^{-1}) = ((x*y)*y^{-1})*x^{-1} = (x*(y*y^{-1}))*x^{-1} = (x * 1) * x^{-1} = x * x^{-1} = 1$, and similarly, we have $(y^{-1} * x^{-1}) * (x * y) = 1$. This implies that $y^{-1} * x^{-1}$ is a left and right inverse of $x * y$.

(c) This follows from the equation $1 * 1 = 1$. $\square$

1.12 Definition In a semigroup S we set $x^n := x * \cdots * x$ (n factors) for any $x \in S$ and $n \in \mathbb{N}$. If S is a monoid we also define $x^0 := 1$ for all $x \in S$. If additionally x is invertible, we define $x^{-n} := x^{-1} * \cdots * x^{-1}$ (n factors) for any $n \in \mathbb{N}$.

1.13 Remark For an element x in a semigroup (resp. monoid) one has

$$x^m * x^n = x^{m+n} \quad \text{and} \quad (x^m)^n = x^{mn},$$

for all $m, n \in \mathbb{N}$ (resp. all $m, n \in \mathbb{N}_0$). If x is an invertible element in a monoid, these rules hold for all $m, n \in \mathbb{Z}$. This can be proved by distinguishing the cases that m, n are positive, negative or equal to 0.

Moreover, if x and y are elements in a commutative semigroup (resp. monoid) then

$$(x * y)^n = x^n * y^n \quad \text{for all } n \in \mathbb{N} \text{ (resp. all } n \in \mathbb{N}_0).$$

If x and y are invertible elements in a commutative monoid, this holds for all $n \in \mathbb{Z}$.

Exercises

1. Determine the invertible elements of the monoids among the examples in 1.2.

2. Prove the statement in Example 1.10.

3. Let S be the set of all matrices

$$\begin{pmatrix} 0 & a \\ 0 & b \end{pmatrix}$$

with entries $a, b \in \mathbb{Z}$. Show that S is a semigroup under matrix multiplication and show that S has a right identity but no left identity. Determine all right identities. Give an example of a semigroup which has a left identity but no right identity.

4. Let G be a semigroup which has a left identity element e such that every element of G has a left inverse with respect to e, i.e., for every $x \in G$ there exists an element $y \in G$ with $yx = e$. Show that e is an identity element and that each element of G is invertible. (In other words, G is a *group*; see Section 2 for a definition.)

5. (a) Let S, T, U, and V be sets and let $X \subseteq S \times T$, $Y \subseteq T \times U$, and $Z \subseteq U \times V$ be subsets. Define

$$X * Y := \{(s, u) \in S \times U \mid \exists t \in T: \ (s, t) \in X \text{ and } (t, u) \in Y\} \subseteq S \times U.$$

Show that

$$(X * Y) * Z = X * (Y * Z).$$

(b) Let S be a set. Show that $(\mathcal{P}(S \times S), *)$ is a monoid. Is it commutative?

(c) What are the invertible elements in the monoid of Part (b)?

2 Groups

From now on through the rest of this chapter we will usually write abstract binary operations in the multiplicative form $(x, y) \mapsto xy$ and denote identity elements by 1.

2.1 Definition A *group* is a monoid in which every element is invertible. A group is called *abelian* if it is commutative. The *order* of a group G is the number of its elements. It is denoted by $|G|$.

2.2 Remark If G is a semigroup with a left (resp. right) identity e and if every element of G has a left (resp. right) inverse with respect to e, then G is a group. (see Exercise 4 of Section 1.)

2.3 Examples (a) $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$ are abelian groups, but $(\mathbb{N}_0, +)$ is not a group.

(b) $(\mathbb{Q}\smallsetminus\{0\}, \cdot)$, $(\mathbb{R}\smallsetminus\{0\}, \cdot)$, $(\mathbb{C}\smallsetminus\{0\}, \cdot)$ are abelian groups, but $(\mathbb{Z}\smallsetminus\{0\}, \cdot)$ and $(\mathbb{Q}, \cdot)$ are not groups.

(c) $(\{1\}, \cdot)$ and $(\{0\}, +)$ are groups of order 1. A group of order 1 is called a *trivial group.*

(d) For any set X, the set $\mathrm{Sym}(X) := \{f : X \to X \mid f \text{ is bijective}\}$ is a group under composition. It is called the *symmetric group on* X. Its elements are called *permutations* of X. If $|X| = n$, then $|\mathrm{Sym}(X)| = n!$. We write $\mathrm{Sym}(n)$ instead of $\mathrm{Sym}(\{1, 2, \dots, n\})$ and call $\mathrm{Sym}(n)$ the *symmetric group of degree* n. We use the following notation for $\pi \in \mathrm{Sym}(n)$:

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

So if, for instance, π and ρ are elements of $\mathrm{Sym}(3)$ given by

$$\pi = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \quad \text{and} \quad \rho = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

then

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

(e) If $G_1, G_2, \dots, G_n$ are groups, then also their *direct product*

$$G_1 \times G_2 \times \cdots \times G_n$$

is a group under the binary operation defined by

$$(x_1, \ldots, x_n)(y_1, \ldots, y_n) := (x_1y_1, \ldots, x_ny_n)\,.$$

(f) For every $n \in \mathbb{N}$, the sets $\mathrm{GL}_n(\mathbb{Q})$, $\mathrm{GL}_n(\mathbb{R})$, $\mathrm{GL}_n(\mathbb{C})$ of invertible matrices with entries in $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, respectively, form groups under multiplication.

2.4 Definition Let G and H be groups. A map $f\colon G \to H$ is called a *homomorphism*, if $f(xy) = f(x)f(y)$ for all $x, y \in G$. The set of all homomorphisms from G to H is denoted by $\mathrm{Hom}(G, H)$. A homomorphism $f\colon G \to H$ is called

(a) a *monomorphism* if f is injective,

(b) an *epimorphism* if f is surjective,

(c) an *isomorphism* if f is bijective (often indicated by $f\colon G \xrightarrow{\sim} H$),

(d) an *endomorphism* if $G = H$,

(e) an *automorphism* if $G = H$ and f is bijective.

2.5 Remark Let $f\colon G \to H$ be a homomorphism between groups G and H. Then $f(1_G) = 1_H$ and $f(x^{-1}) = f(x)^{-1}$ for all $x \in G$. Moreover, if also $g\colon H \to K$ is a homomorphism between H and a group K, then $g \circ f\colon G \to K$ is a homomorphism. If $f\colon G \to H$ is an isomorphism, then also its inverse $f^{-1}\colon H \to G$ is an isomorphism. The automorphisms $f\colon G \to G$ form again a group under composition, called the *automorphism group* of G and denoted by $\mathrm{Aut}(G)$.

2.6 Examples (a) For each $n \in \mathbb{N}$, the map $(\mathbb{Z}, +) \to (\mathbb{Z}, +)$, $k \mapsto nk$, is a monomorphism.

(b) $(\mathbb{R}, +) \to (\mathbb{R}_{>0}, \cdot)$, $x \mapsto e^x$, is an isomorphism.

(c) Let G be a group and let $g \in G$. Then $c_g\colon G \to G$, $x \mapsto gxg^{-1}$, is an automorphism of G with inverse $c_{g^{-1}}$. One calls c_g the *inner automorphism induced by g* (or *conjugation with g*). Note that $c_g \circ c_h = c_{gh}$ for $g, h \in G$. Thus, $G \mapsto \mathrm{Aut}(G)$, $g \mapsto c_g$, is a group homomorphism.

(d) For each $n \in \mathbb{N}$, the sign map

$$\mathrm{sgn}\colon \mathrm{Sym}(n) \to (\{\pm 1\}, \cdot)\,, \quad \pi \mapsto \prod_{1 \leqslant i < j \leqslant n} \frac{\pi(j) - \pi(i)}{j - i}\,,$$

is a homomorphism (see Exercise 2). To see that $\mathrm{sgn}(\pi) \in \{\pm 1\}$, let $\mathcal{P}_n^{(2)}$ denote the set of all subsets $\{i,j\}$ of $\{1,\ldots,n\}$ of cardinality 2 and note that

$$|\mathrm{sgn}(\pi)| = \prod_{\{i,j\}\in\mathcal{P}_n^{(2)}} \frac{|\pi(j)-\pi(i)|}{|j-i|} = \frac{\prod_{\{i,j\}\in\mathcal{P}_n^{(2)}} |\pi(j)-\pi(i)|}{\prod_{\{i,j\}\in\mathcal{P}_n^{(2)}} |j-i|} = 1\,,$$

since, for fixed $\pi \in \mathrm{Sym}(n)$, the function $\mathcal{P}_n^{(2)} \to \mathcal{P}_n^{(2)}$, $\{i,j\} \mapsto \{\pi(i),\pi(j)\}$, is a bijection. If $\mathrm{sgn}(\pi) = 1$ (resp. $\mathrm{sgn}(\pi) = -1$), then we call π an *even* (resp. *odd*) permutation.

(e) For every $n \in \mathbb{N}$, the determinant map $\det\colon \mathrm{GL}_n(\mathbb{R}) \to (\mathbb{R} \smallsetminus \{0\}, \cdot)$ is an epimorphism.

2.7 Definition Two groups G and H are called *isomorphic*, if there exists an isomorphism $f\colon G \xrightarrow{\sim} H$. In this case we write $G \cong H$.

2.8 Remark (a) The relation $\cong$ ('is isomorphic to') is an equivalence relation, i.e., for groups G, H, K we have:

(i) $G \cong G$.

(ii) If $G \cong H$ then $H \cong G$.

(iii) If $G \cong H$ and $H \cong K$ then $G \cong K$.

(b) Isomorphic groups G and H behave identically in all respects. In fact, if $f\colon G \xrightarrow{\sim} H$ is an isomorphism, every statement about G can be translated into a statement about H using f, and vice-versa. G and H are basically the same group: one arises from the other by renaming the elements using f, but keeping the multiplication.

2.9 Definition Let G be a group. A subset H of G is a called a *subgroup* of G if the following hold:

(i) If $x, y \in H$ then $xy \in H$.

(ii) $1_G \in H$.

(iii) If $x \in H$ then x^{-1} in H.

In this case, H together with the restricted binary operation $H \times H \to H$, $(x,y) \mapsto xy$, is again a group. We write $H \leqslant G$, if H is a subgroup of G. A subgroup H of G is called a *proper subgroup*, if $H \neq G$. In this case we write $H < G$.

2.10 Proposition *Let G be a group and let H be a subset of G. Then the following are equivalent:*

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

(ii) *H is non-empty and if $x, y \in H$ then also $xy^{-1} \in H$.*

Proof Exercise 3. □

2.11 Examples (a) For each group G one has $\{1_G\} \leqslant G$ and $G \leqslant G$. The subgroup $\{1_G\}$ is called the *trivial subgroup* of G.

(b) If $H \leqslant G$ and $K \leqslant H$ then $K \leqslant G$. Also, if $K \subseteq H \leqslant G$ and $K \leqslant G$ then $K \leqslant H$.

(c) The intersection of any collection of subgroups of a group G is again a subgroup. (Warning: In general, the union of subgroups is not a subgroup.)

(d) $\mathbb{Z}$, $\mathbb{Q}$ and $\mathbb{R}$ are subgroups of $(\mathbb{C}, +)$.

(e) For any non-empty subsets $X_1, X_2, \ldots, X_n$ of a group G we define

$$X_1 X_2 \cdots X_n := \{x_1 x_2 \cdots x_n \mid x_1 \in X_1, \ldots, x_n \in X_n\}.$$

In general, this is not a subgroup, even if $X_1, \ldots, X_n$ are. For subgroups $H, K \leqslant G$ one has (see Exercise 4):

$$HK \leqslant G \iff KH = HK.$$

In any case, if H and K are finite subgroups one has (see Excercise 5):

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

(f) If X is a non-empty subset of a group G, its *normalizer* is defined as

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

Note that $gXg^{-1} = X \iff c_g(X) = X \iff gX = Xg$. One always has $N_G(X) \leqslant G$.

Moreover, the *centralizer* of X is defined as

$$C_G(X) := \{g \in G \mid gxg^{-1} = x \text{ for all } x \in X\}.$$

Note that $g \in C_G(X) \iff c_g$ is the identity on $X \iff gx = xg$ for all $x \in X$. It is easy to check that $C_G(X) \leqslant N_G(X)$ is again a subgroup. If $X = \{x\}$ consists only of one element we also write $C_G(x)$ instead of $C_G(\{x\})$.

(g) The subgroup $Z(G) := C_G(G) = \{g \in G \mid gx = xg \text{ for all } x \in G\}$ is called the *center* of G. It is an abelian subgroup.

(h) If $f\colon G \to H$ is a group homomorphism and if $U \leqslant G$ and $V \leqslant H$, then $f(U) \leqslant H$ and $f^{-1}(V) := \{g \in G \mid f(g) \in V\} \leqslant G$. In particular, the *image of* f, $\mathrm{im}(f) := f(G)$, is a subgroup of H, and the *kernel of* f, $\ker(f) := f^{-1}(\{1_H\})$ is a subgroup of G. Note: f is injective if and only if $\ker(f) = 1$. (See Exercise 7.)

The kernel of $\mathrm{sgn}\colon \mathrm{Sym}(n) \to \{\pm 1\}$ is called the *alternating group of degree* n and is denoted by $\mathrm{Alt}(n)$.

The kernel of $\det\colon \mathrm{GL}_n(\mathbb{R}) \to (\mathbb{R} \smallsetminus \{0\}, \cdot)$ is called the *special linear group of degree* n over $\mathbb{R}$ and is denoted by $\mathrm{SL}_n(\mathbb{R})$.

2.12 Theorem *The subgroups of* $(\mathbb{Z}, +)$ *are the subsets of the form* $n\mathbb{Z} := \{nk \mid k \in \mathbb{Z}\}$ *for* $n \in \mathbb{N}_0$.

Proof For every $n \in \mathbb{Z}$, the map $\mathbb{Z} \to \mathbb{Z}$, $k \mapsto kn$, is a group homomorphism (cf. Example 2.6(a)) with image $n\mathbb{Z}$. By Example 2.11(h), it is a subgroup of $\mathbb{Z}$.

Conversely, assume that $H \leqslant \mathbb{Z}$. If $H = \{0\}$, then $H = 0\mathbb{Z}$ and we are done. So assume that $H \neq \{0\}$. Then H contains a non-zero integer and with it its inverse. So, H contains a positive integer. Let n be the smallest positive integer contained in H. We will show that $H = n\mathbb{Z}$. First, since $n \in H$ also $n+n, n+n+n, \ldots \in H$. Since H is a subgroup also the inverses of these elements, namely $-n, -n + (-n), \ldots$ are in H. Thus, $n\mathbb{Z} \leqslant H$. To show the other inclusion, take an arbitrary element h of H and write it as $h = qn+r$ with $q \in \mathbb{Z}$ and $r \in \{0, 1, \ldots, n-1\}$. Then we have $r = h - qn \in H$ which implies $r = 0$ (by the minimality of n). This shows that $h = qn \in n\mathbb{Z}$. So, $H \leqslant n\mathbb{Z}$. □

2.13 Definition Let G be a group and let $X \subseteq G$ be a subset.

(a) The *subgroup generated by* X is defined as

$$\langle X \rangle := \{x_1^{\epsilon_1} \cdots x_k^{\epsilon_k} \mid k \in \mathbb{N},\ x_1, \ldots, x_k \in X,\ \epsilon_1, \ldots, \epsilon_k \in \{\pm 1\}\}\,.$$

If $X = \emptyset$ one defines $\langle X \rangle := \{1_G\}$. Clearly, $\langle X \rangle$ is a subgroup of G. Moreover, if U is a subgroup of G which contains X then U also contains $\langle X \rangle$. Thus, $\langle X \rangle$ is characterized as the the smallest subgroup of G which contains X.

Moreover, one has

$$\langle X\rangle = \bigcap_{X\subseteq U\leqslant G} U\,,$$

i.e., $\langle X\rangle$ is the intersection of all subgroups of U that contain X.

(b) If $\langle X\rangle = G$, then we call X a *generating set* or a *set of generators* of G. If G is generated by a single element, then G is called *cyclic.*

2.14 Examples (a) Let G be a group and let $x, y \in G$. The element $[x, y] := xyx^{-1}y^{-1}$ is called the *commutator* of x and y. One has $xy = [x, y]yx$. Thus, $[x, y] = 1$ if and only if $xy = yx$, i.e., x and y commute. The subgroup of G generated by all the commutators $[x, y]$, $x, y \in G$, is called the *commutator subgroup* (or the *derived subgroup*) of G and it is denoted by G' or $[G, G]$. Note that $[x, y]^{-1} = [y, x]$. Therefore,

$$G' = \{[x_1, y_1]\cdots[x_k, y_k] \mid k \in \mathbb{N},\ x_1, \ldots, x_k, y_1, \ldots, y_k \in G\}\,.$$

Note that

$$G' = \{1\} \iff G \text{ is abelian} \iff Z(G) = G\,.$$

(b) The elements

$$x = \begin{pmatrix} 1 & 2 & 3 & 4\\ 2 & 1 & 4 & 3\end{pmatrix} \qquad y = \begin{pmatrix} 1 & 2 & 3 & 4\\ 3 & 4 & 1 & 2\end{pmatrix}$$

generate a subgroup V_4 of Sym(4), which is called the *Klein* 4*-group.* One checks easily that $x^2 = 1$, $y^2 = 1$ and

$$xy = yx = \begin{pmatrix} 1 & 2 & 3 & 4\\ 4 & 3 & 2 & 1\end{pmatrix} =: z\,.$$

This shows that $V_4 = \{1, x, y, z\}$ and we obtain the following multiplication table:

	1	x	y	z
1	1	x	y	z
x	x	1	z	y
y	y	z	1	x
z	z	y	x	1

2.15 Definition Let G be a group and let $H \leqslant G$. For $x, y \in G$ we define $x \,{}_H\!\sim y$ if $x^{-1}y \in H$. This defines an equivalence relation on G (verify). The equivalence class containing $x \in G$ is equal to xH (verify) and is called the *left coset* of H containing x. The set of equivalence classes is denoted by G/H. The number $|G/H|$ is called the *index* of H in G and is denoted by $[G : H]$.

2.16 Remark Let G be a group and let $H \leqslant G$. In a similar way one defines the relation $\sim_H$ on G by $x \sim_H y$ if $xy^{-1} \in H$. This is again an equivalence relation. The equivalence class of $x \in G$ is equal to Hx, the *right coset* of H containing x. The set of right cosets is denoted by $H\backslash G$. We will mostly work with left cosets. If G is abelian then $xH = Hx$ for all $x \in G$. However, in general this is not the case.

2.17 Example Fix $n \in \mathbb{N}_0$ and $k \in \mathbb{Z}$. Then the set $k + n\mathbb{Z}$ is a left and right coset of $n\mathbb{Z}$ in $(\mathbb{Z}, +)$. For example,

$$2 + 5\mathbb{Z} = \{\ldots, -8, -3, 2, 7, 12, \ldots\}\,.$$

For this particular choice ($G = \mathbb{Z}$ and $H = n\mathbb{Z}$) we also write $x \equiv y \mod n$ instead of $x \,{}_H\!\sim y$ and say "x is *congruent* to y *modulo* n". The coset $k + n\mathbb{Z}$ is called the *congruence class* of k *modulo* n. One has

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

and $[\mathbb{Z} : n\mathbb{Z}] = n$.

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

(a) *For each $g \in G$, the map $H \to gH$, $h \mapsto gh$, is a bijection. In particular, any two left cosets of H have the same cardinality, namely $|H|$.*

(b) *For each $g \in G$, the map $H \to Hg$, $h \mapsto hg$, is a bijection. In particular, any two right cosets of H have the same cardinality, namely $|H|$.*

(c) *The map $G/H \to H\backslash G$, $gH \mapsto Hg^{-1}$, is well-defined and bijective. In particular, $|G/H| = |H\backslash G|$.*

Proof (a) It is easy to verify that $gH \to H$, $x \mapsto g^{-1}x$, is an inverse.

(b) One verifies easily that $Hg \to H$, $x \mapsto xg^{-1}$, is an inverse.

(c) In order to show that the map is well-defined assume that $g_1, g_2 \in G$ such that $g_1H = g_2H$. We need to show that then $Hg_1^{-1} = Hg_2^{-1}$. But, we have: $g_1H = g_2H \iff g_1^{-1}g_2 \in H \iff Hg_1^{-1} = Hg_2^{-1}$. Finally, the map $H\backslash G \to G/H$, $Hg \mapsto g^{-1}H$, is an inverse. □

2.19 Corollary (Lagrange 1736–1813) *Let H be a subgroup of a group G. Then*

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

(with the usual rules for the quantity ∞). In particular, if G is a finite group then $|H|$ and $[G : H]$ are divisors of $|G|$.

Proof G is the disjoint union of the left cosets of H. There are $[G : H]$ such cosets, and each one has $|H|$ elements by Proposition 2.18(a). □

2.20 Examples (a) The subgroups V_4 and $\mathrm{Alt}(4)$ of $\mathrm{Sym}(4)$ have order 4 and 12, which are divisors of 24 (in accordance with Lagrange's Theorem). By Lagrange, $\mathrm{Sym}(4)$ cannot have a subgroup of order 10. We will see later: $\mathrm{Alt}(4)$ does not have a subgroup of order 6, although 6 divides 12.

(b) Let G be a finite group whose order is a prime p. Then, by Lagrange, 1 and G are the only subgroups of G. Moreover, G is cyclic, generated by any element $x \neq 1$. In fact, $H := \langle x \rangle$ is a subgroup of G with $1 < |H|$. Thus $H = G$.

Exercises

1. Prove the statements in Remark 2.5.

2. Let $n \in \mathbb{N}$. For pairwise distinct elements $a_1, \ldots, a_k$ in $\{1, \ldots, n\}$ we denote by $(a_1, a_2, \ldots, a_k)$ the permutation $\sigma \in \mathrm{Sym}(n)$ given by $\sigma(a_1) = a_2$, $\sigma(a_2) = a_3, \ldots, \sigma(a_{k-1}) = a_k$, $\sigma(a_k) = a_1$, and $\sigma(a) = a$ for all other $a \in \{1, \ldots, n\}$. Such an element is called a *k-cycle*. A 2-cycle is also called a *transposition*.

(a) Show that every element in $\mathrm{Sym}(n)$ is a product of disjoint cycles.

(b) Show that every cycle is a product of transpositions.

(c) Show that every transposition is a product of an odd number of *simple* transpositions, i.e., transpositions of the form $(i, i+1)$, $i = 1, \ldots, n-1$.

(d) Let $\sigma \in \mathrm{Sym}(n)$. A pair (i, j) of natural numbers i, j with $1 \leqslant i < j \leqslant n$ is called an *inversion* for σ if $\sigma(j) < \sigma(i)$. We denote by $l(\sigma)$ the number of inversions of σ. Show that for a transposition $\tau = (a, b)$ with $1 \leqslant a < b \leqslant n$ one has $l(\tau) = 2(b - a) - 1$.

(e) Show that for every $i = 1, \ldots, n-1$ one has

$$l((i,i+1)\sigma) - l(\sigma) = \begin{cases} 1 & \text{if } \sigma^{-1}(i) < \sigma^{-1}(i+1), \\ -1 & \text{if } \sigma^{-1}(i) > \sigma^{-1}(i+1). \end{cases}$$

(f) Show that if $\sigma \in \mathrm{Sym}(n)$ can be written as a product of r transpositions then $r \equiv l(\sigma) \mod 2$. Conclude that if σ can also be written as a product of s transpositions then $r \equiv s \mod 2$.

(g) Show that the map $\mathrm{Sym}(n) \to \{\pm 1\}$, $\sigma \mapsto (-1)^{l(\sigma)}$, is a group homomorphism which coincides with the homomorphism sgn from class and that $\mathrm{sgn}(\tau) = -1$ for every transposition τ.

3. Prove the statement in Proposition 2.10.

4. Let H and K be subgroups of a group G. Show that

$$HK \leqslant G \iff KH = HK\,.$$

5. Let H and K be finite subgroups of a group G. Show that

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

Hint: Consider the function $f : H \times K \to HK$ given by $f(h,k) = hk$. Show that for every element $x \in HK$ there exist precisely $|H \cap K|$ elements $(h,k) \in H \times K$ with $hk = x$.

6. Show that for any non-empty subset X of a group G, the normalizer of X, $N_G(X)$, and the centralizer of X, $C_G(X)$, is again a subgroup of G. Show also that $C_G(X)$ is contained in $N_G(X)$.

7. Let $f\colon G \to H$ be a group homomorphism.

(a) If $U \leqslant G$ then $f(U) \leqslant H$.

(b) If $V \leqslant H$ then $f^{-1}(V) := \{g \in G \mid f(g) \in V\}$ is a subgroup of G. (The subgroup $f^{-1}(V)$ is also called the *preimage* of V under f. Note that the notation $f^{-1}(V)$ does not mean that f has an inverse.)

(c) Show that f is injective if and only if $\ker(f) = \{1\}$.

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

(a) Show that the relation ${}_H\!\sim$ on G defined in Definition 2.15 is an equivalence relation.

(b) Show that the equivalence class of the element $g \in G$ with respect to ${}_H\!\sim$ is equal to gH.

9. Let G and A be groups and assume that A is abelian. Show that the set $\mathrm{Hom}(G, A)$ of group homomorphisms from G to A is again an abelian group under the multiplication defined by

$$(f_1 \cdot f_2)(g) := f_1(g)f_2(g) \quad \text{for } f_1, f_2 \in \mathrm{Hom}(G, A) \text{ and } g \in G.$$

10. Consider the elements $\sigma := (1, 2, 3)$ and $\tau := (1, 2)$ of $\mathrm{Sym}(3)$. Here we used the cycle notation from Exercise 2.

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

(b) Show that $\{\sigma, \tau\}$ is a generating set of $\mathrm{Sym}(3)$.

(c) Show that every element of $\mathrm{Sym}(3)$ can be written in the form $\sigma^i\tau^j$ with $i \in \{0, 1, 2\}$ and $j \in \{0, 1\}$.

(d) Compute all subgroups of $\mathrm{Sym}(3)$ and their normalizers and centralizers.

(e) Compute the commutator subgroup of $\mathrm{Sym}(3)$ and the center of $\mathrm{Sym}(3)$.

11. Consider the elements $\sigma := (1, 2, 3, 4)$ and $\tau := (1, 4)(2, 3)$ of $\mathrm{Sym}(4)$.

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

(b) Determine the subgroup $\langle\sigma, \tau\rangle$ of $\mathrm{Sym}(4)$. It is called the *dihedral group* of order 8 and is denoted by D_8.

(c) Determine $Z(D_8)$.

(d) Determine the derived subgroup D_8' of D_8.

12. Let G and H be groups and let $f\colon G \to H$ be an isomorphism.

(a) Show that G is abelian if and only if H is abelian.

(b) Let X be a subset of G and set $Y := f(X) \subseteq H$. Show that $f(\langle X\rangle) = \langle Y\rangle$, $f(N_G(X)) = N_H(Y)$, $f(C_G(X)) = C_H(Y)$.

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

(d) Show that $f(Z(G)) = Z(H)$.

(e) Show that $f(G') = H'$.

13. (Dedekind's Identity) Let U, V, W be subgroups of a group G with $U \leqslant W$. Show that

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

14. (a) Let p be a prime, let $C_p = \langle x\rangle$ be a cyclic group of order p and set $G := C_p \times C_p$. Show that G has exactly $p + 1$ subgroups of order p.

(b) A group of 25 mathematicians meets for a 6 day conference. Between the morning and afternoon lectures they have their lunch in a room with 5 round tables and 5 chairs around each table. The organizer would like to assign every day new places at the tables in such a way that each participant has eaten with any other one at least once at the same table. Is this possible? (Hint: Use (a) and use convenient equivalence relations on G.)

3 Normal Subgroups and Factor Groups

3.1 Theorem *Let G be a group, let N be a subgroup of G, and let $\nu\colon G \to G/N$ denote the function defined by $\nu(g) := gN$. Then the following are equivalent:*

(i) *G/N is a group under $(g_1N, g_2N) \mapsto (g_1N)(g_2N)$, where $(g_1N)(g_2N)$ is defined as the product of the subsets g_1N and g_2N of G as in Example 2.11(e).*

(ii) *G/N has a group structure such that the function ν is a homomorphism.*

(iii) *There exists a group H and a group homomorphism $f\colon G \to H$ such that* $\ker(f) = N$.

(iv) *$gNg^{-1} \subseteq N$ for all $g \in G$.*

(v) *$gNg^{-1} = N$ for all $g \in G$.*

(vi) *$gN = Ng$ for all $g \in G$.*

Proof (i)⇒(ii): Use the group structure defined in (i). We need to show that ν is a homomorphism. For $g_1, g_2 \in G$ we have $\nu(g_1)\nu(g_2) = (g_1N)(g_2N)$ which must be again a left coset by (i). But $(g_1N)(g_2N)$ contains the element g_1g_2. This implies that $(g_1N)(g_2N) = (g_1g_2)N$. Thus, $\nu(g_1)\nu(g_2) = (g_1N)(g_2N) = (g_1g_2)N = \nu(g_1g_2)$, and ν is a homomorphism.

(ii)⇒(iii): Set $H := G/N$, which has a group structure, by (ii), such that $f := \nu$ is a homomorphism. Moreover, since ν is a homomorphism, $\nu(1) = N$ must be the identity element of G/N. Thus, $\ker(\nu) = \{g \in G \mid gN = N\} = N$.

(iii)⇒(iv): For each $g \in G$ and each $n \in N$ one has

$$f(gng^{-1}) = f(g)f(n)f(g^{-1}) = f(g) \cdot 1 \cdot f(g)^{-1} = 1$$

which shows that $gng^{-1} \in \ker(f) = N$. Thus $gNg^{-1} \subseteq N$ for all $g \in G$.

(iv)⇒(v): Let $g \in G$. Then, (iv) applied to the element g^{-1} yields $g^{-1}Ng \subseteq N$. Applying c_g then implies $N = gg^{-1}Ngg^{-1} \subseteq gNg^{-1}$. Together with (iv) for g we obtain (v) for g.

(v)⇒(vi): For each $g \in G$ we have $gN = gNg^{-1}g \overset{(v)}{=} Ng$.

(vi)⇒(i): For any $g_1, g_2 \in G$ we have

$$(g_1N)(g_2N) \overset{\text{(vi)}}{=} g_1g_2NN = g_1g_2N \tag{3.1.a}$$

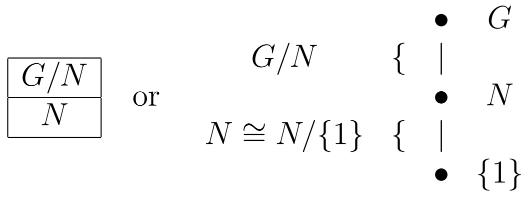
so that $(g_1N, g_2N) \mapsto (g_1N)(g_2N)$ is a binary operation on G/N. Obviously, it is associative. Moreover, by (3.1.a), $N = 1 \cdot N$ is an identity element, and for any $g \in G$, $g^{-1}N$ is an inverse of gN. □

3.2 Definition If the conditions (i)–(vi) in Theorem 3.1 are satisfied, we call N a *normal* subgroup of G and write $N \trianglelefteq G$. We write $N \triangleleft G$, if N is a proper normal subgroup of G. If $N \trianglelefteq G$ then (i) and (vi) in the previous theorem imply that the set G/N of left cosets is again a group under the binary operation

$$(g_1N, g_2N) \mapsto (g_1N)(g_2N) = g_1g_2NN = g_1g_2N\,.$$

It is called the *factor group* of G with respect to N, or shorter 'G modulo N'. Moreover, by the proof of (i)⇒(ii), the function $\nu\colon G \to G/N$, $g \mapsto gN$, is a homomorphism, called the *canonical epimorphism* or *natural epimorphism.*

3.3 Examples (a) We always have $\{1\} \trianglelefteq G$ and $G \trianglelefteq G$. If G and $\{1\}$ are the only normal subgroups of G and if $G \neq \{1\}$, we call G a *simple* group. By Lagrange's Theorem, groups of prime order are always simple. If G is not simple, there exists $\{1\} < N \triangleleft G$ and we think of G as being built from the two groups N and G/N. This is often depicted as



We may think of G/N as an approximation to G. An element of G/N determines an element of G up to an error term in N, and the multiplication in G/N determines the multiplication in G up to an error term in N.

(b) If G is a group and $H \leqslant Z(G)$, then $H \trianglelefteq G$. In particular, $Z(G) \trianglelefteq G$. In an abelian group G, every subgroup is normal (since $G = Z(G)$). The center of G is even more special. For every $f \in \mathrm{Aut}(G)$ one has $f(Z(G)) = Z(G)$ (verify!). A subgroup $N \leqslant G$ with $f(N) = N$ for all $f \in \mathrm{Aut}(G)$ is called *characteristic* in G. In this case we write $N \underset{\text{char}}{\trianglelefteq} G$. Note that $N \underset{\text{char}}{\trianglelefteq} G$ implies that $N \trianglelefteq G$ (since $c_g \in \mathrm{Aut}(G)$ for all $g \in G$).

(c) Let G be a group and let $G' \leqslant H \leqslant G$, where G' denotes the commutator subgroup of G, cf. Example 2.14(a). Then $H \trianglelefteq G$ and G/H is abelian. In fact, for any $g \in G$ and $h \in H$ one has

$$ghg^{-1} = ghg^{-1}h^{-1}h = [g,h]h \in G'H \leqslant H\,,$$

and for any $x, y \in G$ one has

$$(xH)(yH) = xyH = xy[y^{-1},x^{-1}]H = yxH = (yH)(xH)\,.$$

Here, the second equality holds, since $[y^{-1},x^{-1}] \in H$. In particular, with $H = G'$, we obtain that G' is normal in G and that G/G' is abelian.

Conversely, if N is a normal subgroup of G with abelian factor group G/N, then $G' \leqslant N \leqslant G$. In fact, let $x, y \in G$. Then one has

$$[x,y]N = xyx^{-1}y^{-1}N = (xN)(yN)(x^{-1}N)(y^{-1}N) = [xN, yN] = N\,,$$

which implies that $[x,y] \in N$. Thus, we have $G' \leqslant N$.

The above two considerations show that G' is the smallest (with respect to inclusion) normal subgroup of G with abelian factor group. This factor group G/G' is called the *commutator factor group* of G and it is denoted by G^{ab}.

(d) If $H \leqslant G$ with $[G:H] = 2$ then $H \triangleleft G$. In fact, for $g \in H$ we have $gH = H = Hg$, and for $g \in G \smallsetminus H$ we have $gH = G \smallsetminus H = Hg$, since there are only two left cosets and two right cosets and one of them is H.

(e) For every subgroup H of G one has $H \trianglelefteq N_G(H) \leqslant G$. Moreover, $N_G(H) = G$ if and only if $H \trianglelefteq G$.

(f) For each subset X of a group G one has $C_G(X) \trianglelefteq N_G(X)$ (see Exercises). In particular, setting $X = G$, we obtain again $Z(G) \trianglelefteq G$.

(g) For each $n \in \mathbb{N}$ one has $\mathrm{Alt}(n) = \ker(\mathrm{sgn}) \trianglelefteq \mathrm{Sym}(n)$.

(h) For each $n \in \mathbb{N}$ one has $\mathrm{SL}_n(\mathbb{R}) = \ker(\det) \trianglelefteq \mathrm{GL}_n(\mathbb{R})$.

(i) Let $G := \mathrm{Sym}(3)$ and let

$$H := \left\langle \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \right\rangle = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \right\}.$$

Then $H \ntrianglelefteq G$, since

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \notin H\,.$$

3.4 Theorem (Fundamental Theorem of Homomorphisms, Universal Property of $\nu\colon G \to G/N$) *Let G be a group, $N \trianglelefteq G$, and let $\nu\colon G \to G/N$, $g \mapsto gN$, denote the natural epimorphism.*

For every homomorphism $f\colon G \to H$ with $N \leqslant \ker(f)$, there exists a unique homomorphism $\overline{f}\colon G/N \to H$ such that $\overline{f} \circ \nu = f$:

$$\begin{tikzcd}
G \arrow[r, "f"] \arrow[d, "\nu"'] & H \\
G/N \arrow[ur, dotted, "\overline{f}"'] &
\end{tikzcd}$$

Moreover, $\ker(\overline{f}) = \{aN \mid a \in \ker(f)\} = \ker(f)/N$ *and* $\operatorname{im}(\overline{f}) = \operatorname{im}(f)$.

Proof (a) Existence: Let $a, b \in G$ with $aN = bN$. Then $a^{-1}b \in N$ and $f(b) = f(aa^{-1}b) = f(a)f(a^{-1}b) = f(a)$, since $N \leqslant \ker(f)$. Therefore, the function $\overline{f}\colon G/N \to H$, $aN \mapsto f(a)$, is well-defined. It is a homomorphism, since

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

for all $a, b \in G$. Moreover, for all $a \in G$, we have $\overline{f}(\nu(a)) = \overline{f}(aN) = f(a)$. Thus, $\overline{f} \circ \nu = f$.

(b) Uniqueness: If also $\tilde{f}\colon G/N \to H$ satisfies $\tilde{f} \circ \nu = f$, then $\tilde{f}(aN) = (\tilde{f} \circ \nu)(a) = (\overline{f} \circ \nu)(a) = \overline{f}(aN)$, for all $a \in G$. Thus $\tilde{f} = \overline{f}$.

(c) For all $a \in G$ we have

$$aN \in \ker(\overline{f}) \iff \overline{f}(aN) = 1 \iff f(a) = 1 \iff a \in \ker(f)\,.$$

Therefore, $\ker(\overline{f}) = \{aN \in G/N \mid a \in \ker(f)\} = \ker(f)/N$.

Finally, $\operatorname{im}(\overline{f}) = \{\overline{f}(aN) \mid a \in G\} = \{f(a) \mid a \in G\} = \operatorname{im}(f)$. $\square$.

3.5 Remark (a) Assume the notation of Theorem 3.4. Note that $\nu\colon G \to G/N$ has the property that $N \leqslant \ker(f)$, or equivalently that $\nu(N) = \{1\}$. The homomorphism ν is *universal with this property* in the sense that every other homomorphism $f\colon G \to H$ with the property $f(N) = \{1\}$ can be factored in a unique way through ν.

(b) In the situation of Theorem 3.4 we also say that f *induces* the homomorphism $\overline{f}$.

3.6 Corollary *Let $f\colon G \to H$ be a homomorphism. Then f induces an isomorphism $\overline{f}\colon G/\ker(f) \xrightarrow{\sim} \mathrm{im}(f)$. If f is an epimorphism then $G/\ker(f) \cong H$.*

Proof This follows immediately from Theorem 3.4, choosing $N := \ker(f)$. Note that $\overline{f}$ is injective, since $\ker(\overline{f}) = \ker(f)/\ker(f) = \{\ker(f)\} = \{1_{G/\ker(f)}\}$ is the trivial subgroup of $G/\ker(f)$. □

3.7 Example For $n \geqslant 2$, the sign homomorphism $\mathrm{sgn}\colon \mathrm{Sym}(n) \to \{\pm 1\}$ is surjective with kernel $\mathrm{Alt}(n)$. By the Fundamental Theorem of Homomorphisms, we obtain an isomorphism $\mathrm{Sym}(n)/\mathrm{Alt}(n) \cong \{\pm 1\}$. In particular, $[\mathrm{Sym}(n) : \mathrm{Alt}(n)] = 2$ and $|\mathrm{Alt}(n)| = n!/2$ by Lagrange's Theorem, Corollary 2.19.

Before we state the next theorem, note that the additive groups $\mathbb{Z}$ and $\mathbb{Z}/n\mathbb{Z}$ (for $n \in \mathbb{N}$) are cyclic, generated by 1 and $1 + n\mathbb{Z}$, respectively. The next theorem shows that, up to isomorphism, there are no other cyclic groups.

3.8 Theorem (Classification of cyclic groups) *Let G be a cyclic group generated by the element $g \in G$.*

(a) *If G is infinite then $G \cong \mathbb{Z}$, $G = \{g^k \mid k \in \mathbb{Z}\}$ and, for all $i, j \in \mathbb{Z}$, one has $g^i = g^j$ if and only if $i = j$.*

(b) *If G is of finite order n then $G \cong \mathbb{Z}/n\mathbb{Z}$, $G = \{1, g, g^2, \ldots, g^{n-1}\}$ and, for all $i, j \in \mathbb{Z}$, one has $g^i = g^j$ if and only if $i \equiv j \mod n$.*

Proof We consider the function $f\colon \mathbb{Z} \to G$, $k \mapsto g^k$. It is a homomorphism, since $g^k g^l = g^{k+l}$ for all $k, l \in \mathbb{Z}$. We have $G = \langle g \rangle = \{g^k \mid k \in \mathbb{Z}\}$ which implies that f is an epimorphism. By Theorem 2.12 we have $\ker(f) = n\mathbb{Z}$ for some $n \in \mathbb{N}_0$. By Theorem 3.4 we obtain an isomorphism $\overline{f}\colon \mathbb{Z}/n\mathbb{Z} \to G$, $k + n\mathbb{Z} \mapsto g^k$. This implies that G is infinite if and only if $n = 0$. Now all the assertions follow from considering the isomorphism $\overline{f}$. □

3.9 Theorem (Fermat, 1601–1665) *Let G be a finite group, let $g \in G$ and let $k \in \mathbb{Z}$. Then $g^k = 1$ if and only if $|\langle g \rangle|$ divides k. In particular, $g^{|G|} = 1$.*

Proof Since G is finite, the order of $\langle g \rangle$ is finite. Applying Theorem 3.8(b) to the cyclic group $\langle g \rangle$, we obtain

$$g^k = 1 \iff g^k = g^0 \iff k \equiv 0 \mod |\langle g \rangle| \iff |\langle g \rangle| \text{ divides } k\,.$$

□

3.10 Definition Let G be a group and let $g \in G$. One calls $|\langle g \rangle| \in \mathbb{N} \cup \{\infty\}$ the *order* of g and denotes it by $o(g)$. If $o(g)$ is finite then, by Theorem 3.9, we have $o(g) = \min\{n \in \mathbb{N} \mid g^n = 1\}$, and if also $|G|$ is finite then $o(g)$ divides $|G|$ (by Lagrange).

3.11 Theorem (1st Isomorphism Theorem) *Let G be a group and let $N, H \leqslant G$ be subgroups such that $H \leqslant N_G(N)$ (this is satisfied for instance if $N \trianglelefteq G$). Then*

$$HN = NH \leqslant G\,, \quad N \trianglelefteq HN\,, \quad H \cap N \trianglelefteq H$$

and

$$H/H \cap N \to HN/N\,, \quad h(H \cap N) \mapsto hN\,,$$

is an isomorphism.

Proof For all $h \in H$ and $n \in N$ we have $hn = (hnh^{-1})h \in NH$ and $nh = h(h^{-1}nh) \in HN$, since $H \leqslant N_G(N)$. Thus, $HN = NH$. By Examples 2.11(e), HN is a subgroup of G. Moreover, for $n \in N$ and $h \in H$ we have $nhN(nh)^{-1} = nhNh^{-1}n^{-1} = nNn^{-1} = N$, since $h \in N_G(N)$. Thus $N \trianglelefteq NH$. The composition of the inclusion $H \subseteq HN$ and the natural epimorphism $HN \to HN/N$ is a homomorphism $f\colon H \to HN/N$, $h \mapsto hN$. It is surjective, since $hnN = hN = f(h)$ for all $h \in H$ and $n \in N$. Its kernel is $H \cap N$. Thus, $H \cap N \trianglelefteq H$, and, by Corollary 3.6, f induces an isomorphism $\overline{f}\colon H/H \cap N \to HN/N$, $h(H \cap N) \mapsto hN$. □

3.12 Theorem (Correspondence Theorem and 2nd Isomorphism Theorem) *Let G be a group, let $N \trianglelefteq G$ and let $\nu\colon G \to G/N$ denote the canonical epimorphism. The function*

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

is a bijection with inverse $\Psi\colon X \mapsto \nu^{-1}(X)$. For subgroups H, H_1 and H_2 of G which contain N one has:

$$H_1 \leqslant H_2 \iff H_1/N \leqslant H_2/N \quad \textit{and} \quad H \trianglelefteq G \iff H/N \trianglelefteq G/N\,.$$

Moreover, if $N \leqslant H \trianglelefteq G$ then $(G/N)/(H/N) \cong G/H$.

Proof Since images and preimages of subgroups are again subgroups (see Examples 2.11(g) applied to ν), the maps Φ and Ψ have values in the indicated sets and obviously respect inclusions. In fact, in regards to the map Ψ, note that $N = \ker(\nu) = \nu^{-1}(\{1\})$ is contained in $\nu^{-1}(X)$ for every subgroup X of G/N. For every $N \leqslant H \leqslant G$ we have $\nu^{-1}(\nu(H)) = H$, since $N \leqslant H$ (see also Exercise 6). And for every $X \leqslant G/N$ we have $\nu(\nu^{-1}(X)) = X$, since ν is surjective (see also Exercise 6). Thus, Φ and Ψ are inverse bijections.

The statement concerning H_1 and H_2 now follows immediately, since $H_1 \leqslant H_2 \leqslant G$ implies $\nu(H_1) \leqslant \nu(H_2)$ and $X_1 \leqslant X_2 \leqslant G/N$ implies $\nu^{-1}(X_1) \leqslant \nu^{-1}(X_2)$. Moreover, for $N \leqslant H \leqslant G$, $h \in H$ and $g \in G$ we have

$$ghg^{-1} \in H \iff ghg^{-1}N \in H/N \iff (gN)(hN)(g^{-1}N) \in H/N\,.$$

This shows that $N_G(H)/N = N_{G/N}(H/N)$. In particular, H is normal in G if and only if H/N is normal in G/N. Finally, for $N \leqslant H \trianglelefteq G$, the composition $f\colon G \to (G/N)/(H/N)$ of the two canonical epimorphisms $G \to G/N$ and $G/N \to (G/N)/(H/N)$ is an epimorphism with kernel H. Now, Corollary 3.6 induces an isomorphism $\overline{f}\colon G/H \to (G/N)/(H/N)$. □

3.13 Proposition *Every subgroup and factor group of a cyclic group is cylic.*

Proof Let G be a cyclic group generated by $g \in G$. If $N \trianglelefteq G$ then G/N is generated by gN. To prove that subgroups of G are again cyclic, we may assume that $G = \mathbb{Z}$ or $G = \mathbb{Z}/n\mathbb{Z}$ for $n \in \mathbb{N}$, using Theorem 3.8 and Exercise 5. In the first case ($G = \mathbb{Z}$), by Theorem 2.12, subgroups of $\mathbb{Z}$ are of the form $k\mathbb{Z}$, $k \in \mathbb{Z}$, and $k\mathbb{Z}$ is cyclic, generated by k. Now consider the second case $G = \mathbb{Z}/n\mathbb{Z}$ with $n \in \mathbb{N}$. By the Correspondence Theorem, subgroups of $\mathbb{Z}/n\mathbb{Z}$ are of the form $k\mathbb{Z}/n\mathbb{Z}$ with $n\mathbb{Z} \leqslant k\mathbb{Z} \leqslant \mathbb{Z}$. But $k\mathbb{Z}$ is cyclic and, by the initial argument of the proof, with $k\mathbb{Z}$ also every factor group of $k\mathbb{Z}$ is cyclic. □

Exercises

1. Let M and N be normal subgroups of a group G. Show that also $M \cap N$ and MN are normal subgroups of G.

2. Let G be a group and let X be a subset of G. Show that $C_G(X) \trianglelefteq N_G(X)$.

3. Let G be a group. Show that $Z(G)$ and G' are characteristic subgroups of G.

4. (a) Let G be a group, let N be a normal subgroup of G, and let $\nu\colon G \to G/N$, $g \mapsto gN$, denote the natural epimorphism. Show that, for every group H, the function

$$\mathrm{Hom}(G/N, H) \mapsto \{f \in \mathrm{Hom}(G, H) \mid N \leqslant \ker(f)\}\,, \quad \alpha \mapsto \alpha \circ \nu\,,$$

is bijective.

(b) Let G be a group and let A be an abelian group. Let $\nu\colon G \to G^{\mathrm{ab}} := G/G'$ denote the canonical epimorphism. Show that, with the group structure from Exercise 2.9 on the homomorphism sets, the map

$$\mathrm{Hom}(G^{\mathrm{ab}}, A) \to \mathrm{Hom}(G, A)\,, \quad \alpha \mapsto \alpha \circ \nu\,,$$

is a group isomorphism.

5. Let G and H be groups and let $f\colon G \to H$ be an isomorphism. Moreover, let $N \trianglelefteq G$ and set $M := f(N)$. Show that M is normal in H and that $G/N \cong H/M$.

6. (a) Let $f\colon G \to H$ be a group homomorphism and let $U \leqslant G$ and $V \leqslant H$ be subgroups. Show that

$$f^{-1}(f(U)) = U\ker(f) \quad \text{and} \quad f(f^{-1}(V)) = V \cap \mathrm{im}(f)\,.$$

(b) Let G be a group, let $N \trianglelefteq G$ and let $\nu\colon G \to G/N$ denote the canonical epimorphism. Show that for every subgroup U of G one has $\nu(U) = UN/N$.

7. Let G be a group. Show that:

(a) $H \underset{\text{char}}{\trianglelefteq} G \Rightarrow H \trianglelefteq G$.

(b) $M \underset{\text{char}}{\trianglelefteq} N \underset{\text{char}}{\trianglelefteq} G \Rightarrow M \underset{\text{char}}{\trianglelefteq} G$.

(c) $M \underset{\text{char}}{\trianglelefteq} N \trianglelefteq G \Rightarrow M \trianglelefteq G$.

(d) $M \trianglelefteq N \trianglelefteq G \not\Rightarrow M \trianglelefteq G$. (Give a counterexample.)

8. Let G be a cyclic group of order n and let $m \in \mathbb{N}$ be a divisor of n. Show that G has precisely one subgroup of order m.

9. (Butterfly Lemma or Zassenhaus Lemma or 3rd Isomorphism Theorem) Let U and V be subgroups of a group G and let $U_0 \trianglelefteq U$ and $V_0 \trianglelefteq V$. Show that

$$U_0(U \cap V_0) \trianglelefteq U_0(U \cap V)\,, \quad (U_0 \cap V)V_0 \trianglelefteq (U \cap V)V_0\,, \quad (U_0 \cap V)(U \cap V_0) \trianglelefteq U \cap V$$

and

$$U_0(U \cap V)/U_0(U \cap V_0) \cong (U \cap V)/(U_0 \cap V)(U \cap V_0) \cong (U \cap V)V_0/(U_0 \cap V)V_0\,.$$

To see the 'butterfly', draw a diagram of the involved subgroups.

10. Let G be a finite group and let π be a set of primes. An element x of G is called a π-*element* if its order involves only primes from π. It is called a π'-*element* if its order involves only primes outside π.

(a) Let $g \in G$. Assume that we can write $g = xy$ with a π-element $x \in G$ and a π'-element $y \in G$ satisfying $xy = yx$. Show that x and y are powers of g.

(b) Show that for given $g \in G$ there exist unique elements $x, y \in G$ satisfying:

$$x \text{ is a } \pi\text{-element, } y \text{ is a } \pi'\text{-element, } g = xy \text{ and } xy = yx.$$

(The element x is called the π-*part* of g and the element y is called the π'-*part* of g. Notation: $x = g_\pi$, $y = g_{\pi'}$.)

11. Let G and H be groups and let $p_1\colon G \times H \to G$, $(g, h) \mapsto g$, and $p_2\colon G \times H \to H$, $(g, h) \mapsto h$, denote the projection maps. Note that they are epimorphisms. This exercise gives a description of all subgroups of $G \times H$.

(a) Let $X \leqslant G \times H$. Set

$$k_1(X) := \{g \in G \mid (g, s) \in X\} \quad \text{and} \quad k_2(X) := \{h \in H \mid (1, h) \in X\}\,.$$

Let $i \in \{1, 2\}$. Show that $k_i(X) \trianglelefteq p_i(X)$. Moreover, show that the composition $\pi_i\colon X \to p_i(X) \to p_i(X)/k_i(X)$ of the projection map p_i and the natural epimorphism induces an isomorphism $\overline{\pi}_i\colon X/(k_1(X) \times k_2(X)) \overset{\sim}{\to} p_i(X)/k_i(X)$.

(b) Let $K_1 \trianglelefteq P_1 \leqslant G$, let $K_2 \trianglelefteq P_2 \leqslant H$, and let $\eta\colon P_1/K_1 \overset{\sim}{\to} P_2/K_2$ be an isomorphism. Define

$$X := \{(g, h) \in P_1 \times P_2 \mid \eta(gK_1) = hK_2\}\,.$$

Show that X is a subgroup of $G \times H$.

(c) Use the constructions in (a) and (b) to show that the set of subgroups of $G \times H$ is in bijection with the set of all quintuples $(P_1, K_1, \eta, P_2, K_2)$ such that $K_1 \trianglelefteq P_1 \leqslant G$, $K_2 \trianglelefteq P_2 \leqslant H$, and $\eta\colon P_1/K_1 \overset{\sim}{\to} P_2/K_2$ is an isomorphism.

4 Normal and Subnormal Series, Solvable Groups

4.1 Definition A *subnormal series* of a group G is a finite sequence

$$G = G_0 \trianglerighteq G_1 \trianglerighteq G_2 \trianglerighteq \cdots \trianglerighteq G_l = \{1\}\,.$$

If G_i is normal in G for every $i = 1, \ldots, l$ then we call the sequence a *normal series.* The groups G_{i-1}/G_i, $i = 1, \ldots, l$, are called the *factors* and the number l is called the *length* of the subnormal series. A subnormal series is called a *composition series* if each of its factors is simple.

4.2 Examples (a) Not every group has a composition series. For example, $(\mathbb{Z}, +)$ does not have one. In fact, every non-trivial subgroup of $\mathbb{Z}$ is again isomorphic to $\mathbb{Z}$ and therefore not simple. Clearly, however, every finite group has a composition series.

(b) One composition series of $\mathbb{Z}/6\mathbb{Z}$ is

$$\mathbb{Z}/6\mathbb{Z} \triangleright 2\mathbb{Z}/6\mathbb{Z} \triangleright 6\mathbb{Z}/6\mathbb{Z}\,.$$

Its factors are isomorphic to $\mathbb{Z}/2\mathbb{Z}$ and $\mathbb{Z}/3\mathbb{Z}$. Another composition series of $\mathbb{Z}/6\mathbb{Z}$ is

$$\mathbb{Z}/6\mathbb{Z} \triangleright 3\mathbb{Z}/6\mathbb{Z} \triangleright 6\mathbb{Z}/6\mathbb{Z}\,.$$

Its factors are isomorphic to $\mathbb{Z}/3\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z}$.

(c) $\mathrm{Sym}(3) \triangleright \mathrm{Alt}(3) \triangleright \{1\}$ is a composition series of $\mathrm{Sym}(3)$ with factors isomorphic to $\mathbb{Z}/2\mathbb{Z}$ and $\mathbb{Z}/3\mathbb{Z}$.

(d) $\mathrm{Sym}(4) \triangleright \mathrm{Alt}(4) \triangleright V_4 \triangleright \langle(1,2)(3,4)\rangle \triangleright \{1\}$ is a composition series of $\mathrm{Sym}(4)$ with factors isomorphic to $\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z}$.

4.3 Theorem (Jordan-Hölder) *Let G be a group and let*

$$G = G_0 \triangleright G_1 \triangleright G_2 \triangleright \cdots \triangleright G_l = \{1\}\,.$$

and

$$G = H_0 \triangleright H_1 \triangleright H_2 \triangleright \cdots \triangleright H_m = \{1\}\,.$$

be two composition series of G. Then $l = m$ and there exists a permutation $\sigma \in \mathrm{Sym}(l)$ such that $G_{i-1}/G_i \cong H_{\sigma(i)-1}/H_{\sigma(i)}$ for all $i = 1, \ldots .l$.

Proof Induction on $n := \min\{l, m\}$. If $n = 0$ then $G = 1$, $l = m = 0$ and there is nothing to show. If $n = 1$, then G is simple, $l = m = 1$ and all assertions are obviously true. We assume from now on that $n \geqslant 2$ and that all assertions of the theorem hold for $n-1$. Since G/G_1 is simple and since

$$G/G_1 = G_1H_0/G_1 \trianglerighteq G_1H_1/G_1 \trianglerighteq \cdots \trianglerighteq G_1H_m/G_1 = \{1\} \qquad (4.3.a)$$

is a subnormal series of G/G_1 (note that $G_1H_i \trianglelefteq G_1H_{i-1}$ for $i = 1, \ldots, m$) we have $G_1H_{i-1}/G_1 = G/G_1$ and $G_1H_i/G_1 = G_1/G_1$ for a unique $i \in \{1, \ldots, m\}$. This implies

$$H_i \leqslant G_1\,, \quad G_1H_{i-1} = G \quad \text{and} \quad H_{i-1} \nleqslant G_1\,. \qquad (4.3.b)$$

The group homomorphism $\mu\colon H_{i-1} \to G/G_1$, $h \mapsto hG_1$, has image $H_{i-1}G_1/G_1 = G/G_1$. Thus, μ is surjective. Moreover, since $H_i \leqslant G_1$, we obtain $H_i \leqslant \ker(\mu)$ and there exists a surjective group homomorphism $\bar{\mu}\colon H_{i-1}/H_i \to G/G_1$. Since H_{i-1}/H_i is simple and $\ker(\bar{\mu}) \neq H_{i-1}/H_i$ (since $\bar{\mu}$ is surjective), we obtain that $H_i/H_i = \ker(\bar{\mu}) = \ker(\mu)/H_i = (H_{i-1} \cap G_1)/H_i$. Thus, $\bar{\mu}$ is an isomorphism,

$$H_{i-1}/H_i \cong G/G_1 \quad \text{and} \quad H_{i-1} \cap G_1 = H_i\,. \qquad (4.3.c)$$

Note that

$$G_1 \triangleright G_2 \triangleright \cdots \triangleright G_l = \{1\} \qquad (4.3.d)$$

is a composition series of G_1 of length $l-1$. Consider also the following subnormal series of G_1:

$$G_1 = H_0 \cap G_1 \trianglerighteq H_1 \cap G_1 \trianglerighteq \cdots \trianglerighteq H_{i-1} \cap G_1 = H_i \triangleright H_{i+1} \triangleright \cdots \triangleright H_m = \{1\}\,. \qquad (4.3.e)$$

Note that $H_j \cap G_1 \trianglelefteq H_{j-1} \cap G_1$ for $j = 1, \ldots, i-1$, and that $H_{i-1} \cap G_1 = H_i$ by Equation (4.3.c). We claim that

$$H_{j-1} \cap G_1/H_j \cap G_1 \cong H_{j-1}/H_j \quad \text{for } j = 1, \ldots, i-1\,. \qquad (4.3.f)$$

If we can show this claim then the sequence (4.3.e) (with "$= H_i$" omitted) is a composition series of G_1 of length $m-1$ with factors isomorphic to

$$H_0/H_1\,, \ldots\,, H_{i-2}/H_{i-1}\,, H_i/H_{i+1}\,, \ldots\,, H_{m-1}/H_m\,.$$

Comparing this with the composition series (4.3.d) of G_1 of length $l-1$ and using the induction hypothesis together with the isomorphism in (4.3.c) immediately yields the desired result. So it suffices to show (4.3.f). To this end, consider the group homomorphism $\nu\colon H_{j-1}\cap G_1 \to H_{j-1}/H_j$, $x \mapsto xH_j$. Since $\ker(\nu) = H_{j-1}\cap G_1 \cap H_j = H_j \cap G_1$, we obtain a monomorphism

$$\bar{\nu}\colon H_{j-1}\cap G_1/H_j \cap G_1 \to H_{j-1}/H_j\,, \quad x(H_j\cap G_1) \mapsto xH_j\,,$$

with the same image as ν, namely $(H_{j-1}\cap G_1)H_j/H_j$. By Dedekind's identity (see homework) we have $(H_{j-1}\cap G_1)H_j = H_{j-1}\cap G_1H_j$. But, by (4.3.b), we have $G_1H_j \geqslant G_1H_{i-1} = G$ and obtain $(H_{j-1}\cap G_1)H_j = H_{j-1}\cap G = H_{j-1}$. Thus, $\bar{\nu}$ is surjective, the claim (4.3.f) is proved and the theorem holds. □

4.4 Definition Let G be a group which has a composition series. The length of a composition series of G is called the *composition length* of G. It does not depend on the choice of a composition series. The factors of a composition series of G are called the *composition factors* of G. They are uniquely determined by G up to isomorphism and reordering.

4.5 Examples (a) Sym(3) and $\mathbb{Z}/6\mathbb{Z}$ are non-isomorphic groups with the same composition factors, namely $\mathbb{Z}/2\mathbb{Z}$ and $\mathbb{Z}/3\mathbb{Z}$, cf. Examples 4.2.

(b) The composition factors of Sym(4) are $\mathbb{Z}/2\mathbb{Z}$ (with multiplicity 3) and $\mathbb{Z}/3\mathbb{Z}$ (with multiplicity 1), cf. Examples 4.2.

(c) If $2 \leqslant n \in \mathbb{N}$ has prime decomposition $n = p_1^{e_1}\cdots p_r^{e_r}$, then $\mathbb{Z}/n\mathbb{Z}$ has composition factors $\mathbb{Z}/p_1\mathbb{Z}$ (with multiplicity e_1), ..., $\mathbb{Z}/p_r\mathbb{Z}$ (with multiplicity e_r).

4.6 Remark One may think of a finite group as being put together from its composition factors. In this sense, the finite simple groups are the atoms of arbitrary finite groups. The determination of all finite simple groups was one of the largest projects in mathematics. About 50–100 mathematicians were involve and the results cover about 10,000 pages scattered in journals. The project was more or less completed in 1980.

4.7 Definition A group G is called *solvable* if it has a subnormal series with abelian factors.

4.8 Examples (a) Every abelian group G is solvable, since $G \trianglerighteq \{1\}$ is a subnormal series with abelian factors.

(b) The groups Sym(3) and Sym(4) are solvable (by the subnormal series given in Examples 4.2(c) and (d)).

4.9 Theorem *Let G be a finite group. Then G is solvable if and only if every composition factor of G is a cyclic group of prime order.*

Proof $\Leftarrow$: This is obvious, since a cyclic group is abelian.

$\Rightarrow$: We choose a subnormal series of G with abelian factors. After omitting repetitions we can refine it to a composition series of G. The factors of this composition series are isomorphic to factor groups of subgroups of abelian groups and therefore again abelian. It suffices now to show that every finite abelian simple group S is cyclic of prime order. Let $1 \neq s \in S$ be arbitrary. Then the group generated by s is a non-trivial and normal (since S is abelian) subgroup of S. Since S is simple, we obtain $S = \langle s \rangle$ and S is cyclic and isomorphic to $\mathbb{Z}/n\mathbb{Z}$ for some $n \in \mathbb{N}$ with $n > 1$. Let p be a prime factor of n. Then $p\mathbb{Z}/n\mathbb{Z}$ is a proper normal subgroup of the simple group $\mathbb{Z}/n\mathbb{Z}$. This implies that $p\mathbb{Z}/n\mathbb{Z}$ is the trivial group. Thus, $p\mathbb{Z} = n\mathbb{Z}$ and $p = n$. □

4.10 Definition Let G be a group. The *higher derived subgroups* or *higher commutator subgroups* $G^{(i)}$, $i \in \mathbb{N}_0$, of G are recursively defined by

$$G^{(0)} := G\,, \quad G^{(1)} := G'\,, \quad G^{(2)} := (G^{(1)})'\,, \quad \ldots\,, \quad G^{(i+1)} := (G^{(i)})'\,, \quad \ldots$$

4.11 Proposition *Let G be a group and $i \in \mathbb{N}_0$.*

(a) $G^{(i)} \underset{\text{char}}{\trianglelefteq} G$.

(b) *If $H \leqslant G$ then $H^{(i)} \leqslant G^{(i)}$.*

(c) *If $N \trianglelefteq G$ then $(G/N)^{(i)} = G^{(i)}N/N$.*

Proof This is proved by induction on i (Exercise 2). □

4.12 Proposition *A group G is solvable if and only if there exists $s \in \mathbb{N}_0$ with $G^{(s)} = \{1\}$.*

Proof $\Leftarrow$: If $G^{(s)} = 1$ then $G = G^{(0)} \trianglerighteq G^{(1)} \trianglerighteq \cdots \trianglerighteq G^{(s)} = \{1\}$ is a subnormal series of G with abelian factors. Thus, by definition, G is solvable.

$\Rightarrow$: Assume that G is solvable and let $G = G_0 \trianglerighteq G_1 \trianglerighteq \cdots \trianglerighteq G_l = \{1\}$ be a subnormal series with abelian factors. It suffices to show that $G^{(i)} \leqslant G_i$ for $i \in \{0, \ldots, l\}$. But this follows easily by induction on i. In fact, $G^{(0)} = G = G_0$, and if we have shown the statement for $i \in \{0, \ldots, l-1\}$ then we can conclude, by Proposition 4.11(b), that $G^{(i+1)} = (G^{(i)})' \leqslant G_i' \leqslant G_{i+1}$, since G_i/G_{i+1} is abelian, cf. Example 3.3(c). $\square$

4.13 Proposition *Subgroups and factor groups of solvable groups are solvable.*

Proof Let G be solvable. By Proposition 4.12, there exists $s \in \mathbb{N}_0$ with $G^{(s)} = \{1\}$.

If $H \leqslant G$ then, by Proposition 4.11(b), we obtain $H^{(s)} \leqslant G^{(s)} = \{1\}$. Now, Proposition 4.12 implies that H is solvable.

If $N \trianglelefteq G$ then, by Proposition 4.11(c), we obtain $(G/N)^{(s)} = G^{(s)}N/N = N/N = \{1\}$. Again, Proposition 4.12 implies that G/N is solvable. $\square$

4.14 Proposition *Let G be a group and let $N \trianglelefteq G$. If G/N and N are solvable then G is solvable.*

Proof By Proposition 4.12 there exist $r, s \in \mathbb{N}_0$ such that $(G/N)^{(r)} = \{1\}$ and $N^{(s)} = \{1\}$. By Proposition 4.11(c), we obtain $G^{(r)}N/N = \{1\}$ and therefore $G^{(r)} \leqslant N$. Now Proposition 4.11(b) implies $G^{(r+s)} = (G^{(r)})^{(s)} \leqslant N^{(s)} = \{1\}$. By Proposition 4.12, G is solvable. $\square$

4.15 Remark (a) Using representation theory, Burnside showed in 1911 that groups of order $p^a q^b$, where p, q are primes and $a, b \in \mathbb{N}_0$, are solvable.

(b) Feit and Thompson showed in 1963 that groups of odd order are solvable. The proof has 254 pages.

Exercises

1. (a) Show that Alt(4) is the derived subgroup of Sym(4).

(b) Find all composition series of Sym(4).

(c) Determine the higher derived subgroups of Sym(4).

2. Let G be a group and $i \in \mathbb{N}_0$.

(a) Show that $G^{(i)} \underset{\text{char}}{\trianglelefteq} G$.

(b) Show that $H^{(i)} \leqslant G^{(i)}$ for all $H \leqslant G$.

(c) Show that $(G/N)^{(i)} = G^{(i)}N/N$ for all $N \trianglelefteq G$.

3. Show that a group is solvable if and only if it has a normal series with abelian factors.

4. Recall the definition of the group D_8 from Exercise 2.11.

(a) Compute all element orders of D_8.

(b) Find a composition series of D_8 and determine its composition factors.

(c) Determine the higher derived subgroups of D_8.

5. Let Q_8 be the subgroup of $\mathrm{GL}_2(\mathbb{C})$ generated by the matrices

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

(a) Show that $a^4 = 1$, $b^2 = a^2$, $bab^{-1} = a^3$.

(b) Show that Q_8 has order 8 and that $Q_8 = \{a^i b^j \mid 0 \leqslant i \leqslant 3,\ 0 \leqslant j \leqslant 1\}$. The group Q_8 is called the *quaternion group* of order 8.

(c) Determine all the element orders.

(d) Determine all subgroups of Q_8 and their normalizers. Find a composition series of Q_8 and determine its composition factors.

(e) Determine the higher derived subgroups of Q_8.

(f) Show that Q_8 is not isomorphic to D_8 (see Exercise 2.11).

5 Group Actions

5.1 Definition (a) A *(left) action* of a group G on a set X is a map

$$\alpha\colon G\times X\to X\,,\quad (g,x)\mapsto \alpha(g,x)=:{}^{g}x\,,$$

satisfying

(i) ${}^{1}x=x$ for all $x\in X$ and

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

A *(left) G-set* is a set X together with a (left) action α of G on X.

Let X and Y be G-sets and let $f\colon X\to Y$ be a function. We call f a *morphism of G-sets* (or *G-equivariant*) if $f({}^{g}x)={}^{g}f(x)$ for all $g\in G$ and $x\in X$. We call the G-sets X and Y *isomorphic* (notation $X\cong Y$), if there exists a bijective G-equivariant map $f\colon X\to Y$. In this case, $f^{-1}\colon Y\to X$ is again G-equivariant.

(b) Let X be a G-set. For $x\in X$, the subset

$$\mathrm{stab}_G(x):=G_x:=\{g\in G\mid {}^{g}x=x\}\subseteq G$$

is called the *stabilizer* of x in G. It is easy to verify that G_x is a subgroup of G. The element $x\in X$ is called a *fixed point* if $G_x=G$. Moreover, for an element $x\in X$, the subset

$$[x]_G:=\{\,{}^{g}x\mid g\in G\}\subseteq X$$

is called the *orbit* of x under G. For $x,y\in X$ we write $x\sim y$ if there exists $g\in G$ such that ${}^{g}x=y$. It follows immediately from the axioms (i) and (ii) in (a) that this defines an equivalence relation on X and that the equivalence class containing x is the orbit of x. (Verify!)

(c) Let X be a G-set. The *kernel* of the action $\alpha\colon G\times X\to X$ of G on X is defined as $\{g\in G\mid {}^{g}x=x$ for all $x\in X\}$. It is equal to $\cap_{x\in X}G_x$ and a normal subgroup of G (verify!). The action α and the G-set X are called

(i) *faithful*, if $\ker(\alpha)=\{1\}$,

(ii) *trivial*, if $\ker(\alpha)=G$, and

(ii) *transitive*, if X consists only of one orbit, i.e., for any $x,y\in X$ there exists $g\in G$ such that ${}^{g}x=y$.

5.2 Remark One can also define right actions of a group G on a set X in a similar way and use the notation x^g for $x \in X$ and $g \in G$. It is easy to verify that if one has a right action of G on X then

$$ {}^{g}x := x^{g^{-1}} \quad (g \in G\,, x \in X) $$

defines a left action of G on X. Conversely, if one has a left action of G on X then

$$ x^g := {}^{g^{-1}}x \quad (g \in G\,, x \in X) $$

defines a right action of G on X.

5.3 Examples (a) Let X be any set. $G = \mathrm{Sym}(X)$ acts on X via ${}^{\pi}x := \pi(x)$.

(b) Let G be a group, $H \leqslant G$, and set $X := G/H$. Then G/H is a G-set under the action $\alpha\colon G \times G/H \to G/H$, $(g, aH) \mapsto gaH$. Note that α is well-defined. This action is often called *left translation*.

(c) Let G be a group and $X := G$. Then G acts on X by conjugation: $(g, x) \mapsto c_g(x) = gxg^{-1} =: {}^{g}x$ for $g, x \in G$. We call $x, y \in G$ *conjugate* (under G), if there exists $g \in G$ such that ${}^{g}x = y$. The orbit of $x \in G$ is called the *conjugacy class* of x. The kernel of the conjugation action of G on G is $Z(G)$, and $\mathrm{stab}_G(x) = G_x = C_G(x)$. Similarly, G acts by conjugation on the set of subsets of G. If Y is any subset of G and $g \in G$, then by ${}^{g}Y$ we usually mean $c_g(Y) = gYg^{-1}$. One has $\mathrm{stab}_G(Y) = N_G(Y)$, the normalizer of Y.

(d) Let G be a group and let X be the set of subgroups of G. Then G acts on X by conjugation: $(g, H) \mapsto {}^{g}H := gHg^{-1}$. The orbit of $H \leqslant G$ is called the *conjugacy class* of H. The stabilizer of H is $N_G(H)$. We have $H \trianglelefteq G \iff N_G(H) = G \iff H$ is a fixed point.

5.4 Proposition *Let X be a G-set.*

(a) *For every $g \in G$, the map $\pi_g\colon X \to X$, $x \mapsto {}^{g}x$, is bijective, i.e., $\pi_g \in \mathrm{Sym}(X)$.*

(b) *The map $\rho\colon G \to \mathrm{Sym}(X)$, $g \mapsto \pi_g$, is a group homomorphism. It is called the* permutation representation *of G associated with the G-set X.*

(c) *The kernel of the action of G on X is equal to* $\ker(\rho)$.

Proof For $g, h \in G$ and $x \in X$ we have $(\pi_g \circ \pi_h)(x) = {}^{g}({}^{h}x) = {}^{(gh)}x = \pi_{gh}(x)$ and $\pi_1(x) = {}^{1}x = x$. Thus,

$$ \pi_g \circ \pi_h = \pi_{gh} \quad \text{and} \quad \pi_1 = \mathrm{id}_X\,. $$

This implies $\pi_g \circ \pi_{g^{-1}} = \pi_1 = \mathrm{id}_X = \pi_1 = \pi_{g^{-1}} \circ \pi_g$, showing (a). Moreover the equation $\pi_g \circ \pi_h = \pi_{gh}$ shows (b). Finally, an element $g \in G$ is in the kernel of the action of G on X if and only if ${}^g x = x$ for all $x \in X$. This happens if and only if $\pi_g(x) = x$ for all $x \in X$, which in turn is equivalent to $\pi_g = \mathrm{id}_X$ and to $g \in \ker(\rho)$. □

5.5 Remark (a) Conversely, assume that G is a group, X is a set, and $\rho\colon G \to \mathrm{Sym}(X)$ is a homomorphism. Then

$${}^g x := (\rho(g))(x)\,,$$

for $g \in G$ and $x \in X$, definies an action of G on X. This construction is inverse to the construction in Proposition 5.4. (Verify!)

(b) Let X be a G-set and $x \in X$. Then $\mathrm{stab}_G({}^g x) = {}^g\mathrm{stab}_G(x)$ $(= g \cdot \mathrm{stab}_G(x) \cdot g^{-1})$. (Verify!)

(c) Every orbit of X is a transitive G-set in its own right and X is the disjoint union of its orbits.

5.6 Theorem (Cayley) *Every group G is isomorphic to a subgroup of a symmetric group. If G is finite of order n then G is isomorphic to a subgroup of* $\mathrm{Sym}(n)$.

Proof G acts on $X := G$ (by left translation) via $G \times X \to X$, $(g, x) \mapsto gx$. By Proposition 5.4, we obtain a group homomorphism $\rho\colon G \to \mathrm{Sym}(X)$, $g \mapsto \pi_g$, with $\pi_g(x) := gx$, for $g \in G$ and $x \in X$. Since $\pi_g = \mathrm{id}_X$ implies $gx = x$ for all $x \in X$, we obtain that $\ker(\rho) = 1$ so that ρ is injective and induces an isomorphism $G \cong \mathrm{im}(\rho) \leqslant \mathrm{Sym}(X)$. Finally, note that if $f\colon X_1 \to X_2$ is a bijection between two sets then $\mathrm{Sym}(X_1) \to \mathrm{Sym}(X_2)$, $\pi \mapsto f \circ \pi \circ f^{-1}$, is a group isomorphism. Thus, if X has n elements then $\mathrm{Sym}(X) \cong \mathrm{Sym}(n)$ and the proof is complete. □

5.7 Theorem *Let G be a group and let X be a G-set.*

(a) *For each $x \in X$, the map*

$$f\colon G/G_x \to [x]_G\,, \quad gG_x \mapsto {}^g x\,,$$

is an isomorphism of G-sets. Here, G/G_x is a G-set under left translation (cf. Example 5.3(b)).

(b) *Let $\mathcal{R} \subseteq X$ be a set of representatives for the orbits of X under G (i.e., $\mathcal{R}$ contains precisely one element from each orbit). Then one has the* orbit equation:

$$|X| = \sum_{x \in \mathcal{R}} [G : G_x]\,,$$

with the usual rules for '∞'. In particular, if X is a transitive G-set, then $|X| = [G : G_x]$ for any element $x \in X$.

Proof (a) The function f is well-defined, since for $g \in G$ and $h \in G_x$ one has ${}^{gh}x = {}^{g}x$. By the definition of $[x]_G$ the function f is surjective. It is G-equivariant, since

$$f({}^{g_1}(g_2G_x)) = f(g_1g_2G_x) = {}^{(g_1g_2)}x = {}^{g_1}({}^{g_2}x) = {}^{g_1}f(g_2G_x)\,.$$

Finally, f is injective: If $g_1, g_2 \in G$ satisfy $f(g_1G_x) = f(g_2G_x)$ then ${}^{g_1}x = {}^{g_2}x$ and ${}^{g_2^{-1}g_1}x = x$ so that $g_2^{-1}g_1 \in G_x$ and $g_1G_x = g_2G_x$.

(b) The cardinality $|X|$ is equal to $\sum_{x\in\mathcal{R}} |[x]_G|$, since X is the disjoint union of its orbits, see Remark 5.5(c). Moreover, each orbit $[x]_G$ is a transitive G-set and by part (a) we have $|[x]_G| = |G/G_x| = [G : G_x]$. □

5.8 Remark Part (a) of the previous theorem shows that every transitive G-set X is isomorphic to G/H with $H = G_x$ for any $x \in X$. Moreover, it is easy to see that, for any subgroups H and K of G, one has $G/H \cong G/K$ as G-sets if and only if H and K are G-conjugate (see Exercise 1).

5.9 Example Assume that G acts on itself by conjugation. Then $G_x = C_G(x)$ and the orbit equation becomes

$$|G| = \sum_{x\in\mathcal{R}} [G : C_G(x)]\,,$$

where $\mathcal{R} \subseteq G$ is a set of representatives of the conjugacy classes of G. Moreover, for every $x \in G$ we have:

$$x \text{ is a fixed point } \iff G = C_G(x) \iff x \in Z(G)\,.$$

Thus, $Z(G) \subseteq \mathcal{R}$.

5.10 Theorem *Let p be a prime and let G be a group of order p^k with $k \in \mathbb{N}$. Then $|Z(G)| > 1$. Moreover, G is solvable.*

Proof The orbit equation from Example 5.9 yields

$$0 \equiv |G| = \sum_{x \in \mathcal{R}} [G : C_G(x)] \equiv |Z(G)| \mod p\,.$$

since $[G : C_G(x)]$ is divisible by p if $x \notin Z(G)$. Therefore, p divides $|Z(G)|$. Together with $|Z(G)| \geqslant 1$ this proves that $|Z(G)| > 1$. Since $Z(G)$ is abelian and normal in G, Proposition 4.14 and an easy induction on $|G|$ implies that G is solvable. □

5.11 Definition Groups of order p^k for a prime p and $k \in \mathbb{N}_0$ are called p-groups. A subgroup H of an arbitrary group G is called a *p-subgroup* if H is a p-group. If G is finite and $P \leqslant G$ is a p-subgroup such that p does not divide $[G : P]$ then P is called a *Sylow p-subgroup* of G. An element of G which has order p^l for some $l \in \mathbb{N}_0$ is called a *p-element.*

5.12 Theorem (Sylow, 1832–1918) *Let p be a prime and let G be a finite group of order $n = p^a m$ with $a \in \mathbb{N}_0$, $m \in \mathbb{N}$, $p \nmid m$.*

(a) *For every $b \in \{0, 1, \ldots, a\}$, the number $n_G(p^b)$ of subgroups of G of order p^b satisfies the congruence*

$$n_G(p^b) \equiv 1 \mod p\,.$$

In particular, G has a subgroup of order p^b for every $b = 0, \ldots, a$.

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

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

Proof (a) The statement is cleary true for $b = 0$. So fix $b \in \{1, 2, \ldots, a\}$ and set

$$\Omega := \{X \subseteq G \mid |X| = p^b\}\,.$$

Then $|\Omega| = \binom{n}{p^b}$. G acts on Ω by left translation: $(g, X) \mapsto gX$. Let $\mathcal{R} \subseteq \Omega$ be a set of representatives of the G-orbits of Ω. The orbit equation yields:

$$\binom{n}{p^b} = |\Omega| = \sum_{X \in \mathcal{R}} [G : G_X]\,. \qquad (5.12.a)$$

Claim 1: For every $X \in \mathcal{R}$ one has $|G_X| \mid p^b$. *Proof:* Since $G_X = \{g \in G \mid gX = X\}$, we have $G_X X = X$ and G_X acts on X by translation. But each orbit of this action has length $|G_X|$, since $gx = g'x$ implies $g = g'$ for all $x \in X$ and $g, g' \in G_X$. Thus $|X| = p^b$ equals $|G_X|$ multiplied by the number of orbits.

Claim 2: If $|G_X| = p^b$ then the G-orbit of $X \in \Omega$ contains a subgroup of G. *Proof:* Since $|G_X| = p^b$, G_X acts transitively on X and we have $X = G_X x$ for some $x \in X$. Thus, $x^{-1}X = x^{-1}G_X x$ is a subgroup of G in the G-orbit of X.

Claim 3: If the G-orbit of $X \in \Omega$ contains a subgroup U of G then this orbit equals G/U, and in particular, $[G : G_X] = [G : U] = p^{a-b}m$, $|G_X| = p^b$ and U is the only subgroup in this orbit. *Proof:* The orbit of X equals the orbit of U which is G/U. If $gU \in G/U$ is a subgroup of G then $1 \in gU$ and $gU = U$. The remaining statements clearly hold.

Claim 4: One has

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

Proof: We use the orbit equation (5.12.a). Let $X \in \mathcal{R}$. If the orbit of X contains no subgroup of G then by Claims 1 and 2 we have $|G_X| \mid p^{b-1}$ and consequently $[G : G_X] \equiv 0 \mod p^{a-b+1}m$. If the orbit of X contains a subgroup of G then it contains exactly one subgroup and $[G : G_X] = p^{a-b}m$ by Claim 3. This proves Claim 4.

Claim 5: One has $n_G(p^b) \equiv 1 \mod p$. *Proof:* Let H be an arbitrary group of order $n = |G|$. Then, by Claim 4 for H, we have

$$p^{a-b}m \cdot n_H(p^b) \equiv \binom{n}{p^b} \equiv p^{a-b}m \cdot n_G(p^b) \mod p^{a-b+1}$$

and this implies

$$n_H(p^b) \equiv n_G(p^b) \mod p$$

Using $H = \mathbb{Z}/n\mathbb{Z}$ and noting that $n_H(p^b) = 1$ (Homework), we obtain $n_G(p^b) \equiv 1 \mod p$.

(b) Assume that U is a p-subgroup of G and that P is a Sylow p-subgroup of G. Consider the set $\Gamma := \{gPg^{-1} \mid g \in G\}$ and note that it is a transitive G-set under conjugation. The stabilizer of P is $N_G(P)$ and since $P \leqslant N_G(P)$ we obtain $|\Gamma| = [G : N_G(P)] \mid [G : P] = m$. Thus, p does not divide $|\Gamma|$. With G also U acts on Γ by conjugation. Let $\mathcal{S}$ denote a set of representatives for the U-orbits of Γ. By the orbit equation we have $|\Gamma| = \sum_{Q\in\mathcal{S}}[U : U_Q]$. Since

U is a p-group and since $|\Gamma|$ is not divisible by p, there exists $Q \in \mathcal{S}$ such that $[U : U_Q] = 1$, or equivalently such that $U \leqslant N_G(Q)$. This implies that UQ is a subgroup of G. Since $|UQ| = |U| \cdot |Q|/|U \cap Q|$, UQ is a p-subgroup of G and it contains the subgroup Q of order $|P| = p^a$. By Lagrange we obtain $UQ = Q$, and then $U \leqslant Q$. This proves (b).

(c) If U, in the proof of Part (b), is a Sylow p-subgroup of G it follows that $U = Q$ and that U is conjugate to P. □

5.13 Remark Let G be a finite group, let p be a prime. We will denote the set of Sylow p-subgroups of G by $\mathrm{Syl}_p(G)$. By Sylow's Theorem, $\mathrm{Syl}_p(G)$ is a transitive G-set under conjugation. If $P \in \mathrm{Syl}_p(G)$, the orbit equation implies

$$|\mathrm{Syl}_p(G)| = [G : N_G(P)] \,.$$

Since $P \leqslant N_G(P)$, this implies that $n_G(p^a) = |\mathrm{Syl}_p(G)|$ divides $[G : P] = m$ (in the notation of Sylow's Theorem). Thus we have the two fundamental conditions

$$|\mathrm{Syl}_p(G)| \equiv 1 \mod p \quad \text{and} \quad |\mathrm{Syl}_p(G)| \mid m \,.$$

Moreover, since $|\mathrm{Syl}_p(G)| = [G : N_G(P)]$, we also have: P is normal in G if and only if P is the only Sylow p-subgroup, i.e., if $\mathrm{Syl}_p(G) = \{P\}$.

5.14 Theorem (Cauchy 1789–1857) *Let G be a finite group and let p be a prime divisor of $|G|$. Then G has an element of order p.*

Proof By Sylow's Theorem 5.12(a), G has a subgroup of order p. This subgroup must be cyclic and every generator of it has order p. □

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

Proof From Theorem 5.10 we know that every p-group is solvable. So we may assume that $p \neq q$.

(a) Assume that $|G| = pq$ and that $p > q$. By Sylow's Theorem we have $n_G(p) \equiv 1 \mod p$ and $n_G(p) \mid q$. This implies $n_G(p) = 1$. Thus, G has only one Sylow p-subgroup P and it is normal in G. Therefore, $1 \triangleleft P \triangleleft G$ is a subnormal series and it has abelian factors.

(b) Assume that $|G| = p^2q$. By Remark 5.13 we have $n_G(p^2) \in \{1, q\}$ and $n_G(q) \in \{1, p, p^2\}$. If $n_G(p^2) = 1$ or $n_G(q) = 1$ then G is has a normal Sylow

p-subgroup or a normal Sylow q-subgroup and Proposition 4.14 together with Theorem 5.10 implies that G is solvable.

From now on we assume that $n_G(p^2) = q$ and $n_G(q) \in \{p, p^2\}$ and show that this leads to a contradiction. By Sylow's Theorem, $q \equiv 1 \mod p$. Thus, $p \mid q-1$, $p < q$, $q \nmid p-1$, and by Sylow's Theorem we obtain $n_G(q) \neq p$. Therefore, we obtain that $n_G(q) = p^2$. Since the intersection of two distinct subgroups of G of order q is the trivial subgroup, the number of elements of order q of G is equal to $n_G(q)(q-1) = p^2(q-1) = |G| - p^2$. Since no element of order q can be contained in a Sylow p-subgroup of G we obtain that G can have only one Sylow p-subgroup. But this contradicts our assumption that $n_G(p^2) = q$. $\square$

Exercises

1. Let G be a group and let H and K be subgroups of G.

(a) Show that there if $f\colon G/H \to G/K$ is a G-equivariant map then there exists $g \in G$ with $H \leqslant gKg^{-1}$.

(b) Show that G/H and G/K are isomorphic G-sets if and only if H and K are conjugate subgroups.

(c) Compute the stabilizer of gH (for $g \in G$) under the left translation action of G on G/H.

2. Let G be a p-group for a prime p and let N be a non-trivial normal subgroup of G. Show that $N \cap Z(G) > \{1\}$.

3. (a) Let G be a group such that $G/Z(G)$ is cyclic. Show that G is abelian.

(b) Show that if a group G has order p^2, for some prime p, then G is abelian.

4. (a) Show that every non-abelian group of order 6 is isomorphic to Sym(3).

(b) Show that every abelian group of order 6 is isomorphic to $\mathbb{Z}/6\mathbb{Z}$.

(c) Show that every group of order 4 is isomorphic to $Z/4\mathbb{Z}$ or to the Klein 4-group V_4.

5. (Frattini Argument) Let G be a finite group, p a prime, $H \trianglelefteq G$ and $P \in \mathrm{Syl}_p(H)$. Show that $G = HN_G(P)$. (Hint: Let $g \in G$ and consider P and gPg^{-1}. Show that both are Sylow p-subgroups of H.)

6. Show that every group of order 1000 is solvable.

7. Let G be a finite group, let p be a prime, let P be a Sylow p-subgroup of G and set $U := N_G(P)$. Show that $N_G(U) = U$.

8. Find the Sylow subgroups of Alt(5) and their normalizers for the primes 2, 3 and 5.

9. What is the minimal $n \in \mathbb{N}$ such that the quaternion group of order 8, Q_8, is isomorphic to a subgroup of Sym(n). (Hint: Show that if Q_8 is isomorphic to a subgroup of Sym(n) then Q_8 acts faithfully on $\{1, \ldots, n\}$. Show that at least one orbit of this action needs to have length 8, by looking at possible element stabilizers. Use Exercise 4.5.)

10. The upper central series

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

of a group G is recursively defined by the equations

$$Z^0(G) = \{1\} \quad \text{and} \quad Z^{i+1}(G)/Z^i(G) = Z(G/Z^i(G)) \text{ for } i \geqslant 0.$$

A group G is called *nilpotent* if there exists $i \in \mathbb{N}$ with $Z^i(G) = G$.

(a) Show that if G is nilpotent then G is also solvable.

(b) Find a group G which is solvable but not nilpotent.

(c) Let p be a prime and let G be a group of order p^k for some $k \in \mathbb{N}_0$. Show that G is nilpotent.

(d) Show that if G is nilpotent and if $H < G$ then $H < N_G(H)$ ("normalizers grow"). (Hint: Let $i \in \mathbb{N}_0$ be maximal with $Z^i(G) \leqslant H$. Show that $H < Z^{i+1}(G)H \leqslant N_G(H)$.)

6 Symmetric and Alternating Groups

6.1 Definition Let $n \in \mathbb{N}$ and $\sigma \in \mathrm{Sym}(n)$. σ is called a *k-cycle* ($k \in \mathbb{N}$) or a cycle of *length* k, if there exist pairwise distinct element $a_1, \ldots, a_k \in \{1, \ldots, n\}$ such that $\sigma(a_1) = a_2$, $\sigma(a_2) = a_3$, …, $\sigma(a_k) = a_1$, and $\sigma(a) = a$ for all $a \in \{1, \ldots, n\} \smallsetminus \{a_1, \ldots, a_k\}$. In this case we write $\sigma = (a_1, \ldots, a_k)$. If $k = 2$, then σ is called a *transposition.* Two cycles $(a_1, \ldots, a_k)$ and $(b_1, \ldots, b_l)$ are called *disjoint* if $\{a_1, \ldots, a_k\} \cap \{b_1, \ldots, b_l\} = \emptyset$.

6.2 Remark (a) Elements of $\mathrm{Sym}(n)$ are functions $\{1, \ldots, n\} \to \{1, \ldots, n\}$. The binary operation on $\mathrm{Sym}(n)$ is given by composition: $\sigma\tau$ means "first apply τ, then σ". (Warning: Some books or computer programs write functions from the right and have the opposite convention: $\sigma\tau$ there means "first apply σ, then τ".)

(b) $(a_1, a_2, \ldots, a_k) = (a_2, a_3, \ldots, a_k, a_1) = \cdots$.

(c) $(a_1, a_2, \ldots, a_k)^{-1} = (a_k, a_{k-1}, \ldots, a_1)$.

(d) If $\sigma = (a_1, a_2, \ldots, a_k)$ and $\tau = (b_1, \ldots, b_l)$ are disjoint cycles, then $\sigma\tau = \tau\sigma$.

(e) Every element $\sigma \in \mathrm{Sym}(n)$ can be written as a product of disjoint cycles (See Exercise 2.2). Usually one omits cycles (a_1) of length 1, because they are the identity. But let us include all these cycles for the following consideration. Then the occurring cycles form precisely the $\langle\sigma\rangle$-orbits of $\{1, \ldots, n\}$ under the natural action of $\mathrm{Sym}(n)$ on $\{1, \ldots, n\}$ (${}^{\sigma}i := \sigma(i)$). Therefore, the decomposition of σ into disjoint cycles is unique. If we order the cycle lengths $k_1 \geqslant k_2 \geqslant \cdots \geqslant k_r (\geqslant 1)$ then the sequence $(k_1, k_2, \ldots, k_r)$ is called the partition of n corresponding to σ, or the *cycle type* of σ. Note that $k_1 + \cdots + k_r = n$. A *partition* of n is a sequence $(k_1, k_2, \ldots, k_r)$ of elements in $\mathbb{N}$ satisfying $k_1 \geqslant k_2 \geqslant \cdots \geqslant k_r$ and $k_1 + \cdots + k_r = n$. For example,

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

has cycle type $(4, 2, 2, 1)$.

(f) If $\sigma \in \mathrm{Sym}(n)$ has cycle type $(k_1, \ldots, k_r)$ then $o(\sigma) = \mathrm{lcm}(k_1, \ldots, k_r)$ (verify!).

6.3 Proposition *Let $\sigma, \tau \in \mathrm{Sym}(n)$. Then: σ and τ are conjugate $\iff$ σ and τ have the same cycle type.*

Proof It is easy to see (see Exercise 1) that

$$\rho \circ (a_1, \ldots, a_k) \circ \rho^{-1} = (\rho(a_1), \ldots, \rho(a_k)) \tag{6.3.a}$$

for every k-cycle $(a_1, \ldots, a_k)$ and every $\rho \in \mathrm{Sym}(n)$

$\Rightarrow$: Let $\sigma \in \mathrm{Sym}(n)$ and write $\sigma = \sigma_1 \cdots \sigma_r$ as a product of disjoint cycles of lengths $k_1, \ldots, k_r$. Conjugation with any $\rho \in \mathrm{Sym}(n)$ yields again a product $\rho\sigma\rho^{-1} = \rho\sigma_1\rho^{-1} \cdots \rho\sigma_r\rho^{-1}$ of disjoint cycles of lengths $k_1, \ldots, k_r$ by equation (6.3.a).

$\Leftarrow$: Assume that the permutations $\sigma = (a_1, a_2, \ldots, a_{k_1})(b_1, b_2, \ldots, b_{k_2}) \cdots$ and $\tau = (a'_1, \ldots, a'_{k_1})(b'_1, \ldots, b'_{k_2}) \cdots$ have the same cycle type $(k_1, k_2, \ldots, k_r)$. Define $\rho \in \mathrm{Sym}(n)$ by $\rho(a_1) := a'_1$, $\rho(a_2) := a'_2, \ldots$. Then, by equation(6.3.a), we obtain $\rho\sigma\rho^{-1} = \tau$. □

6.4 Remark For each $n \in \mathbb{N}$ one obtains in the above way a bijection between the set of conjugacy classes of $\mathrm{Sym}(n)$ and the set of partitions of n.

6.5 Example The number $n = 5$ has the following partitions: (5), $(4,1)$, $(3,2)$, $(3,1,1)$, $(2,2,1)$, $(2,1,1,1)$, $(1,1,1,1,1)$. Thus, $\mathrm{Sym}(5)$ has seven conjugacy classes.

6.6 Proposition (a) $\mathrm{Sym}(n) = \langle\{(1,2),(2,3),\ldots,(n-1,n)\}\rangle$.

(b) $\mathrm{Sym}(n) = \langle\{(1,2),(1,2,3,\ldots,n)\}\rangle$.

Proof (a) See Exercise 2.2(c).

(b) Set $\sigma := (1,2,\ldots,n)$ and $U := \langle\{(1,2),\sigma\}\rangle$. Then also $(i+1,i+2) = \sigma^i(1,2)\sigma^{-i} \in U$ for all $i = 1,\ldots,n-2$. Thus, $U = \mathrm{Sym}(n)$ by part (a). □

6.7 Theorem *Let $n \in \mathbb{N}$. Then $\mathrm{Alt}(n)$ is solvable if and only if $n \leqslant 4$. And also $\mathrm{Sym}(n)$ is solvable if and only if $n \leqslant 4$.*

Proof Note that $\mathrm{Alt}(n)$ is solvable if and only if $\mathrm{Sym}(n)$ is solvable by Propositions 4.13 and 4.14.

As for $\mathrm{Alt}(n)$, we already have seen that $\mathrm{Alt}(n)$ is solvable for $n \leqslant 4$. Now let $n \geqslant 5$. Define $U \leqslant \mathrm{Alt}(n)$ as the subgroup generated by all 3-cylces. Let $i, j, k, l.m \in \{1, \ldots, n\}$ be 5 pairwise distinct elements. Then

$$[(i,j,l),(i,k,m)] = (i,j,l)(i,k,m)(i,l,j)(i,m,k) = (i,j,k)\,,$$

showing that $U = U'$. This implies that U is not solvable, by Proposition 4.12 and then also that $\mathrm{Alt}(n)$ is not solvable, by Theorem 4.13. $\square$

6.8 Remark It is not difficult to prove that $\mathrm{Alt}(n)$ is a simple group for $n \geqslant 5$. It is also not difficult to show that $\mathrm{Alt}(n)$ is generated by its 3-cycles, even by 3-cycles of the form $(i, i+1, i+2)$, $i = 1, \ldots, n-2$.

6.9 Definition Let $n \geqslant 3$. The subgroup of $\mathrm{Sym}(n)$ generated by $\sigma = (1, 2, 3, \ldots, n)$ and $\tau = (1, n)(2, n-1) \cdots$ is called the *dihedral group* D_{2n}. One usually extends this definition to $D_4 := V_4$ and $D_2 := \mathbb{Z}/2\mathbb{Z}$.

6.10 Proposition *With the above notation one has for* $n \geqslant 3$*:*

(a) $o(\sigma) = n$, $o(\tau) = 2$ *and* $\tau\sigma\tau = \sigma^{-1}$.

(b) $|D_{2n}| = 2n$ *and* $D_{2n} = \{1, \sigma, \sigma^2, \ldots, \sigma^{n-1}, \tau, \sigma\tau, \sigma^2\tau, \ldots, \sigma^{n-1}\tau\}$.

Proof (a) Easy verification.

(b) Since $o(\sigma) = n$, the elements $1, \sigma, \ldots, \sigma^{n-1}$ are pairwise distinct and form the cyclic subgroup $C := \langle\sigma\rangle$ of D_{2n}. Since σ^{-1} is the only element in C that maps 1 to n, we have $\tau \notin C$. Since $\tau\sigma = \sigma^{n-1}\tau$, and $\tau^2 = 1$, we can see that $G = C \cup C\tau$ and that $[G : C] = 2$. Now all the statements follow immediately. $\square$

6.11 Remark Geometric interpretation of D_{2n}: For a natural number $n \geqslant 3$ consider a regular n-gon with center in the origin of the plane $\mathbb{R}^2$. Denote the vertices of the n-gon by the numbers $1, 2, \ldots, n$ in counterclockwise orientation. From classical geometry we know that there are n rotations and n reflections about an axis passing through the origin that take the n-gon to itself. We also know that the composition of any two such geometric operations is again one of them. So they form a group G of order $2n$ under composition. Each element of the group is a linear automorphism of $\mathbb{R}^2$ which permutes the vertices. This defines an action of G on the set of vertices and therefore gives rise to a homomorphism $f\colon G \to \mathrm{Sym}(n)$. Note that the counterclockwise rotation about the angle $2\pi/n$ is mapped to the permutation $\sigma := (1, 2, 3, \ldots, n)$ and that the reflection about the line that intersects the edge between vertex 1 and n perpendicularly at its center is mapped to $\tau := (1, n)(2, n-1) \cdots$. This implies that $f(G)$ contains D_{2n}. But since $|G| = 2n = |D_{2n}|$, we obtain $f(G) = D_{2n}$ and that f is injective.

So $f\colon G \to D_{2n}$ is an isomorphism. For this reason we also say that D_{2n} is the *symmetry group* of the regular n-gon.

6.12 Proposition *Let G be a finite group, $H \leqslant G$ and $N := \bigcap_{g\in G} gHg^{-1}$. Then $N \trianglelefteq G$ and there exists a monomorphism $G/N \to \mathrm{Sym}(n)$ with $n = [G : H]$.*

Proof G acts on G/H by left translation: $(g, aH) \mapsto gaH$. This gives rise to a group homomorphism $\rho\colon G \to \mathrm{Sym}(G/H) \cong \mathrm{Sym}(n)$. Its kernel is the kernel of the action. But this is equal to the intersection of all the stabilizers of elements of G/H. Obviously, H has stabilizer H and therefore gH has stabilizer gHg^{-1}. It follows that the kernel of the action is $N := \bigcap_{g\in G} gHg^{-1}$. Now the fundamental theorem of homomorphisms implies the statement of the proposition. □

6.13 Theorem *For every odd prime p, there exist (up to isomorphism) exactly 2 groups of order $2p$, namely $\mathbb{Z}/2p\mathbb{Z}$ and D_{2p}.*

Proof Since D_{2p} is not abelian, we have $D_{2p} \not\cong \mathbb{Z}/2p\mathbb{Z}$. It suffices now to show that every non-cyclic group G of order $2p$ is isomorphic to D_{2p}. Let $P = \langle a\rangle \in \mathrm{Syl}_p(G)$ and $Q = \langle b\rangle \in \mathrm{Syl}_2(G)$ be a Sylow p-subgroup and a Sylow 2-subgroup, respectively. Since $[G : P] = 2$, P is normal in G. Moreover, Q is not normal in G (since otherwise $aba^{-1} = b$ implies that the element $ab = ba$ has order $2p$). It is easy to see that $G/Q = \{Q, aQ, a^2Q, \ldots, a^{p-1}Q\}$. Applying Proposition 6.12 and its proof with $H = Q$ and $N = 1$ we obtain a monomorphism $f\colon G \to \mathrm{Sym}(p)$, where we use the above ordering of the elements in G/Q. It is now clear that $f(a) = (1, 2, \ldots, p) \in \mathrm{Sym}(p)$. To compute $f(ba)$ note that every element in $G \smallsetminus P$ has order 2, since G is not cyclic and every element of order 1 and p is contained in P. Therefore, $ba^iba^i = 1$ for all $i = 0, \ldots, p-1$ and $ba^i = a^{p-i}b$. This immediately implies that $f(ba) = (1, p)(2, p-1)\cdots$ so that $f(G)$ contains D_{2p}. Comparing orders, we obtain $f(G) = D_{2p}$ and $f\colon G \to D_{2p}$ is an isomorphism. □

Exercises

1. Show that for every cycle $(a_1, \ldots, a_k)$ in $\mathrm{Sym}(n)$ and every $\sigma \in \mathrm{Sym}(n)$ one has

$$\sigma \circ (a_1, \ldots, a_k) \circ \sigma^{-1} = (\sigma(a_1), \sigma(a_2), \ldots, \sigma(a_k))\,.$$

2. Let $p \neq q$ be two primes and let G be a group of order p^2q^2. Show that G is solvable. (Hint: You may assume that $p > q$. Consider the possibilities for $n_G(p^2)$. The difficult case is when $n_G(p^2) = q^2$. In this case, let $P \neq Q$ be Sylow p-subgroups of G. Show that $R := P \cap Q$ has order p, and that R is normal in G. For the latter show that P and Q are contained in $N_G(R)$ and show that this forces $N_G(R) = G$.)

3. Show that every group of order smaller than 60 is solvable.

4. Show that every group of order 72 is solvable.

5. Let G be a finite group and let p be the smallest prime dividing $|G|$. Assume that H is a subgroup of G with $[G : H] = p$. Show that H is normal in G. In particular, every subgroup of index p in a p-group is normal. (Hint: Use the action of G on G/H and its corresponding homomorphism).

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 square to the empty square. Find out if it is possible to obtain the constellation

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

from the first one.

7. Let $G := \mathrm{Alt}(5)$.

(a) Show that the conjugacy classes of G have length 1, 15, 20, 12 and 12. Derive from this that G is a simple group. (Hint: Show that all elements with the same cycle type (except for 5-cycles) are also conjugate in G. For 5-cycles, compute the centralizer in $\mathrm{Sym}(5)$ and in G. Derive from there that the 5-cycles break up into 2 conjugacy classes of the same size. Then note that every normal subgroup of G is a union of conjugacy classes.)

(b) Find all subgroups of $\mathrm{Alt}(5)$, up to conjugation, and find their normalizers. (Hint: There are no subgroups of order 30, 20, or 15. This needs to be proved. Make use of subgroups you already know: $\mathrm{Alt}(4)$, Sylow subgroups for different primes, their normalizers.)

7 Direct and Semidirect Products

7.1 Definition Let H and N be groups. We say that H *acts on N by group automorphisms* if H acts on N (as a set) and additionally

$$^{h}(n_1n_2) = (\,^{h}n_1)(\,^{h}n_2) \tag{7.1.a}$$

for all $h \in H$ and all $n_1, n_2 \in N$. This condition is equivalent to saying that the image of the group homomorphism $\rho\colon H \to \mathrm{Sym}(N)$, $h \mapsto \pi_h$, resulting from the action of H on N is contained in $\mathrm{Aut}(N)$ (in other words, $\pi_h \in \mathrm{Aut}(N)$ for all $h \in H$), cf. Proposition 5.4. Note that in this case $\,^{h}1 = 1$ for all $h \in H$. We say that H acts *trivially* on N if $\,^{h}n = n$ for all $h \in H$ and all $n \in N$.

7.2 Proposition *Let H and N be groups and let H act on N by group automorphisms. The binary operation on $N \times H$, given by*

$$(a, h)(b, k) := (a \cdot \,^{h}b, h \cdot k)\,, \tag{7.2.a}$$

defines a group structure on $N \times H$. The identity element is $(1, 1)$ and the inverse of $(a, h) \in N \times H$ is equal to $(\,^{h^{-1}}a^{-1}, h^{-1})$.

Proof Associativity and the statements about the identity element and inverse elements are easy verifications (Exercise 1). □

7.3 Definition Assume the notation from the previous proposition. The group constructed with the product (7.2.a) is called the *semidirect product of N and H* and is denoted by $N \rtimes H$. If the action of H on N is not clear from the context one also writes $N \rtimes_\rho H$, where $\rho\colon H \to \mathrm{Aut}(N)$ is the permutation representation of H on N corresponding to the action.

7.4 Remark Assume the notation from the last proposition. The function $i\colon N \to N \rtimes H$, $a \mapsto (a, 1)$, is a monomorphism. Moreover, the function $p\colon N \rtimes H \to H$, $(a, h) \mapsto h$, is an epimorphism. Note that $\mathrm{im}(i) = \ker(p) = \{(a, 1) \mid a \in N\}$ is a normal subgroup of $N \rtimes H$ which is isomorphic to N such that $N \rtimes H/\ker(p) \cong H$, by the fundamental theorem of homomorphisms. In this sense, the semidirect product is made up of two pieces, namely the group N and the group H.

Note also that $j\colon H \mapsto N \rtimes H$, $h \mapsto (1,h)$, is a monomorphism and that the two subgroups $\mathrm{im}(i) \cong N$ and $\mathrm{im}(j) \cong H$ of $N \rtimes H$ satisfy $\mathrm{im}(i) \cap \mathrm{im}(j) = \{1\}$ and $\mathrm{im}(i) \cdot \mathrm{im}(j) = N \rtimes H$.

If the action of H on N is trivial then the semidirect product is just the direct product of N and H.

7.5 Example Let G be a group, let N be a normal subgroup of G and let H be a subgroup of G with $H \cap N = \{1\}$ and $HN = G$. Then H acts by conjugation on N and the resulting semidirect product $N \rtimes H$ is isomorphic to G via the homomorphism $N \rtimes H \to G$, $(n,h) \mapsto nh$ (verify). In this case we also say that G is the *(internal) semidirect product* of the normal subgroup N and the subgroup H, or that N is a *normal complement* of H in G.

7.6 Examples (a) For $3 \leqslant n \in \mathbb{N}$, D_{2n} is the semidirect product of the cyclic subgroup $\langle(1,2,\ldots,n)\rangle$ of order n and the cyclic subgroup $\langle(1,n)(2,n-1)\cdots\rangle$ of order 2.

(b) $\mathrm{Sym}(4)$ is the semidirect product of the Klein 4-group V_4 and the subgroup $\mathrm{Sym}(3)$.

(c) $\mathrm{Alt}(4)$ is the semidirect product of the Klein 4-group V_4 and the subgroup $\langle(1,2,3)\rangle$.

7.7 Definition Let G be a group and let H and K be normal subgroups of G. We say that G is the *(internal) direct product* of the normal subgroups H and K if $H \cap K = \{1\}$ and $HK = G$. Note that in this case $hk = kh$ for all $h \in H$ and all $k \in K$, since $[h,k] = hkh^{-1}k^{-1} \in H \cap K = \{1\}$. Moreover, the function $H \times K \to G$, $(h,k) \mapsto hk$, defined on the (external) direct product of H and K is an isomorphism. For this reason we also write $G = H \times K$ if G is the internal direct product of H and K.

7.8 Examples (a) The Klein 4-group is the direct product of the subgroups $\langle(1,2)(3,4)\rangle$ and $\langle(1,3)(2,4)\rangle$.

(b) If $m,n \in \mathbb{N}$ are relatively prime (i.e., $\gcd(m,n) = 1$) then $\mathbb{Z}/mn\mathbb{Z}$ is the direct product of the subgroups $m\mathbb{Z}/mn\mathbb{Z}$ and $n\mathbb{Z}/mn\mathbb{Z}$.

(c) The dihedral group D_{12} is the direct product of the subgroups $\langle\sigma^3\rangle$ of order 2 and $\langle\sigma^2,\tau\rangle$ of order 6. The latter group is isomorphic to $\mathrm{Sym}(3)$ and D_6.

Exercises

1. Prove Proposition 7.2.

2. (a) Let G be a cyclic group of prime order p. Show that $\mathrm{Aut}(G)$ has order $p-1$.

(b) Let G be a group of order pq with primes $p < q$ such that $p \nmid q-1$. Show that G is cyclic.

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 cartesian product group $H \times K$ to G is a group isomorphism.

4. Let G and H be finite groups.

(a) Show that if $U \leqslant G$ and $V \leqslant H$ then $U \times V \leqslant G \times H$.

(b) Assume that G and H have coprime order, i.e., $\gcd(|G|,|H|) = 1$. Show that every subgroup of $G \times H$ is of the form $U \times V$ for some subgroups $U \leqslant G$ and $V \leqslant H$.

(c) Find a counterexample to (b) when one drops the hypothesis that $|G|$ and $|H|$ are coprime.

5. (a) Let H_1, H_2, N_1, N_2 be groups and assume that H_i acts on N_i via the homomorphism $\rho_i \colon H_i \to \mathrm{Aut}(N_i)$ for $i = 1, 2$. Assume further that there are group isomorphisms $\alpha \colon N_1 \to N_2$ and $\kappa \colon H_1 \to H_2$ such that ${}^{\kappa(h)}\alpha(a) = \alpha({}^{h}a)$ for all $a \in N_1$ and $h \in H_1$. Show that $N_1 \rtimes_{\rho_1} H_1 \cong N_2 \rtimes_{\rho_2} H_2$.

(b) Let $p < q$ be primes such that $p \mid q-1$. Show that there are precisely two isomorphism classes of groups of order pq, represented by the cyclic group and a non-abelian semi-direct product.

8 Free Groups and Presentations

8.1 Definition Let X be a set not containing an element denoted by 1 and assume that for every element $x \in X$, the set X does not contain an element denoted by x^{-1}. We define X^{-1} as the set of symbols x^{-1} where x runs through x. Thus, $X \cap X^{-1} = \emptyset$ and the function $X \to X^{-1}$, $x \mapsto x^{-1}$, is a bijection. A *word* with letters from X is a sequence $(a_1, a_2, \ldots)$ with $a_i \in X \cup X^{-1} \cup \{1\}$ such that there exists $n \in \mathbb{N}$ with $1 = a_n = a_{n+1} = a_{n+2} = \cdots$. The word $(1, 1, 1, \ldots)$ is called the *empty word.* A word $(a_1, a_2, a_3, \ldots)$ is called *reduced* if, for all $i \in \mathbb{N}$ and $x \in X$, one has

(i) $a_i = x \Rightarrow a_{i+1} \neq x^{-1}$,

(ii) $a_i = x^{-1} \Rightarrow a_{i+1} \neq x$, and

(iii) $a_i = 1 \Rightarrow a_{i+1} = 1$.

8.2 Remark Every reduced word has the form $(x_1^{\epsilon_1}, x_2^{\epsilon_2}, \ldots, x_n^{\epsilon_n}, 1, 1, \ldots)$ with $n \in \mathbb{N}_0$, $x_1, \ldots, x_n \in X$, $\epsilon_1, \ldots, \epsilon_n \in \{\pm 1\}$, where $x^1 := x$. We abbreviate this word by $x_1^{\epsilon_1} \cdots x_n^{\epsilon_n}$. Two reduced words $x_1^{\epsilon_1} \cdots x_n^{\epsilon_n}$ and $y_1^{\delta_1} \cdots y_m^{\delta_m}$ are equal if and only if $m = n$, $x_i = y_i$ and $\epsilon_i = \delta_i$ for all $i = 1, \ldots, n$. For the empty word we write just 1.

8.3 Proposition *Let X be as in the above definition. The set of reduced words with letters in X is a group $F(X)$, the* free group *on X, under the following multiplication: Let $w = x_1^{\epsilon_1} \cdots x_n^{\epsilon_n}$ and $v = y_1^{\delta_1} \cdots y_m^{\delta_m}$ be elements of $F(X)$ with $n \leqslant m$ and let $k \in \{0, \ldots, n\}$ be maximal with $x_{n-j}^{\epsilon_{n-j}} = y_{j+1}^{-\delta_{j+1}}$ for all $j = 0, \ldots, k-1$. Then the product wv is defined by*

$$(x_1^{\epsilon_1} \cdots x_n^{\epsilon_n})(y_1^{\delta_1} \cdots y_m^{\delta_m}) := \begin{cases} x_1^{\epsilon_1} \cdots x_{n-k}^{\epsilon_{n-k}} y_{k+1}^{\delta_{k+1}} \cdots y_m^{\delta_m}\,, & \text{if } k < n, \\ y_{n+1}^{\delta_{n+1}} \cdots y_m^{\delta_m}\,, & \text{if } k = n < m, \\ 1\,, & \text{if } k = n = m. \end{cases}$$

In the case $n > m$ the product is defined in an obvious analogous way.

Proof The proof of associativity is a straightforward but lengthy case distinction and is left out. The identity element is the empty word 1 and the inverse of $x_1^{\epsilon_1} \cdots x_n^{\epsilon_n}$ is $x_n^{-\epsilon_n} \cdots x_1^{-\epsilon_1}$. □

8.4 Example Let $X = \{a, b, c\}$. Then $(aab^{-1}cbcb^{-1})(bc^{-1}abb) = aab^{-1}cbabb = a^2b^{-1}cbab^2$ is an equation in $F(X)$.

8.5 Remark Let X be as in Definition 8.1. We denote by $i\colon X \to F(X)$ the function defined by $i(x) := (x, 1, 1, \ldots)$. Note that the reduced word $x_1^{\epsilon_1} \cdots x_n^{\epsilon_n}$ is equal to the product $i(x_1)^{\epsilon_1} \cdots i(x_n)^{\epsilon_n}$. This shows that $F(X)$ is generated by the set $\{i(x) \mid x \in X\}$. For $x \in X$ the inverse of $i(x) = (x, 1, \ldots)$ is equal to $(x^{-1}, 1, \ldots) = i(x)^{-1}$, justifying the notation.

8.6 Theorem (Universal property of the free group) *Let X be as in Definition 8.1. For every group G and every function $f\colon X \to G$ there exists a unique group homomorphism $\tilde{f}\colon F(X) \to G$ such that $\tilde{f} \circ i = f$.*

Proof Existence: We set $\tilde{f}(1) := 1$ and $\tilde{f}(x_1^{\epsilon_1} \cdots x_n^{\epsilon_n}) := f(x_1)^{\epsilon_1} \cdots f(x_n)^{\epsilon_n}$. Then, it is easy to check that $\tilde{f}$ is a homomorphism. Moreover, $\tilde{f}(i(x)) = \tilde{f}(x^1) = f(x)^1 = f(x)$ for all $x \in X$.

Uniqueness: Assume that also $\hat{f}\colon F(X) \to G$ is a homomorphism with $\hat{f} \circ i = f$. Then $\hat{f} = \tilde{f}$, since $\hat{f}$ and $\tilde{f}$ coincide on the generating set $i(X)$ of $F(X)$. □

8.7 Definition Let G be a group and let $Y \subseteq G$ be a subset. The *normal subgroup of G generated by Y* is defined as

$$\langle\langle Y \rangle\rangle_G := \langle\langle Y \rangle\rangle := \langle \{gyg^{-1} \mid y \in Y, g \in G\} \rangle \,.$$

It is easy to see that $\langle\langle Y \rangle\rangle$ is the intersection of all normal subgroups of G that contain Y and that it is also the smallest (with respect to inclusion) normal subgroup of G that contains Y.

8.8 Definition (a) Let X be as in Definition 8.1 and let R be a subset of $F(X)$. Then the *group with generators X and relations R* is defined as the group $F(X)/\langle\langle R \rangle\rangle$ and it is denoted by $\langle X \mid R \rangle$.

(b) Let G be a group, let $X \subseteq G$ and let $\tilde{j}\colon F(X) \to G$ be the unique homomorphism defined by the inclusion function $j\colon X \to G$, $x \mapsto x$, via the universal property of $F(X)$. Let $R \subseteq F(X)$ be a subset. We say that the *relations R hold in G* if $R \subseteq \ker(\tilde{j})$. In this case, the fundamental theorem of homomorphisms implies the existence of a homomorphism

$$\bar{j}\colon F(X)/\langle\langle R \rangle\rangle \to G \,.$$

such that the diagram

$$\begin{tikzcd}
X \arrow[r, "i"] \arrow[dr, "j"'] & F(X) \arrow[r, "\nu"] \arrow[d, "\tilde{j}"'] & F(X)/\langle\langle R\rangle\rangle \arrow[dl, "\bar{j}"] \\
& G &
\end{tikzcd}$$

is commutative. If X is a generating set of G and if $\langle\langle R\rangle\rangle = \ker(\tilde{j})$ we write

$$G = \langle X|R\rangle \tag{8.8.a}$$

and say that (8.8.a) is a *presentation* of G with generators X and relations R. This is equivalent to saying that $\bar{j}$ is an isomorphism.

8.9 Remark (a) A group G usually has many different presentations.

(b) Assume that $G = \langle X|R\rangle$ is a presentation of G and that a certain product of elements of X and their inverses is equal to 1. This product can be interpreted as an element in $F(X)$ and there it can be written as a product of conjugates of elements of R. In other words, every relation among the generators X of G can be derived in this way from the relations R.

(c) If $G = \langle X|R\rangle$ is a presentation of G and if $X = \{x_1, \ldots, x_n\}$ and $R = \{r_1, \ldots, r_m\}$ are finite, we also write $G = \langle x_1, \ldots, x_n \,|\, r_1, \ldots, r_m\rangle$ instead of $G = \langle\{x_1, \ldots, x_n\} \mid \{r_1, \ldots, r_m\}\rangle$.

(d) As the following proposition shows, knowing a presentation of a group G helps to define homomorphisms from G to other groups.

8.10 Proposition *Let $G = \langle X|R\rangle$ be a presentation of the group G. Let also H be a group and let $f\colon X \to H$ be a function such that for every element $x_1^{\epsilon_1} \cdots x_n^{\epsilon_n} \in R$ one has $f(x_1)^{\epsilon_1} \cdots f(x_n)^{\epsilon_n} = 1$ in H. Then there exists a unique group homomorphism $\hat{f}\colon G \to H$ such that $\hat{f}(x) = f(x)$ for all $x \in X$.*

Proof The commutative diagram from Definition 8.8 can be extended to a commutative diagram

$$\begin{tikzcd}
& H & \\
X \arrow[ur, "f"] \arrow[r, "i"] \arrow[dr, "j"'] & F(X) \arrow[u, "\tilde{f}"] \arrow[r, "\nu"] \arrow[d, "\tilde{j}"] & F(X)/\langle\langle R\rangle\rangle \arrow[ul, "\overline{f}"'] \arrow[dl, "\bar{j}"] \\
& G &
\end{tikzcd}$$

where $\tilde{f}$ is defined by the universal property of $F(X)$ and $\overline{f}$ is defined by the fundamental theorem of homomorphisms, noting that $R \subseteq \ker(\tilde{f})$ is a consequence of the hypothesis of the proposition. Since $G = \langle X | R\rangle$, the homomorphism $\bar{j}$ is an isomorphism. Now we define $\hat{f} \colon G \to H$ by $\hat{f} := \overline{f} \circ \bar{j}^{-1}$ and obtain

$$\hat{f} \circ j = \overline{f} \circ \bar{j}^{-1} \circ j = \overline{f} \circ \bar{j}^{-1} \circ \tilde{j} \circ i = \overline{f} \circ \bar{j}^{-1} \circ \bar{j} \circ \nu \circ i = \overline{f} \circ \nu \circ i = \tilde{f} \circ i = f$$

as required. Since G is generated by X, the homomorphism $\hat{f}$ is uniquely determined by the condition $\hat{f} \circ j = f$. □

8.11 Example Let $n \geqslant 3$ be a natural number and let $\sigma := (1, 2, \ldots, n) \in \mathrm{Sym}(n)$ and $\tau := (1, n)(2, n-1)(3, n-2) \cdots \in \mathrm{Sym}(n)$. Recall from Definition 6.9 that the dihedral group D_{2n} is defined as $D_{2n} := \langle \sigma, \tau \rangle \leqslant \mathrm{Sym}(n)$.

(a) We will show that

$$D_{2n} = \langle \sigma, \tau \mid \sigma^n, \tau^2, \tau\sigma\tau^{-1}\sigma \rangle \,.$$

Here, with $X := \{\sigma, \tau\}$ and $R := \{\sigma^n, \tau^2, \tau\sigma\tau\sigma\}$, we define $\underline{\sigma} := i(\sigma)$, $\underline{\tau} := i(\tau) \in F(X)$. Since σ and τ generate D_{2n} and since the relations R hold in D_{2n}, the universal property of $F(X)$ and the fundamental theorem of homomorphisms yield a group epimorphism $\bar{j} \colon F(X)/\langle\langle R\rangle\rangle \to D_{2n}$ mapping the coset of $\underline{\sigma}$ (resp. $\underline{\tau}$) to σ (resp. τ). Using the equation $\underline{\tau}\underline{\sigma}\langle\langle R\rangle\rangle = \underline{\sigma}^{-1}\underline{\tau}\langle\langle R\rangle\rangle$ we can rewrite every element $w\langle\langle R\rangle\rangle \in F(X)/\langle\langle R\rangle\rangle$ as $\underline{\sigma}^k\underline{\tau}^l\langle\langle R\rangle\rangle$ with $k, l \in \mathbb{Z}$. Using the equations $\underline{\sigma}^n\langle\langle R\rangle\rangle = \langle\langle R\rangle\rangle$ and $\underline{\tau}^2\langle\langle R\rangle\rangle = \langle\langle R\rangle\rangle$ we can rewrite $\underline{\sigma}^k\underline{\tau}^l\langle\langle R\rangle\rangle = \underline{\sigma}^i\underline{\tau}^j\langle\langle R\rangle\rangle$ with $0 \leqslant i \leqslant n-1$ and $0 \leqslant j \leqslant 1$. This implies that $F(X)/\langle\langle R\rangle\rangle$ has at most $2n$ elements. Since the map

$\bar{j}\colon F(X)/\langle\langle R\rangle\rangle \to D_{2n}$ is surjective, it must be an isomorphism. This means by definition that $G = \langle X|R\rangle$.

(b) Now that we know that $D_{2n} = \langle X|R\rangle$ we can define a homomorphism from D_{2n} to any group H by simply finding elements $s, t \in H$ such that $s^n = 1$, $t^2 = 1$ and $tst^{-1}s = 1$. By Proposition 8.10, for each such pair (s,t) of elements there exists a unique group homomorphism $D_{2n} \to H$ with maps σ to s and τ to t. Thus, Proposition 8.10 implies immediately that

$$\begin{aligned}\mathrm{Hom}(D_{2n}, H) &\to \{(s,t) \in H \times H \mid s^n = t^2 = tst^{-1}s = 1\}\\ \phi &\mapsto (\phi(\sigma), \phi(\tau))\end{aligned}$$

is a bijection.

(c) It is not difficult to show that D_{2n} also has the presentation

$$D_{2n} = \langle \tau, \tau' \mid \tau^2, \tau'^2, (\tau\tau')^n\rangle\,,$$

where $\tau' := \sigma\tau$.

8.12 Example Let $n \geqslant 2$ and set $s_i := (i, i+1) \in \mathrm{Sym}(n)$ for $i = 1, \ldots, n-1$. Then the following relations hold in $\mathrm{Sym}(n)$: $s_i^2 = 1$ for $i = 1, \ldots, n-1$, and $(s_i s_{i+1})^3 = 1$ for $i = 1, \ldots, n-2$. One can show that this is a presentation of $\mathrm{Sym}(n)$.

Exercises

1. (a) Let $X = \{x\}$ be a set with one element. Show that $F(X) \cong \mathbb{Z}$.

(b) Let $n \in \mathbb{N}$. Show that $\langle x \mid x^n\rangle$ is a cyclic group of order n.

(c) Show that $\langle x, y \mid xyx^{-1}y^{-1}\rangle \cong \mathbb{Z} \times \mathbb{Z}$.

2. Show that

$$\langle a, b \mid a^4 = 1, a^2 = b^2, bab^{-1} = a^3\rangle$$

is a presentation of the quaternion group Q_8 of order 8.

3. Let G be a group.

(a) Show that the set of *inner* automorphisms of G,

$$\mathrm{Inn}(G) := \{c_g \mid g \in G\}\,,$$

is a normal subgroup of $\mathrm{Aut}(G)$.

(b) Show that $\mathrm{Inn}(G)$ is isomorphic to $G/Z(G)$.

4. (a) Determine the orders of $\mathrm{Inn}(D_8)$ and $\mathrm{Aut}(D_8)$ and derive that the group $\mathrm{Aut}(D_8)/\mathrm{Inn}(D_8)$ has order 2.

(b) Write down explicitly an element in $\mathrm{Aut}(D_8)$ which is not in $\mathrm{Inn}(D_8)$ by giving the images of generators.

5. Show that $\mathrm{Aut}(Q_8)/\mathrm{Inn}(Q_8)$ is isomorphic to Sym(3). (Hint: Show that $\mathrm{Aut}(Q_8)$ acts on the set X consisting of the 3 subgroups of Q_8 of order 4. Use this to construct an isomorphism.)

Chapter II: Rings

9 Rings: Basic Definitions and Properties

9.1 Definition A *ring* is a set R together with two binary operations $+\colon R\times R\to R$, $(a,b)\mapsto a+b$, and $\cdot\colon R\times R\to R$, $(a,b)\mapsto a\cdot b$, called *addition* and *multiplication*, respectively, such that

(i) $(R,+)$ is an abelian group,

(ii) $(R,\cdot)$ is a monoid, and

(iii) $a\cdot(b+c)=(a\cdot b)+(a\cdot c)$ and $(a+b)\cdot c=(a\cdot c)+(b\cdot c)$ for all $a,b,c\in R$ (distributivity).

If additionally $a\cdot b=b\cdot a$ holds for all $a,b\in R$ then the ring R is called a *commutative* ring.

9.2 Remark Let R be a ring. The identity element with respect to addition is denoted by 0 and called the *zero element*, the identity element with respect to multiplication is denoted by 1 and called the *one element* or *identity element*. Usually we write ab instead of $a\cdot b$ and $a-b$ instead of $a+(-b)$ for $a,b\in R$. To avoid too many parentheses, one has the rule that multiplication has priority over addition. For instance, $a+bc$ always means $a+(bc)$ for $a,b,c\in R$. The following facts for $a,b\in R$ are immediate consequences of the axioms:

(i) $0a=0=a0$.

(ii) $(-a)b=-(ab)=a(-b)$.

(iii) $(-a)(-b)=ab$.

9.3 Examples (a) If one has $0=1$ in some ring R then $R=\{0\}$ and R is called a trivial ring.

(b) $\mathbb{Z}\subset\mathbb{Q}\subset\mathbb{R}\subset\mathbb{C}$ are rings. $\mathbb{N}$ is not a ring.

(c) If R_i, $i\in I$, are rings then the cartesian product $\prod_{i\in I}R_i$ is again a ring with componentwise addition and multiplication. The 0-element is the tuple with entry 0_{R_i} in the i-th component and the 1-element is the tuple with 1_{R_i} in the i-th component.

(d) If R is a ring, one defines its opposite ring R° as the same set R with the same addition as R, but with multiplication $*$ given by $a*b:=ba$. Note that $(R^\circ)^\circ=R$.

(e) Let R be a ring and $n \in \mathbb{N}$. Then $\mathrm{Mat}_n(R)$, the set of $n \times n$-matrices with entries in R is a ring with the usual matrix addition and multiplication.

(f) For every ring R the *polynomial ring* $R[X]$ in the indeterminate X with coefficients in R, given by

$$R[X] = \{a_0 + a_1X + a_2X^2 + \cdots + a_nX^n \mid n \in \mathbb{N}_0, a_0, \ldots, a_n \in R\}$$

is a ring with the usual addition and multiplication of polynomials. Note: We do not view polynomials as functions from R to R, but as abstract sums of the above form. Two polynomials $p(X) = a_0 + a_1X + \cdots a_nX^n$ and $q(X) = b_0+b_1X+\cdots b_mX^m$ are equal if an only if $b_i = a_i$ for all $i \in \mathbb{N}_0$, where we set $a_i := 0$ if $i > n$ and $b_i := 0$ if $i > m$. If $p(X) = a_0 + a_1X + \cdots a_nX^n$ with $a_n \neq 0$ we call a_n the *leading coefficient* of $p(X)$ and $\deg(p(X)) := n$ the *degree* of $p(X)$. The 0-polynomial has no leading coefficient. Its degree is $-\infty$, by definition. Note that $\deg(p(X)q(X)) = \deg(p(X)) + \deg(q(X))$ provided that $ab = 0$ implies $a = 0$ or $b = 0$ for all $a, b \in R$. If $p(X) \in R[X]$ has leading coefficient 1 we call $p(X)$ a *monic* polynomial.

One could introduce $R[X]$ also as the set of all sequences $(a_0, a_1, a_2, \ldots)$ in R with only finitely many non-zero entries together with componentwise addition and multiplication given by $(a_0, a_1, \ldots)(b_0, b_1, \ldots) = (c_0, c_1, c_2, \ldots)$ where $c_i = a_0b_i + a_1b_{i-1} + \cdots + a_ib_0$ for $i \in \mathbb{N}_0$. The element X corresponds to the sequence $(0, 1, 0, \ldots)$. One could also introduce $R[X]$ as the set of functions $f\colon \mathbb{N}_0 \to R$ which are non-zero on only finitely many elements, together with the usual addition of functions and the multiplication given by $(f \cdot g)(i) := \sum_{k=0}^{i} f(k)g(i-k)$ for $i \in \mathbb{N}_0$, also called convolution.

(g) More generally, one introduces the polynomial ring $R[X_1, \ldots, X_n]$ in n indeterminates $X_1, \ldots, X_n$ with coefficients in R in a similar way. Abstractly, one can introduce this ring again as the set of functions $f\colon \mathbb{N}_0^n \to R$ with $f(\underline{i}) \neq 0$ for only finitely many $\underline{i} = (i_1, \ldots, i_n) \in \mathbb{N}_0^n$. More intuitively, one sets $X^{\underline{i}} := X_1^{i_1} \cdots X_n^{i_n}$ for $\underline{i} = (i_1, \ldots, i_n) \in \mathbb{N}_0^n$, and defines $R[X_1, \ldots, X_n]$ as the set of formal finite sums $\sum_{\underline{i}\in\mathbb{N}_0} r_{\underline{i}}X^{\underline{i}}$ (with $r_{\underline{i}} \in R$, all but finitely many equal to 0) with the usual addition and multiplication.

One can also define polynomial rings $R[X_i \mid i \in I]$ for any set of indeterminates X_i, $i \in I$.

(h) If A is an abelian group then its *endomorphism ring* $\mathrm{End}(A) := \mathrm{Hom}(A, A)$ is a ring with pointwise addition ($(f + g)(a) := f(a) + g(a)$ for $f, g \in \mathrm{End}(A)$ and $a \in A$) and composition as multiplication. (Verify!)

(i) If R is a ring and G is a monoid then the *monoid ring* $R[G]$ is the set of all formal sums $\sum_{g\in G} r_g g$ with $g \in G$ and $r_g \in R$ such that all but finitely many coefficients r_g are 0. Addition is defined by

$$(\sum_{g\in G} r_g g) + (\sum_{g\in G} s_g g) = \sum_{g\in G} (r_g + s_g) g$$

and multiplication is defined by

$$(\sum_{g\in G} r_g g)(\sum_{h\in G} s_h h) = \sum_{(g,h)\in G\times G} (r_g s_h)(gh) = \sum_{g\in G} (\sum_{\substack{(x,y)\in G\times G \\ xy=g}} r_x s_y) g \,.$$

If G is a group we call $R[G]$ the *group ring* of G over R. Note that the polynomial ring $R[X]$ can also be interpreted as the monoid ring over the monoid $\mathbb{N}_0$ under addition over the ring R.

9.4 Definition Let R be a ring.

(a) An element $u \in R$ is called a *unit* of R (or *invertible* in R) if there exists $v \in R$ with $uv = 1 = vu$ (i.e., if u is an invertible element in the monoid $(R, \cdot)$.) In this case, the element v is uniquely determined. It is called the *inverse* of u and is denoted by u^{-1}. The set of invertible elements of R forms a group under multiplication. It is called the *unit group* of R and is denoted by $R^\times$ or $U(R)$.

(b) An element $a \in R$ is called a *zero divisor* if there exists $b \in R \smallsetminus \{0\}$ such that $ab = 0$ or $ba = 0$.

9.5 Examples (a) Assume that R is non-trivial ring. Then 0 is a zero-divisor, since $0 \cdot 1 = 0$. The element 0 is the only zero divisor in R if and only if $ab = 0$ implies $a = 0$ or $b = 0$, for all $a, b \in R$.

(b) In the ring $\mathbb{Z}\times\mathbb{Z}$ the element $(2, 0)$ is a zero-divisor, since $(2, 0)\cdot(0, 1) = (0, 0)$.

(c) Let R be a commutative ring. The unit group of the ring $\mathrm{Mat}_n(R)$ is denoted by $\mathrm{GL}_n(R)$ and called the general linear group. Note: A is invertible in $\mathrm{Mat}_n(R)$ if and only if $\det(A)$ is a unit in R. In fact, one direction follows from the product formula for determinants and the other direction follows from the explicit formula for the inverse, involving the inverse of the determinant.

(d) For every group G and every ring R, the elements of G form a subgroup of $(R[G])^\times$.

9.6 Definition Let R be a ring.

(a) R is called an *integral domain* if it is commutative, if $1 \neq 0$ and if 0 is the only zero-divisor of R.

(b) R is called a *division ring* if $1 \neq 0$ and if $R^\times = R \smallsetminus \{0\}$.

(c) R is called a *field* if it is a commutative division ring.

9.7 Examples (a) For any ring R one has: R is a field if and only if it is an integral domain and a division ring.

(b) $\mathbb{Z}$ is an integral domain.

(c) If R is an integral domain then $R[X]$ is an integral domain and $R[X]^\times = R^\times$.

9.8 Definition A subset S of a ring R is called a *subring* if $1_R \in S$ and if for all $a, b \in S$ one also has $a - b \in S$ and $ab \in S$. In this case, S together with the restricted addition and multiplication is again a ring.

9.9 Remark Let R be a ring.

(a) $S := \{(r, 0) \mid r \in R\}$ is not a subring of the ring $R \times R$, since $(1, 1) \notin S$.

(b) Every subring of a field is an integral domain.

(c) The center $Z(R) := \{a \in R \mid ab = ba \text{ for all } b \in R\ \}$ of a ring R is a subring of R.

(d) The intersection of any collection of subrings of R is again a subring of R.

9.10 Definition Let R be a commutative ring and let S be a subring of R. For any subset Y of R we denote by $S[Y]$ the intersection of all subrings of R that contain S and Y. It is the smallest subring of R containing S and Y. It is equal to the set of elements of the form $p(y_1, \ldots, y_n)$ where $n \in \mathbb{N}$, $p(X1, \ldots, X_n) \in S[X_1, \ldots, X_n]$, and $y_1, \ldots, y_n \in Y$.

9.11 Examples (a) $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$ are subrings of each other. $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ are fields.

(b) $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ is a subring of $\mathbb{C}$, called the ring of *Gaussian integers*. It is an integral domain.

(c) $\mathbb{Q}[i] = \{a + bi \mid a, b \in \mathbb{Q}\}$ is a subring of $\mathbb{C}$. It is even a field, called the field of *Gaussian numbers*. In fact,

$$(a + bi)^{-1} = \frac{a}{a^2 + b^2} - \frac{b}{a^2 + b^2} i$$

for $a + bi \neq 0$.

(d) $\mathbb{Z}[\sqrt{5}i] := \{a + b\sqrt{5}i \mid a, b \in \mathbb{Z}\}$ is a subring of $\mathbb{C}$ and an integral domain.

(e) The set of 2×2-matrices

$$\begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix}, \quad \text{with } a, b \in \mathbb{C},$$

form a subring of the ring $\mathrm{Mat}_2(\mathbb{C})$ (verify!). It is a non-commutative division ring. In fact, for a non-zero matrix as above, we have $a\bar{a} + b\bar{b} \neq 0$ and we can check easily that

$$\frac{1}{a\bar{a} + b\bar{b}} \begin{pmatrix} \bar{a} & -b \\ \bar{b} & a \end{pmatrix}$$

is its inverse. This division ring is denoted by $\mathbb{H}$ and called the *quaternion division ring* (discovered by Hamilton in 1843). If one sets

$$1 := \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad i := \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \quad j := \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad k := ij = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix},$$

then $\mathbb{H}$ is a 4-dimensional subspace with basis $\{1, i, j, k\}$ of the 8-dimensional real vector space $\mathrm{Mat}_2(\mathbb{C})$. Note that $i^2 = j^2 = k^2 = -1$, $ij = k, jk = i, ki = j$, and $ji = -k, kj = -i, ik = -j$. The center of $\mathbb{H}$ is equal to $\mathbb{R} \cdot 1$, the field of real numbers. Note that $\{\pm 1, \pm i, \pm j, \pm k\}$ is a subgroup of the unit group of $\mathbb{H}$, isomorphic to the quaternion group Q_8 (verify!).

Exercises

1. (a) Determine the unit group of the ring $\mathbb{Z}[i] := \{a + bi \mid a, b \in \mathbb{Z}\}$, the ring of *Gaussian integers.*

(b) Show that the ring $\mathbb{Z}[\sqrt{2}] := \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$ has infinitely many units and find all units of finite order.

2. (a) Let R be a finite integral domain. Show that R is a field.

(b) Let R be a division ring. Show that $Z(R)$ is a field.

3. Prove the statements on the quaternion division ring $\mathbb{H}$ in Example 9.11(e)

4. Prove the statements in Definition 9.10.

10 Homomorphisms, Ideals and Factor Rings

10.1 Definition Let R and S be rings. A function $f\colon R \to S$ is called a *ring homomorpism* if

$$f(1_R) = 1_S \quad \text{and} \quad f(a+b) = f(a) + f(b) \quad \text{and} \quad f(ab) = f(a)f(b)$$

for all $a, b \in R$. The notions "mono-, epi-, iso-, endo-, and automorphism" are defined as for groups. R and S are called *isomorphic* (notation $R \cong S$ as for groups) if there exists an isomorphism $f\colon R \to S$. If $f\colon \mathrm{R}\to S$ is a ring homomorphism then its *kernel* is defined as $\ker(f) := \{a \in R \mid f(a) = 0\}$.

10.2 Remark Let R and S be rings and let $f\colon R \to S$ be a ring homomorphism.

(a) If $x \in R^\times$ then $f(x) \in S^\times$ with $f(x^{-1}) = f(x)^{-1}$. The restriction of f to the subset $R^\times$ of R is a group homomorphism $f\colon R^\times \to S^\times$.

(b) The composition of two ring homomorphisms is again a ring homomorphism. If a ring homomorphism f is bijective then also f^{-1} is a ring homomorphism. The automorphisms of R form a group $\mathrm{Aut}(R)$, the *automorphism group* of the ring R.

10.3 Examples (a) Complex conjugation is a ring automorphism of $\mathbb{C}$.

(b) For any ring R, $a \in R$ and $n \in \mathbb{Z}$ we define

$$n \cdot a := \begin{cases} a + a + \cdots + a\,, & \text{if } n > 0, \\ 0\,, & \text{if } n = 0, \\ -a - a - \cdots - a\,, & \text{if } n < 0, \end{cases}$$

as we did for groups (now applied to the additive group $(R, +)$). The function $\mathbb{Z} \to R$, $n \mapsto n \cdot 1$, is a ring homomorphism (in fact the unique ring homomorphism from $\mathbb{Z}$ to R). Its image is contained in $Z(R)$. Its kernel must be of the form $k\mathbb{Z}$ for a unique $k \in \mathbb{N}_0$. We call k the *characteristic* of R. It is denoted by $\mathrm{char}(R)$.

(c) Let R be a commutative ring. An *R-algebra* is a ring A together with a homomorphism $\eta\colon R \to A$ such that $\eta(R) \subseteq Z(A)$. Let (A, η) and (A', η') are R-algebras. An R-algebra homomorphism from A to A' is a ring homomorphism $f\colon A \to A'$ such that $f \circ \eta = \eta'$. For instance, the polynomial ring $R[X]$ and the matrix ring $\mathrm{Mat}_n(R)$ are R-algebras with the obvious structure maps, $r \mapsto r$ and $r \mapsto r \cdot I_n$, where I_n denotes the identity matrix. Every ring is a $\mathbb{Z}$-algebra in a unique way (see (b)).

(d) Let R be a commutative ring and let (A, η) be an R-algebra. For every $a \in A$ one has the *evaluation map*

$$\epsilon_a \colon R[X] \to A\,,$$
$$p(X) = r_n X^n + \cdots + r_1 X + r_0 \mapsto p(a) := \eta(r_n)a^n + \cdots \eta(r_1)a + \eta(r_0)\,.$$

It is an R-algebra homomorphism. If $p(a) = 0$ we call the element a a *zero*, or a *root*, of $p(X)$ in A.

10.4 Definition Let R be a ring and let $I \subseteq R$ be an additive subgroup of R, i.e., $0 \in I$ and $x - y \in I$ for all $x, y \in I$.

(a) I is called a *left ideal* if $rx \in I$ for all $r \in R$ and all $x \in I$.

(b) I is called a *right ideal* if $xr \in I$ for all $r \in R$ and all $x \in I$.

(c) I is called an *ideal* (or sometimes for emphasis a *two-sided ideal*) if it is a left and right ideal.

10.5 Proposition *Let R be a ring and let I be an additive subgroup of R. The following are equivalent:*

(i) *I is an ideal of R.*

(ii) *The group $(R/I, +)$ is a ring under $(r+I)(s+I) := rs+I$ for $r, s \in R$.*

(iii) *There exists a ring S and a ring homomorphism $f \colon R \to S$ with $I = \ker(f)$.*

Proof (i)⇒(ii): We know that $(R/I, +)$ is an abelian group. The multiplication from (ii) is well-defined: Let $r, r', s, s' \in R$ with $r + I = r' + I$ and $s + I = s' + I$. Then there exist $x, y \in I$ with $r' = r + x$ and $s' = s + y$. It follows that $r's' + I = (r+x)(s+y) + I = rs + ry + xs + xy + I = rs + I$, since $ry, xs, xy \in I$, as I is an ideal of R. It is easy to check that R/I becomes a monoid with identity element $1 + I$ under this multiplication. Distributivity for R/I follows immediately from the distributivity of R.

(ii)⇒(iii): Let $\nu \colon R \to R/I$, $r \mapsto r + I$, be the natural epimorphism of the additive groups. It is easy to check that it is a ring homomorphism. Obviously, $\ker(f) = I$.

(iii)⇒(i): Let $f \colon R \to S$ be a ring homomorphism with $\ker(f) = I$. For every $r \in R$ and every $x \in I$ we have $f(rx) = f(r)f(x) = 0$ and $f(xr) = f(x)f(r) = 0$. Thus, I is an ideal of R. □

10.6 Definition Let R be a ring and let I be an ideal. The ring R/I with the multiplication defined as in Proposition 10.5(ii) is called the *factor ring* of R with respect to the ideal I. Note that the canonical epimorphism $\nu\colon R \to R/I$ is a ring homomorphism.

10.7 Examples Let R be a ring.

(a) $\{0\}$ and R are always ideals of R. If $R \neq \{0\}$ and if these are the only ideals then R is called *quasi-simple*. (A ring is called *simple* if it is quasi-simple and additionally *artinian*, a notion we will not explain and use in this class.)

(b) Let I be a left or right ideal of R and assume that I contains a unit u of R. Then $I = R$. In fact, in the case of I being a left ideal, we have $1 = u^{-1}u \in I$ and then $r = r \cdot 1 \in I$ for all $r \in R$. A similar argument is used if I is a right ideal.

(c) Let A be a set and let I_α, $\alpha \in A$, be a collection of left ideals of R. Then $\bigcap_{\alpha\in A} I_\alpha$ is again a left ideal of R. Similar statements hold for right ideals and for ideals.

(d) Let $X \subseteq R$ be a subset. The *left ideal of R generated by X* is defined as the intersection of all left ideals of R that contain X. It is the smallest left ideal of R containing X and is denoted by ${}_R(X)$. Similarly, one defines the right ideal and the ideal of R generated by X. They are denoted by $(X)_R$ and by (X), respectively. One has

$$\begin{aligned}
{}_R(X) &= \{r_1x_1 + \cdots + r_nx_n \mid n \in \mathbb{N}_0,\ r_1,\ldots,r_n \in R,\ x_1,\ldots,x_n \in X\}\,,\\
(X)_R &= \{x_1r_1 + \cdots + x_nr_n \mid n \in \mathbb{N}_0,\ r_1,\ldots,r_n \in R,\ x_1,\ldots,x_n \in X\}\,,\\
(X) &= \{r_1x_1s_1 + \cdots + r_nx_ns_n \mid n \in \mathbb{N}_0,\ r_1,\ldots,r_n,s_1,\ldots,s_n \in R,\\
&\qquad\qquad x_1,\ldots,x_n \in X\}\,.
\end{aligned}$$

If $X = \emptyset$ one sets ${}_R(X) = (X)_R = (X) := \{0\}$.

If R is commutative then $(X) = {}_R(X) = (X)_R$. If additionally $X = \{x\}$ consists of only one element then $(x) = xR = Rx$ is called a *principal ideal* of R.

(e) Let I_α, $\alpha \in A$, be a collection of left ideals of R. Then their *sum* is defined by

$$\sum_{\alpha\in A} I_\alpha := \{x_{\alpha_1} + \cdots + x_{\alpha_n} \mid n \in \mathbb{N}_0, \alpha_1,\ldots,\alpha_n \in A, x_{\alpha_1} \in I_{\alpha_1},\ldots,x_{\alpha_n} \in I_{\alpha_n}\}\,.$$

It is again a left ideal, in fact the left ideal generated by $\bigcup_{\alpha\in A} I_\alpha$. One defines sums of right ideals and of ideals the same way. They are again right ideals and ideals, respectively.

(f) Let I and J be ideals. Their *product* $I \cdot J$ (or just IJ) is defined by

$$IJ := \{x_1y_1 + \cdots + x_ny_n \mid n \in \mathbb{N}_0,\ x_1, \ldots, x_n \in I,\ y_1, \ldots, y_n \in J\}\,.$$

It is again an ideal. For ideals I, J, K of R one has $(I+J)+K = I+(J+K)$, $IJ \subseteq I \cap J$, $(IJ)K = I(JK)$, $(I+J)K = IK + JK$, $I(J+K) = IJ + IK$.

(g) The ideals of $\mathbb{Z}$ are precisely the subsets $k\mathbb{Z}$ with $k \in \mathbb{N}_0$. The factor ring of $\mathbb{Z}$ with respect to $k\mathbb{Z}$ is $\mathbb{Z}/k\mathbb{Z}$ with multiplication $(m+k\mathbb{Z})(n+k\mathbb{Z}) = mn + k\mathbb{Z}$. In the ring $\mathbb{Z}$ we have the following identities between ideals:

$$(k) + (l) = (\gcd(k,l))\,, \quad (k) \cap (l) = (\operatorname{lcm}(k,l))\,, \quad (k)(l) = (kl)\,.$$

Note: In order to prove the first equation we need that $\gcd(k,l) \in k\mathbb{Z} + l\mathbb{Z}$, a result that follows from the Euclidean Algorithm for the integers. This is usually proved in elementary number theory. We will prove it again in a later section in a more general situation.

10.8 Theorem (Fundamental Thm. of Homomorphisms for Rings) *Let R and S be rings, let $f\colon R \to S$ be a ring homomorphism and let I be an ideal of R with $I \subseteq \ker(f)$. There exists a unique ring homomorphism $\overline{f}\colon R/I \to S$ such that $\overline{f} \circ \nu = f$, where $\nu\colon R \to R/I$ denotes the natural epimorphism. Moreover, $\operatorname{im}(\overline{f}) = \operatorname{im}(f)$ and $\ker(\overline{f}) = \ker(f)/I$. In particular, $R/\ker(f) \cong \operatorname{im}(f)$ as rings.*

Proof By the fundamental theorem of homomorphisms for groups there exists a unique group homomorphism $\overline{f}\colon R/I \to S$ for the underlying additive groups, such that $\overline{f} \circ \nu = f$. For $r, r' \in R$ we have $\overline{f}((r+I)(r'+I)) = \overline{f}(rr' + I) = f(rr') = f(r)f(r') = \overline{f}(r+I)\overline{f}(r'+I)$. Moreover, $\overline{f}(1+I) = f(1) = 1$. Thus, $\overline{f}$ is a ring homomorphism. The statement about the image and the kernel of $\overline{f}$ only depends on the additive group structure and therefore follows from the group version of the theorem. □

10.9 Theorem (1^{st} Isomorphism Theorem for Rings) *Let R be a ring, let $S \subseteq R$ be a subring and let I be an ideal of R. Then $S + I := \{s + x \mid$*

$s \in S, x \in I\}$ is a subring of R, $S \cap I$ is an ideal of S and there exists a ring isomorphism

$$\phi\colon S/S \cap I \to S + I/I$$

with $\phi(s + (S \cap I)) = s + I$ for all $s \in S$.

Proof For $s, s' \in S$ and $x, x' \in I$ one has $(s+x)(s'+x') = ss' + (sx' + xs' + xx') \in S + I$. Moreover, $1_R \in S \subseteq S + I$ and $S + I$ is an additive subgroup of R. Thus, $S + I$ is a subring of R. Since I is an ideal in R it is also an ideal in $S + I$. For $x \in S \cap I$ and $s \in S$ we have $sx \in S \cap I$ and also $xs \in S \cap I$. Since $S \cap I$ is an additive subgroup of S, it follows that $S \cap I$ is an ideal of S. Finally, the first isomorphism theorem for groups yields a group isomorphism $\phi\colon S/S \cap I \to S + I/I$ with $\phi(s + (S \cap I)) = s + I$. For $s, s' \in S$ we have $\phi((s + (S \cap I))(s' + (S \cap I))) = \phi(ss' + (S \cap I)) = ss' + I = (s + I)(s' + I) = \phi(s + (S \cap I))\phi(s + (S \cap I))$. Since also $\phi(1 + (S \cap I)) = 1 + I$, the group homomorphism ϕ is a ring homomorphism and the theorem is proved. □

10.10 Theorem (Corresp. Thm. and 2nd Isom. Thm. for Rings) *Let R be a ring, let I be an ideal of R and let $\nu\colon R \to R/I$ denote the natural epimorphism.*

(a) *The function $S \mapsto S/I$ defines a bijection between the subrings of R containing I and the subrings of R/I. Its inverse is $T \mapsto \nu^{-1}(T)$.*

(b) *The function $J \mapsto J/I$ defines a bijection between the left (resp. right, resp. two-sided) ideals of R containing I and the left (resp. right, resp. two-sided) ideals of R/I.*

(c) *If J is an ideal of R containing I then $(R/I)/(J/I) \cong (R/J)$ as rings.*

Proof This follows immediately from the correspondence theorem and the second isomorphism theorem for groups after verifying that images and preimages of (left, right) ideals (resp. subrings) under a ring epimorphism are again (left, right) ideals (resp. subrings). The latter is an easy homework problem. □

10.11 Theorem (Chinese Remainder Theorem) *Let R be a ring, let $n \in \mathbb{N}$, let $I_1, \ldots, I_n$ be ideals of R and denote by γ the function*

$$\gamma\colon R \to R/I_1 \times \cdots \times R/I_n\,, \quad r \mapsto (r + I_1, \ldots, r + I_n)\,.$$

(a) *γ is a ring homomorphism with* $\ker(\gamma) = \bigcap_{k=1}^{n} I_k$. *In particular, $R/(I_1 \cap \cdots \cap I_n)$ is isomorphic to a subring of $R/I_1 \times \cdots \times R/I_n$.*

(b) *If $I_k + I_l = R$ for all $k, l \in \{1, \ldots, n\}$ with $k \neq l$ then γ is surjective. In particular, in this case one has*

$$R/(I_1 \cap \cdots \cap I_n) \cong R/I_1 \times \cdots \times R/I_n\,.$$

(c) *If $I_k + I_l = R$ for all $k, l \in \{1, \ldots, n\}$ with $k \neq l$ and R is commutative then $I_1 \cap \cdots \cap I_n = I_1 \cdots I_n$. In particular, in this case one has*

$$R/(I_1 \cdots I_n) \cong R/I_1 \times \cdots \times R/I_n\,.$$

Proof (a) This is an easy verification.

(b) For each pair (k, l) with $k, l \in \{1, \ldots, n\}$ and $k \neq l$ we can find elements $a_{kl} \in I_k$ and $b_{kl} \in I_l$ such that $a_{kl} + b_{kl} = 1$. For every $l \in \{1, \ldots, n\}$ set $s_l := a_{1l}a_{2l} \cdots a_{nl}$, a product with $n-1$ factors (there is no factor a_{ll}). Then $s_l \in I_k$ for every $k \neq l$ and $s_l \in 1 + I_l$. The latter follows from $s_l = (1 - b_{1l})(1 - b_{2l}) \cdots (1 - b_{nl})$. To show the surjectivity of γ let $r_1, \ldots, r_n \in R$ be arbitrary and set $r := r_1s_1 + r_2s_2 + \ldots + r_ns_n$. By the above properties of the elements s_l, we have for every $k \in \{1, \ldots, n\}$ the equation $r + I_k = (r_1s_1 + I_k) + \cdots + (r_ns_n + I_k) = r_ks_k + I_k = (r_k + I_k)(s_k + I_k) = (r_k + I_k)(1 + I_k) = r_k + I_k$. Thus, $\gamma(r) = (r_1 + I_1, \ldots, r_n + I_n)$.

(c) Obviously, $I_1 \cdots I_n \subseteq I_1 \cap \cdots \cap I_n$. It suffices to show the other inclusion. We do this by induction on n. The case $n = 1$ is trivial. We also need to consider the case $n = 2$ for later use. Let a_{kl} and b_{kl} be as in the proof of part (b) (for $k, l \in \{1, 2\}$ with $k \neq l$). Then for every $r \in I_1 \cap I_2$ we have

$$r = r(a_{12} + b_{12}) = ra_{12} + rb_{12} = a_{12}r + rb_{12} \in I_1I_2, .$$

Finally, if $n \geqslant 3$ and a_{kl} and b_{kl} are as before then we have

$$1 = (a_{1n} + b_{1n}) \cdots (a_{n-1,n} + b_{n-1,n}) \in I_1 \cdots I_{n-1} + I_n$$

which implies that $(I_1 \cdots I_{n-1}) + I_n = R$. Note that by induction we have $I_1 \cdots I_{n-1} = I_1 \cap \cdots \cap I_{n-1}$. Using this and the case $n = 2$ applied to the two ideals $I_1 \cdots I_{n-1}$ and I_n we obtain $(I_1 \cap \cdots \cap I_{n-1}) \cap I_n \subseteq (I_1 \cdots I_{n-1}) \cap I_n \subseteq (I_1 \cdots I_{n-1})I_n$ and the theorem is proved. □

10.12 Corollary *Let $m_1, \dots, m_r \in \mathbb{N}$ be pairwise coprime and set $m := m_1 \cdots m_r$. Then*

$$\begin{aligned} \mathbb{Z}/m\mathbb{Z} &\to \mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_r\mathbb{Z} \\ a + m\mathbb{Z} &\mapsto (a + m_1\mathbb{Z}, \cdots, a + m_r\mathbb{Z}) \end{aligned}$$

is an isomorphism. In particular, for any $a_1, \dots, a_r \in \mathbb{Z}$, there exists $a \in \mathbb{Z}$ such that $a \equiv a_i \mod m_i$ for all $i \in \{1, \dots, r\}$. Moreover, the integer a is uniquely determined modulo m.

Proof Follows immediately from Theorem 10.11. □

10.13 Example Let $n = p_1^{e_1} \cdots p_r^{e_r}$ be the prime factorization of the natural number $n \geqslant 2$. Then

$$\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/p_1^{e_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_r^{e_r}\mathbb{Z}$$

as rings and in particular as additive groups. So, for example, $\mathbb{Z}/12\mathbb{Z} \cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$.

10.14 Definition The *Euler φ-function* (also called *Euler's totient function*) $\varphi\colon \mathbb{N} \to \mathbb{N}$ is defined by

$$\varphi(n) := |(\mathbb{Z}/n\mathbb{Z})^\times| \,.$$

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

(a) For $a \in \mathbb{Z}$ one has

$$\begin{aligned} & a + n\mathbb{Z} \in (\mathbb{Z}/n\mathbb{Z})^\times \\ \iff & \text{there exists } b \in \mathbb{Z} \text{ with } (a + n\mathbb{Z})(b + n\mathbb{Z}) = 1 + n\mathbb{Z} \\ \iff & \text{there exists } b \in \mathbb{Z} \text{ with } ab + n\mathbb{Z} = 1 + n\mathbb{Z} \\ \iff & \text{there exist } b, c \in \mathbb{Z} \text{ with } 1 = ab + nc \\ \iff & \gcd(a, n) = 1 \,. \end{aligned}$$

Thus, $\varphi(n) = |\{a \in \{1, \dots, n\} \mid \gcd(a, n) = 1\}|$.

(b) If $n = m_1 \cdots m_r$ with pairwise coprime natural numbers $m_1, \dots, m_r$ then the isomorphism in the Chinese Remainder Theorem induces an isomorphism of the unit groups

$$(\mathbb{Z}/n\mathbb{Z})^\times \cong (\mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_r\mathbb{Z})^\times = (\mathbb{Z}/m_1\mathbb{Z})^\times \times \cdots \times (\mathbb{Z}/m_r\mathbb{Z})^\times \,.$$

Thus, $\varphi(n) = \varphi(m_1)\cdots\varphi(m_r)$. In particular, if $n = p_1^{e_1}\cdots p_r^{e_r}$ is the prime factorization of n then $\varphi(n) = \varphi(p_1^{e_1})\cdots\varphi(p_r^{e_r})$.

(c) For a prime p, $e \in \mathbb{N}$ and $i \in \{1,\dots,p^e\}$ we have $\gcd(i,p^e) > 1$ if and only if $p \mid i$. This implies that $\varphi(p^e) = p^e - p^{e-1} = p^{e-1}(p-1)$.

Altogether, if $n = p_1^{e_1}\cdots p_r^{e_r}$ is the prime factorization of n then

$$\varphi(n) = p_1^{e_1-1}(p_1-1)\cdots p_r^{e_r-1}(p_r-1)\,.$$

10.16 Theorem (Fermat) *For every $n \in \mathbb{N}$ and $a \in \mathbb{Z}$ one has*

$$\gcd(a,n) = 1 \iff a^{\varphi(n)} \equiv 1 \mod n\,.$$

In particular, for a prime p and $a \in \mathbb{Z}$ one has

$$p \nmid a \iff a^{p-1} \equiv 1 \mod p$$

Proof If $\gcd(a,n) = 1$ then $a + n\mathbb{Z} \in (\mathbb{Z}/n\mathbb{Z})^\times$, by Remark 10.15(a), and $(a+n\mathbb{Z})^{\varphi(n)} = 1 + n\mathbb{Z}$, since the group $(\mathbb{Z}/n\mathbb{Z})^\times$ has order $\varphi(n)$. Conversely, if $a^{\varphi(n)} \equiv 1 \mod n$ then there exists $q \in \mathbb{Z}$ with $a^{\varphi(n)} - qn = 1$. This implies $\gcd(a,n) = 1$. □

10.17 Definition Let R be a ring. An ideal M of R is called *maximal* if $M \neq R$ and if there exists no ideal I of R with $M \subset I \subset R$. Note that by the correspondence theorem we have for every ideal M of R: M is a maximal ideal of R if and only if R/M is a quasi-simple ring. Similarly, one defines maximal left and right ideals.

10.18 Proposition *Let R be a commutative ring. Then, R is quasi-simple if and only if R is a field.*

Proof $\Rightarrow$: Let $a \in R \smallsetminus \{0\}$. As R is quasi-simple we have $aR = R$. This implies that there exists $b \in R$ with $ab = 1$. Thus a is a unit of R. By definition, R is a field.

$\Leftarrow$: This is immediate, since every non-zero ideal contains a unit, and therefore is equal to R. □

10.19 Definition Let R be a commutative ring. An ideal P of R is called a *prime ideal* if $P \neq R$ and if P has the following property: For all $a, b \in R$ with $ab \in P$ one has $a \in P$ or $b \in P$.

10.20 Proposition *Let R be a commutative ring and let I be an ideal of R.*

(a) I is a maximal ideal of $R \iff R/I$ is a field.

(b) I is a prime ideal of $R \iff R/I$ is an integral domain.

Proof (a) I is maximal if and only if R/I is quasi-simple. By Proposition 10.18, R/I is quasi-simple if and only if R/I is a field.

(b) $\Rightarrow$: $R/I \neq \{0\}$, since $I \neq R$. Let $a, b \in R$ with $(a+I)(b+I) = 0_{R/I}$. Then $ab + I = I$ and $ab \in I$. Since I is a prime ideal we have $a \in I$ or $b \in I$. Thus, $a + I = I = 0_{R/I}$ or $b + I = I = 0_{R/I}$.

$\Leftarrow$: Since $R/I \neq \{0\}$ we have $I \neq R$. Let $a, b \in R$ with $ab \in I$. Then $0_{R/I} = ab + I = (a+I)(b+I)$. Since R/I is an integral domain, we obtain $a + I = 0_{R/I}$ or $b + I = 0_{R/I}$. Thus, $a \in I$ or $b \in I$. □

10.21 Examples (a) By Proposition 10.20, in a commutative ring R every maximal ideal is a prime ideal, but in general not every prime ideal is maximal. For instance, $\{0\}$ is a prime ideal of $\mathbb{Z}$ but not a maximal ideal.

(b) Let $n \in \mathbb{N}_0$. The ideal $n\mathbb{Z}$ is a maximal ideal of $\mathbb{Z}$ if and only if n is a prime. Thus, $\mathbb{Z}/n\mathbb{Z}$ is a field if and only if n is a prime. Moreover, the prime ideals of $\mathbb{Z}$ are the ideals $p\mathbb{Z}$, with p a prime, together with the trivial ideal $\{0\}$.

10.22 Definition (a) A *partially ordered set* $(X, \leqslant)$ is a set X together with a relation $\leqslant$ satisfying:

(i) $x \leqslant x$,

(ii) $x \leqslant y$ and $y \leqslant x \Rightarrow x = y$, and

(iii) $x \leqslant y$ and $y \leqslant z \Rightarrow x \leqslant z$,

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

A partially ordered set $(X, \leqslant)$ is called *totally ordered* if for every $x, y \in X$ one has $x \leqslant y$ or $y \leqslant x$.

(b) Let $(X, \leqslant)$ be a partially ordered set and let $Y \subseteq X$. An element $x \in X$ is called an *upper bound* of Y if $y \leqslant x$ for all $y \in Y$.

(c) Let $(X, \leqslant)$ be a partially ordered set. An element $x \in X$ is called *maximal* in X if for every element $y \in X$ one has: $x \leqslant y \Rightarrow x = y$.

10.23 Lemma (Zorn's Lemma) *Let $(X, \leqslant)$ be a non-empty partially ordered set and assume that every totally ordered subset of X has an upper bound in X. Then X has a maximal element.*

10.24 Remark We do not prove Zorn's Lemma. It is equivalent to the axiom of choice which is used as one of the axioms in set theory. Zorn's Lemma is for example used in the proof that every vector space has a basis. We illustrate its use in the following theorem.

10.25 Theorem *Let R be a ring and let I be a left (resp. right, resp. two-sided) ideal of R with $I \neq R$. Then there exists a maximal left (resp. right, resp, two-sided) ideal M of R with $I \leqslant M$. In particular, every non-zero ring has maximal left, right and two-sided ideals.*

Proof We only prove the statement about left ideals. The others are proved in the same way. Consider the set $\mathcal{X}$ of all left ideals J of R with $I \subseteq J \subset R$. This set is non-empty (as $I \in \mathcal{X}$) and partially ordered by inclusion. Let $\mathcal{Y}$ be a totally ordered subset of $\mathcal{X}$. By Zorn's Lemma it suffices to show that there exists an upper bound for $\mathcal{Y}$ in $\mathcal{X}$. Let J_* denote the union of all elements J of $\mathcal{Y}$. Then it is easy to see that J_* is again a left ideal. Obviously, it contains all elements of $\mathcal{Y}$, so it is an upper bound of $\mathcal{Y}$. We still need to show that $J_* \in \mathcal{X}$. Since $I \subseteq J_*$, it suffices to show that $J_* \neq R$. Assume that $J_* = R$. Then $1 \in J_*$. Since J_* is the union of the left ideals $J \in \mathcal{Y}$, there exists $J \in \mathcal{Y}$ such that $1 \in J$. But this is a contradiction, since every element $J \in \mathcal{X}$ satisfies $J \neq R$. Thus, $J_* \neq R$, $J_* \in \mathcal{X}$, and the proof is complete. □

Exercises

1. Let $f\colon R \to S$ be a ring homomorphism. Show the following statements.

(a) If T is a subring of R then $f(T)$ is a subring of S.

(b) If U is a subring of S then $f^{-1}(U)$ is a subring of R.

(c) If J is a left (resp. right, resp. two-sided) ideal of S then $f^{-1}(J)$ is a left (resp. right, resp. two-sided) ideal of R.

(d) If f is surjective and I left (resp. right, resp. two-sided) ideal of R then $f(I)$ is a left (resp. right, resp. two-sided) ideal of S.

2. Let D be a division ring.

(a) Show that $\{0\}$ and D are the only ideals of D.

(b) Let R be a non-trivial ring and let $f\colon D \to R$ be a ring homomorphism. Show that f is injective.

3. (a) Let F be a field. Show that the characteristic of F is either a prime number or 0.

(b) Let p be a prime and let R be a ring with p elements. Show that $R \cong \mathbb{Z}/p\mathbb{Z}$ as rings.

4. Let R be a ring. An element $r \in R$ is called *nilpotent* if there exists $n \in \mathbb{N}$ such that $r^n = 0$.

(a) Show that if $r \in R$ is nilpotent then $1 - r$ is a unit of R.

(b) Show that if R is commutative then the nilpotent elements of R form an ideal N of R.

(c) Show that if R is commutative and N is the ideal of nilpotent elements then 0 is the only nilpotent element of R/N.

5. Let $G =< a >$ be a multiplicatively written cyclic group of order n.

(a) Show that, for every $k \in \mathbb{N}$, the order of the element a^k is equal to $n/\gcd(k, n)$.

(b) Show that G has $\varphi(n)$ generators.

(c) Show that $\sum_{d|n} \varphi(d) = n$. (Hint: Use Problem 3.8 and count elements of order d in G.)

(d) Let H be a finite group of order n and assume that H has at most one subgroup of order d for every divisor d of n. Show that H is cyclic. (Hint: Count elements of H of given order and use (c).)

6. Let R be a ring and let $n \in \mathbb{N}$.

(a) Show that if I is an ideal of R then the set $\mathrm{Mat}_n(I)$ of all matrices with entries in I is an ideal of $\mathrm{Mat}_n(R)$.

(b) Show that every ideal of $\mathrm{Mat}_n(R)$ is of the form $\mathrm{Mat}_n(I)$ for some ideal I of R. (Hint: Let J be an ideal of $\mathrm{Mat}_n(R)$ and let I be the set of all elements of R which occur in some matrix in J. Show that I is an ideal and that $J = \mathrm{Mat}_n(I)$.)

(c) Let D be a division ring and let $n \in \mathbb{N}$. Show that the matrix ring $\mathrm{Mat}_n(D)$ is a quasi-simple ring.

7. Let I be the ideal of $\mathbb{Z}[X]$ generated by the elements 2 and X.

(a) Show that a polynomial

$$a_0 + a_1X + \cdots + a_nX^n \in \mathbb{Z}[X]$$

belongs to I if and only if a_0 is even.

(b) Show that I is a maximal ideal of $\mathbb{Z}[X]$.

11 Divisibility in Integral Domains

Throughout this section R denotes an integral domain. Thus, R is a commutative ring with $1 \neq 0$ and $ab = 0$ implies $a = 0$ or $b = 0$ for all $a, b \in R$.

11.1 Definition Let a and b be elements of R.

(a) One says that a *divides* b in R (notation $a \mid b$) if there exists $c \in R$ with $ac = b$.

(b) One says that a and b are *associate* in R (notation $a \sim b$) if $a \mid b$ and $b \mid a$.

11.2 Remark Let $a, b, c, b_1, \ldots, b_n, r_1, \ldots, r_n \in R$ and let $u \in R^\times$. Then the following rules are easily verified from the definitions:

(a) $a \mid a$ and $a \mid 0$.

(b) $0 \mid a$ if and only if $a = 0$.

(c) $u \mid a$.

(d) $a \mid u$ if and only if $a \in R^\times$.

(e) If $a \mid b$ and $b \mid c$ then $a \mid c$.

(f) If $a \mid b_1, \ldots, a \mid b_n$ then $a \mid r_1 b_1 + \cdots r_n b_n$.

(g) $a \mid b$ if and only if $bR \subseteq aR$.

(h) $\sim$ is an equivalence relation on R.

11.3 Proposition *For $a, b \in R$ the following are equivalent:*

(i) $a \sim b$.

(ii) $aR = bR$.

(iii) *There exists $u \in R^\times$ with $au = b$.*

Proof (i) $\iff$ (ii): This is immediate from Remark 11.2(g).

(ii)$\Rightarrow$(iii): First note that if $a = 0$ then also $b = 0$, since $b \in aR$, and then $a \cdot 1 = b$. We assume from now on that $a \neq 0$. Since $aR = bR$ there exist $c, d \in R$ such that $b = ac$ and $a = bd$. Substituting the first expression for b in the last equation we obtain $a = acd$. This implies $a - acd = 0$ and $a(1 - cd) = 0$. Since $a \neq 0$ and since R is an integral domain, we obtain $1 = cd$. In particular $c \in R^\times$ and (iii) holds.

(iii)$\Rightarrow$(i): Obviously, $au = b$ implies $a \mid b$. Since u is a unit in R we also have $a = bu^{-1}$ and therefore $b \mid a$. □

11.4 Remark (a) In $\mathbb{Z}$, every integer a is associate to a and to $-a$, and to no other element.

(b) $\{a \in R \mid a \sim 1\} = R^\times$ and $\{a \in R \mid a \sim 0\} = \{0\}$.

(c) The group $R^\times$ acts on R by left multiplications: $(u, a) \mapsto ua$. The orbits of this group action are the equivalence classes with respect to $\sim$.

(d) For $a_1, \ldots, a_n \in R$ one has

$$(a_1, \ldots, a_n) = \{r_1 a_1 + \cdots r_n a_n \mid r_1, \ldots, r_n \in R\} = a_1 R + \cdots + a_n R\,.$$

(e) For $d \in R$ and $a_1, \ldots, a_n \in R$ one has

$$\begin{aligned} d \mid a_1, \ldots, d \mid a_n \iff a_1 \in dR, \ldots, a_n \in dR &\iff (a_1, \ldots, a_n) \subseteq dR \\ &\iff a_1 R + \cdots + a_n R \subseteq dR\,. \end{aligned}$$

In this case the element d is called a *common divisor* of $a_1, \ldots, a_n$. Every unit is a common divisor of $a_1, \ldots, a_n$. If these are the only common divisors of $a_1, \ldots, a_n$ then we call $a_1, \ldots, a_n$ *coprime*. The elements $a_1, \ldots, a_n$ are called *pairwise coprime* if a_i and a_j are coprime whenever $i \neq j$. For instance, -6, 15 and 10 are coprime in $\mathbb{Z}$, but they are not pairwise coprime.

(f) For $m \in R$ and $a_1, \ldots, a_n \in R$ one has

$$a_1 \mid m, \ldots, a_n \mid m \iff m \in a_1 R, \ldots, m \in a_n R \iff mR \subseteq a_1 R \cap \cdots \cap a_n R\,.$$

In this case we call m a *common multiple* of $a_1, \ldots, a_n$.

11.5 Definition Let $a_1, \ldots, a_n \in R$.

(a) A common divisor d of $a_1, \ldots, a_n$ is called a *greatest common divisor* of $a_1, \ldots, a_n$ if every common divisor of $a_1, \ldots, a_n$ divides d. The set of all greatest common divisors of $a_1, \ldots, a_n$ is denoted by $\gcd(a_1, \ldots, a_n)$.

(b) A common multiple m of $a_1, \ldots, a_n$ is called a *least common multiple* of $a_1, \ldots, a_n$ if m divides every common multiple of $a_1, \ldots, a_n$. The set of all least common multiples of $a_1, \ldots, a_n$ is denoted by $\mathrm{lcm}(a_1, \ldots, a_n)$.

11.6 Remark A greatest common divisor (resp. least common multiple) of $a_1, \ldots, a_n \in R$ does not exist in general. But if there exists one then $\gcd(a_1, \ldots, a_n)$ (resp. $\mathrm{lcm}(a_1, \ldots, a_n)$) is a single full associate class (verify!). For instance, in $\mathbb{Z}$ we have $\gcd(6, 15) = \{-3, 3\}$ and $\mathrm{lcm}(6, 15) = \{-30, 30\}$.

11.7 Example We want to take a closer look at the ring $R := \mathbb{Z}[\sqrt{5}i] = \{a + b\sqrt{5}i \mid a, b \in \mathbb{Z}\}$. A useful tool to study R is the *norm map* $N\colon R \to \mathbb{N}_0$ defined by

$$N(a + b\sqrt{5}i) := (a + b\sqrt{5}i)(a - b\sqrt{5}i) = |a + b\sqrt{5}i|^2 = a^2 + 5b^2 . \quad (11.7.a)$$

One has $N(rs) = N(r)N(s)$ for all $r, s \in R$. Thus, for $r, t \in R$, we have

$$r \mid t \text{ in } R \;\Rightarrow N(r) \mid N(t) \text{ in } \mathbb{Z}. \quad (11.7.b)$$

First we show that $R^\times = \{-1, 1\}$. Clearly, 1 and -1 are units in R. Conversely, assume that $u \in R^\times$. Then, by (11.7.b), $N(u)N(u^{-1}) = N(1) = 1$ and $N(u) = 1$ or $N(u) = -1$. But $a^2 + 5b^2 = 1$ has precisely two solutions, namely $(a, b) = (\pm 1, 0)$ (corresponding to $u = \pm 1$) and $a^2 + 5b^2 = -1$ has no solution.

In the sequel we will show that the elements $r := 6$ and $s := 2(1 + \sqrt{5}i)$ of R don't have a greatest common divisor. First we determine all common divisors of r and s. Assume that $t = a + b\sqrt{5}i$ is a common divisor of r and s. Then, since the norm map is multiplicative, $N(t) = a^2 + 5b^2$ is a divisor of $N(r) = 36$ and also a divisor of $N(s) = 24$. Thus, $N(t)$ is a divisor of 12. This implies that $a^2 + 5b^2 \in \{1, 2, 3, 4, 6, 12\}$. By inspection one finds that 2, 3 and 12 are not of the form $a^2 + 5b^2$. Moreover,

$$\begin{aligned} N(t) = 1 &\iff t \in \{\pm 1\}, \\ N(t) = 4 &\iff t \in \{\pm 2\}, \\ N(t) = 6 &\iff t \in \{\pm(1 + \sqrt{5}i), \pm(1 - \sqrt{5}i)\}. \end{aligned}$$

Clearly, $\pm 1, \pm 2, \pm(1 + \sqrt{5}i)$ are common divisors of 6 and $2(1 + \sqrt{5}i)$. On the other hand, $1 - \sqrt{5}i \nmid 2(1 + \sqrt{5}i)$, since

$$\frac{2 + 2\sqrt{5}i}{1 - \sqrt{5}i} = \frac{(2 + 2\sqrt{5}i)(1 + \sqrt{5}i)}{6} = \frac{-8 + 4\sqrt{5}i}{6} = -\frac{1}{3} + \frac{2}{3}\sqrt{5}i \notin R .$$

Thus, ± 1, ± 2 and $\pm(1 + \sqrt{5}i)$ are the common divisors of r and s. But none of them is a greatest common divisor, since $N(\pm 1) = 1$, $N(\pm 2) = 4$ and $N(\pm(1 + \sqrt{5}i)) = 6$.

11.8 Definition Let $p \in R \smallsetminus \{0\}$ and assume that p is not a unit in R.

(a) p is called *irreducible* if for all $a, b \in R$ one has: $p = ab \Rightarrow a \in R^\times$ or $b \in R^\times$.

(b) p is called a *prime element* if for all $a, b \in R$ one has: $p \mid ab \Rightarrow p \mid a$ or $p \mid b$.

11.9 Remark (a) If $p \in R$ is irreducible (resp. a prime element) in R then every element of R that is associated to p is as well irreducible (resp. a prime element).

(b) If p is a prime element then p is irreducible. In fact assume that $p = ab$ with $a, b \in R$. Since p is a prime element it follows that $p \mid a$ or $p \mid b$. Without loss of generality, assume that $p \mid a$. Then $a = pc$ for some $c \in R$. It follows that $p = ab = pcb$. This implies that $bc = 1$ and that $b \in R^\times$, as desired.

11.10 Example (a) For $R = \mathbb{Z}$ and $p \in \mathbb{Z}$ on has: p is a prime element $\iff$ p is irreducible $\iff$ $|p|$ is a prime number.

(b) In $R = \mathbb{Z}[\sqrt{5}i]$ the element $p := 1+\sqrt{5}i$ is irreducible. In fact, assume that $1 + \sqrt{5}i = rs$. Then $6 = N(1 + \sqrt{5}i) = N(r)N(s)$. Since 2 and 3 are not in the image of N, we obtain $N(r) = 1$ or $N(s) = 1$. But this means $r = \pm 1 \in R^\times$ or $s = \pm 1 \in R^\times$, as desired. However, p is not a prime element, since $p \mid p(1-\sqrt{5}i) = 6 = 2 \cdot 3$ but $p \nmid 2$ and $\nmid 3$ (because $N(p) = 6$, $N(2) = 4$ and $N(3) = 9$).

11.11 Proposition *Let $p \in R \smallsetminus \{0\}$. Then p is a prime element in R if and only if pR is a prime ideal of R.*

Proof $\Rightarrow$: Since p is not a unit, we have $pR \neq R$. Assume that $a, b \in R$ are such that $ab \in pR$. Then $p \mid ab$. Since p is a prime element, we obtain $p \mid a$ or $p \mid b$. This implies $a \in pR$ or $b \in pR$ as desired.

$\Leftarrow$: Since $pR \neq R$, the element p is not a unit in R. Assume that $a, b \in R$ are such that $p \mid ab$. Then $ab \in pR$, and since pR is a prime ideal, we obtain $a \in pR$ or $b \in pR$. But this means $p \mid a$ or $p \mid b$, as desired. □

11.12 Theorem *Assume that $r, s \in \mathbb{N}_0$ and that $p_1, \ldots, p_r$ and $q_1, \ldots, q_s$ are prime elements in R such that $p_1 \cdots p_r = q_1 \cdots q_s$. Then $r = s$ and after a suitable renumbering of the elements $q_1, \ldots, q_s$ one has $p_i \sim q_i$, for all $i = 1, \ldots, r$.*

Proof We prove the result by induction on r. Let $r = 0$. Then $q_1 \cdots q_s = 1$. If $s > 0$ then q_1 is a unit in contradiction to being a prime element. Therefore, $s = 0$. Now let $r \geqslant 1$ and assume that the statement is true for all smaller values of r. Since $p_1 \cdots p_r = q_1 \cdots q_s$, we have $p_r \mid q_1 \cdots q_s$. Since p_r is a prime element, we have $p_r \mid q_i$ for some $i = 1, \ldots, s$. After renumbering the elements $q_1, \ldots, q_s$ we may assume that $p_r \mid q_s$. Then there exists $u \in R$ with $q_s = up_r$. As q_s is also irreducible by Remark 11.9, we have $u \in R^\times$ and p_r is associated to q_s. Now we have $p_1 \cdots p_r = q_1 \cdots q_{s-1} u p_r$ and after canceling p_r on both sides we have $p_1 \cdots p_{r-1} = q_1 \cdots q_{s-2}(q_{s-1}u)$. Thus, by induction, $r - 1 = s - 1$, and after reordering the elements $q_1, \ldots, q_{s-2}, q_{s-1}$, we have $p_1 \sim q_1$, …, $p_{r-2} \sim q_{r-2}$ and $p_{r-1} \sim q_{r-1}u \sim q_{r-1}$. □

Exercises

1. Prove the statements in Remark 11.2.

2. Let $R := \mathbb{Z}[\sqrt{5}i] = \{a + b\sqrt{5}i \mid a, b \in \mathbb{Z}\}$.

(a) Compute all common divisors of 9 and $3(2 + \sqrt{5}i)$.

(b) Do 9 and $3(2 + \sqrt{5}i)$ have a greatest common divisor?

(c) Consider the ideal $I := (2, 1 + \sqrt{5}i)$. Show that I is not principal. Show that R/I has precisely 2 elements. Show that $I^2 = (2)$.

(d) Show that $R/2R$ is a ring with 4 elements which is neither isomorphic to $\mathbb{Z}/4\mathbb{Z}$ nor to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

3. Show that the ideal (X) of $\mathbb{Z}[X]$ is a prime ideal but not a maximal ideal.

4. Let R be an integral domain and let $a_1, \ldots, a_n \in R$. Consider the partially ordered set $\mathcal{I}$ of principal ideals I of R which contain $(a_1, \ldots, a_n)$ (partially ordered by inclusion). Show that the set $\gcd(a_1, \ldots, a_n)$ is non-empty if and only if the poset $\mathcal{I}$ has a smallest element (i.e., an element dR satisfying $dR \subseteq I$ for all $I \in \mathcal{I}$), by showing the following more precise statements:

(a) If $d \in \gcd(a_1, \ldots, a_n)$ then dR is the smallest element in $\mathcal{I}$.

(b) If $\mathcal{I}$ has a smallest element dR then $d \in \gcd(a_1, \ldots, a_n)$.

5. Let R be an integral domain and let $a \in R \smallsetminus \{0\}$. Show that the following are equivalent:

(i) a is irreducible.

(ii) aR is maximal in the set of all principal ideals different from R (partially ordered by inclusion).

12 Unique Factorization Domains (UFD), Principal Ideal Domains (PID), and Euclidean Domains

Throughout this section R denotes an integral domain.

12.1 Definition The integral domain R is called a *unique factorization domain* (or UFD) if every non-zero element $a \in R$ with $a \notin R^\times$ can be written as a product of prime elements. Note that in this case these prime elements are uniquely determined by a in the sense of Theorem 11.12.

12.2 Theorem *The following are equivalent:*

(i) *R is a unique factorization domain.*

(ii) *Every non-zero element $a \in R$ with $a \notin R^\times$ can be written as a product of irreducible elements and if $p_1 \cdots p_r = q_1 \cdots q_s$ with irreducible elements $p_1, \ldots, p_r, q_1, \ldots, q_s \in R$ then $r = s$ and $p_i \sim q_i$ after a suitable renumbering of the elements $q_1, \ldots, q_s$.*

(iii) *Every non-zero element $a \in R$ with $a \notin R^\times$ can be written as a product of irreducible elements and every irreducible element of R is a prime element.*

Proof (iii)⇒(i): This is obvious.

(iii)⇒(ii): This is immediate from Theorem 11.12.

(i)⇒(iii): Since every prime element is irreducible, it suffices to show that every irreducible element a of R is a prime element. By (i), there exist prime elements $p_1, \ldots, p_r$ of R with $a = p_1 \cdots p_r$. Since a is irreducible, we have $r = 1$ and $a = p_1$ is a prime element.

(ii)⇒(iii): We need to show that every irreducible element p of R is a prime element. Assume that $p \mid ab$ for $a, b \in R$. Then $pc = ab$ for some $c \in R$. We may assume that $a \neq 0$ (since otherwise $p \mid a$ and we are done) and that $b \neq 0$. Also, we may assume that $a \notin R^\times$ (since otherwise $pca^{-1} = b$ and $p \mid b$ so that we are done) and $b \notin R^\times$. Then also $0 \neq c \notin R^\times$ (since if c is a unit then $p = (c^{-1}a)b$ can be written as a product of two non-units, contradicting the fact that p is a prime element). Thus, we can write $a = p_1, \ldots, p_k$, $b = q_1, \ldots, q_l$, $c = r_1, \ldots, r_m$ as product of irreducible elements and obtain $pr_1 \cdots r_m = p_1 \cdots p_k q_1 \cdots q_l$. The uniqueness part of (ii) implies that $p \sim p_i$ or $p \sim q_j$ for some $i \in \{1, \ldots, l\}$ or $j \in \{1, \ldots, l\}$. Thus, $p \mid a$ or $p \mid b$. □

12.3 Remark Assume that R is a UFD and let $\mathcal{P}$ be a set of representatives for the prime elements of R with respect to the equivalence relation $\sim$. Then every element $a \in R \smallsetminus \{0\}$ has a unique prime factorization

$$a = u \prod_{p \in \mathcal{P}} p^{e_p}$$

with $u \in R^\times$, $e_p \in \mathbb{N}_0$ such that $e_p = 0$ for all but finitely many $p \in \mathcal{P}$. Let also $b \in R \smallsetminus \{0\}$ and let $b = v \prod_{p \in \mathcal{P}} p^{f_p}$ be its prime factorization. Then the following statements follow easily from the unique prime factorization:

(a) $a \mid b \iff e_p \leqslant f_p$ for all $p \in \mathcal{P}$.

(b) $\prod_{p \in \mathcal{P}} p^{\min\{e_p, f_p\}}$ is a greatest common divisor of a and b.

(c) $\prod_{p \in \mathcal{P}} p^{\max\{e_p, f_p\}}$ is a least common multiple of a and b.

(d) a and b are coprime (i.e., $1 \in \gcd(a, b)$) if and only if, for every $p \in \mathcal{P}$, one has $e_p = 0$ or $f_p = 0$.

(e) If $d \in \gcd(a, b)$ and $m \in \operatorname{lcm}(a, b)$ then $ab \sim dm$.

(f) If a and b are coprime and $c \in R$ satisfies $a \mid c$ and $b \mid c$, then $ab \mid c$.

12.4 Example (a) $\mathbb{Z}$ is a UFD and we may choose for $\mathcal{P}$ the set of positive prime numbers.

(b) $\mathbb{Z}[\sqrt{5}i]$ is not a UFD, since $1 + \sqrt{5}i$ is irreducible but not a prime element, cf. Example 11.10

12.5 Definition R is called a *principal ideal domain* (or PID) if every ideal I of R is principal, i.e., $I = (a) = aR$ for some element $a \in R$.

12.6 Example $\mathbb{Z}$ is a PID, since every ideal of $\mathbb{Z}$ is of the form $n\mathbb{Z}$ for some $n \in \mathbb{N}_0$.

12.7 Proposition *Assume that R is a PID and let $p \in R \smallsetminus \{0\}$. Then the following are equivalent:*

(i) *(p) is a maximal ideal.*

(ii) *(p) is a prime ideal.*

(iii) *p is a prime element.*

(iv) *p is irreducible.*

Proof (i) $\Rightarrow$ (ii): This was shown in Example 10.21.

(ii) $\Longleftrightarrow$ (iii): This is the statement of Proposition 11.11.

(iii) $\Rightarrow$ (iv): This was shown in Remark 11.9(b).

(iv) $\Rightarrow$ (i): We have $(p) \neq R$, since $p \notin R^\times$. Now assume that I is an ideal of R with $(p) \subseteq I \neq R$. We will show that $I = (p)$. Since R is a PID, there exists $a \in R$ with $I = (a)$. It follows that $p = ab$ for some $b \in R$. Since $I \neq R$, a is not a unit. Since p is irreducible, the element b must be a unit in R. Since $p = ab$, we obtain $(p) = (a) = I$. This shows (i). $\square$

12.8 Theorem *If R is a PID then R is a UFD.*

Proof Assume that R is not a UFD. Then, by Proposition 12.7 and Theorem 12.2, there exists a non-zero element $a_1 \in R \smallsetminus R^\times$ such that a_1 is not a product of irreducible elements. In particular, a_1 is not irreducible itself. Thus, we can write $a_1 = a_2 b_2$ with non-zero elements $a_2, b_2 \in R \smallsetminus R^\times$. Since a_1 is not a product of irreducible elements the same must be true for a_2 or b_2. After interchanging a_2 with b_2 we may assume that a_2 is not a product of irreducible elements. Note that, since b_2 is not a unit in R, we have $(a_1) \subset (a_2)$. We can repeat the above with a_2 in place of a_1 to obtain an element a_3 which is not a product of irreducible elements such that $(a_2) \subset (a_3)$. We can iterate this process to obtain an infinite strictly ascending chain $(a_1) \subset (a_2) \subset (a_3) \subset \cdots$. Note that $I := \bigcup_{n \in \mathbb{N}} (a_n)$ is an ideal of R. Since R is a PID, there exists $a \in I$ such that $I = (a)$. But by the construction of I there exists $n \in \mathbb{N}$ such that $a \in (a_n)$. This implies $(a) \subseteq (a_n)$ and we obtain the contradiction $(a) \subseteq (a_n) \subset (a_{n+1}) \subseteq I = (a)$. Thus, R is a UFD. $\square$

12.9 Theorem (Bezout) *Let R be a PID and let $a_1, \ldots, a_n, d \in R$.Then,*

$$d \in \gcd(a_1, \ldots, a_n) \iff (d) = (a_1, \ldots, a_n)\,.$$

In particular, if $d \in \gcd(a_1, \ldots, a_n)$ then there exist $r_1, \ldots, r_n \in R$ such that $d = r_1 a_1 + \cdots + r_n a_n$.

Proof $\Rightarrow$: There exists $a \in R$ with $(a_1, \ldots, a_n) = (a)$. From Remark 11.4(e) it follows that $a \in \gcd(a_1, \ldots, a_n)$. Since also $d \in \gcd(a_1, \ldots, a_n)$ we have $a \sim d$. Thus, $(d) = (a) = (a_1, \ldots, a_n)$.

$\Leftarrow$: This follows immediately from Remark 11.4(e). $\square$

12.10 Corollary *Let R be a PID and let $a_1, \ldots, a_n \in R$. Then $a_1, \ldots, a_n$ are coprime if and only if there exist $r_1, \ldots, r_n \in R$ with $1 = r_1a_1 + \cdots + r_na_n$.*

Proof This is immediate from Theorem 12.9. □

12.11 Definition R is called a *Euclidean domain* if there exists a function $N\colon R \to \mathbb{N}_0$ with $N(0) = 0$ such that for any two elements $a, b \in R$ with $b \neq 0$ there exist $q, r \in R$ with $a = bq + r$ and with $r = 0$ or $N(r) < N(b)$. In this case, N is called a *Euclidean norm* for R. (A Euclidean domain can have more than one Euclidean norm.)

12.12 Example (a) The ring $\mathbb{Z}$ is a Euclidean domain with $N\colon \mathbb{Z} \to \mathbb{N}_0$, $a \mapsto |a|$.

(b) For every field F the polynomial ring $F[X]$ is a Euclidean domain with $N\colon F[X] \to \mathbb{N}_0$ defined by $N(0) := 0$ and $N(p(X)) := \deg(p(X))$ for $p(X) \in F[X] \smallsetminus \{0\}$. (See Homework problem).

(c) The ring of Gaussian integers, $R := \mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$, is a Euclidean domain with $N\colon \mathbb{Z}[i] \mapsto \mathbb{N}_0$, $\alpha = a + bi \mapsto a^2 + b^2 = \alpha\overline{\alpha} = |\alpha|^2$. In fact, let $\alpha, \beta \in R$ with $\beta \neq 0$. We can write $\alpha/\beta = x + yi$ with $x, y \in \mathbb{Q}$. Choose $m, n \in \mathbb{Z}$ such that $|x - m| \leqslant 1/2$ and $|y - n| \leqslant 1/2$, and set $\gamma := m + ni \in R$ and $\rho := \alpha - \beta\gamma \in R$. Obviously, $\alpha = \gamma\beta + \rho$ and

$$\begin{aligned} N(\rho) &= |\alpha - \beta\gamma|^2 = |\beta|^2|\frac{\alpha}{\beta} - \gamma|^2 = N(\beta)|(x - m) + (y - n)i|^2 \\ &= N(\beta)((x - m)^2 + (y - n)^2) \leqslant N(\beta)((\frac{1}{2})^2 + (\frac{1}{2})^2) \leqslant \frac{1}{2}N(\beta) \\ &< N(\beta)\,, \end{aligned}$$

since $N(\beta) \neq 0$. Here we used that the norm map N is also defined (and multiplicative) on $\mathbb{Q}[i]$, even on $\mathbb{C}$, by $N(a + bi) = a^2 + b^2$ for $a, b \in \mathbb{R}$.

12.13 Theorem *If R is a Euclidean domain then R is a PID. More precisely, if N is a Euclidean norm for R and if $I \neq \{0\}$ is an ideal of R then $I = (b)$ for every $b \in I \smallsetminus \{0\}$ with $N(b) = \min\{N(a) \mid a \in I \smallsetminus \{0\}\}$.*

Proof It suffices to show the second statement. Since $b \in I$, one has $(b) \subseteq I$. Conversely, let $a \in I$. Since $b \neq 0$, there exist $q, r \in R$ with $a = qb + r$ and with $r = 0$ or $N(r) < N(b)$. Note that $r = a - qb \in I$. If $r \neq 0$ then $N(r) < N(b)$ contradicting our choice of b. Thus, $r = 0$ and $a = qb \in I$. □

12.14 Remark (Euclidean Algorithm) Assume that R is a Euclidean domain and that N is a Euclidean norm for R. For $a, b \in R \smallsetminus \{0\}$ one can compute a greatest common divisor d of a and b and also elements $r, s \in R$ with $d = ra + sb$ using the *Euclidean Algorithm*, i.e., by finding elements $n \in \mathbb{N}_0$, $q_1, \ldots, q_{n+1} \in R$ and $r_1, \ldots, r_n \in R$ with

$$\begin{aligned} a &= q_1 b + r_1, & r_1 &\neq 0, & N(r_1) &< N(b), \\ b &= q_2 r_1 + r_2, & r_2 &\neq 0, & N(r_2) &< N(r_1), \\ r_1 &= q_3 r_2 + r_3, & r_3 &\neq 0, & N(r_3) &< N(r_2), \\ &\vdots & &\vdots & &\vdots \\ r_{n-2} &= q_n r_{n-1} + r_n, & r_n &\neq 0, & N(r_n) &< N(r_{n-1}), \\ r_{n-1} &= q_{n+1} r_n \, . \end{aligned}$$

Then r_n is a greatest common divisor of a and b and can be expressd as a linear combination of a and b using the above equations. (If already $r_1 = 0$ then b is a greatest common divisor of a and b.)

More explicitly: Compute triples $(u_i, v_i, w_i) \in R^3$, $i = 0, 1, \ldots$, recursively as follows:

Step 1: Set $(u_0, v_0, w_0) := (1, 0, a)$ and $(u_1, v_1, w_1) := (0, 1, b)$.

Step 2: If (u_i, v_i, w_i) with $w_i \neq 0$ is computed then find elements q_i and r_i with

$$w_{i-1} = q_i w_i + r_i \text{ such that } r_i = 0 \text{ or } N(r_i) < N(w_i)$$

and set

$$(u_{i+1}, v_{i+1}, w_{i+1}) := (u_{i-1}, v_{i-1}, w_{i-1}) - q_i(u_i, v_i, w_i) \, .$$

If $w_{i+1} = 0$ then $w_i \in \gcd(a, b)$ and $w_i = u_i a + v_i b$. If $w_{i+1} \neq 0$ then repeat Step 2.

Exercises

1. Let F be a field and let $f(X) \in F[X]$ be a polynomial in the indeterminate X with coefficients in F. Let $g(X) \in F[X]$ be a non-zero polynomial. Show that there exist polynomials $q(X), r(X) \in F[X]$ such that $f(X) = q(X)g(X) + r(X)$ and $\deg(r(X)) < \deg(g(X))$. This proves the statement in Example 12.12, and therefore $F[X]$ is a Euclidean domain. (Hint: Assume that $n := \deg(f(X)) \geqslant \deg(g(X)) =: m$. Now use induction on $n - m$. First write $f(X) = aX^{n-m}g(X) + r_1(X)$ with an appropriate $a \in F$ and $r_1(X) \in F(X)$ of degree smaller than n. Then use the induction hypothesis for $r_1(X)$ in place of $f(X)$.)

2. Let F be a field and let $f(X) \in F[X]$ be a polynomial in the indeterminate X with coefficients in F.

(a) Show that if $a \in F$ is a root of $f(X)$ then $f(X) = (X - a)q(X)$ for some $q(X) \in F[X]$.

(b) Assume that $f(X) \neq 0$. Show that $f(X)$ has at most $\deg(f)$ roots in F. (Hint: Use induction on $\deg(f(X))$.)

(c) Let F be a field and let $H \leqslant F^\times$ be a finite (multiplicative) subgroup. Show that H is cyclic. (Hint: Use part (b) and Exercise 10.5(d).)

(d) Show that $(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic.

3. Let p be an odd prime. Furthermore let $r \in \mathbb{Z}$ be such that $r+p\mathbb{Z}$ generates $(\mathbb{Z}/p\mathbb{Z})^\times$ as group.

(a) Show that there exists $t \in \mathbb{Z}$ such that $(r + tp)^{p-1} \not\equiv 1 \mod p^2$.

(b) Let $t \in \mathbb{Z}$ be as in (a). Show that $(r+pt)+p^n\mathbb{Z}$ is a generator of $(\mathbb{Z}/p^n\mathbb{Z})^\times$ for every $n \in \mathbb{N}$. (Hint: Use induction on n. In order to show that a group element g has order $p^{n-1}(p-1)$ it suffices to show that $p-1$ divides $o(g)$ and that $g^{p^{n-2}(p-1)} \neq 1$.)

4. (a) Let F be a field and let $a \in F$. Show that $F[X]/(X-a) \cong F$ as rings. (Hint: Use the evaluation homomorphism with respect to a and Exercise 2(a).)

(b) Show that $\mathbb{R}[X]/(X^2 - 1) \cong \mathbb{R} \times \mathbb{R}$ as rings. (Hint: Use the Chinese Remainder Theorem.)

(c) Show that $\mathbb{R}[X]/(X^2 + 1) \cong \mathbb{C}$ as rings. (Hint: Use the evaluation homomorphism with respect to a suitable complex number.)

5. Let $F := \mathbb{Z}/3\mathbb{Z}$. Compute a greatest common divisor $d(X)$ of $f(X) = X^4 - X^3 + X - 1$ and $g(X) = X^3 + X^2 + X + 1$ in $F[X]$ and find polynomials $p(X), q(X) \in F[X]$ with $d(X) = p(X)f(X) + q(X)g(X)$.

6. Let $R := \mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$. Compute a greatest common divisor of $\alpha = 10$ and $\beta = 1 - 5i$ using the Euclidean Algorithm.

7. Let $R := \mathbb{Z}[i]$. Show the following (thus giving an overview over all prime elements in R and giving the prime factorization in R of every prime number in $\mathbb{Z}$). (Hint: make use of the norm map).

(a) Every prime element π of R divides precisely one prime number of $\mathbb{Z}$.

(b) If $\pi \in R$ is such that $N(\pi)$ is a prime number in $\mathbb{Z}$, then π is a prime element in R.

(c) $2 = (1 - i)(1 + i)$ is a prime factorization of 2 in R and $(1 - i) \sim (1 + i)$.

(d) If p is a prime number in $\mathbb{Z}$ with $p \equiv 3 \mod 4$, then p is also a prime element in R.

(e) If p is a prime number in $\mathbb{Z}$ with $p \equiv 1 \mod 4$, then there exists $z \in \mathbb{Z}$ with $z^2 \equiv -1 \mod p$. (Hint: use that $(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic.)

(f) If p is a prime number in $\mathbb{Z}$ with $p \equiv 1 \mod 4$, then $p = \pi \cdot \overline{\pi}$ for a prime element π of R such that $\overline{\pi}$ is also a prime element which is not associate to π.

8. Let $n \in \mathbb{N}$ and assume $n = p_1^{e_1} \cdots p_r^{e_r}$ is its prime factorization. Then the following are equivalent:

(i) n can be written as a sum of two squares, i.e., $n = x^2 + y^2$ for some $x, y \in \mathbb{N}_0$.

(ii) For every $i \in \{1, \ldots, r\}$ such that $p_i \equiv 3 \mod 4$, the exponent e_i is even.

(Hint: Use Exercise 7.)

9. Show that the ring $R := \mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$ is a Euclidean domain. (Hint: Show that $N\colon R \to \mathbb{N}_0$, $a + b\sqrt{2} \mapsto |a^2 - 2b^2|$, is a Euclidean norm for R.)

13 Localization

Throughout this section let R denote a commutative ring.

13.1 Theorem *Let $S \subseteq R$ be a multiplicatively closed subset of R containing* 1.

(a) *The relation on $R \times S$ defined by*

$$(r_1, s_1) \sim (r_2, s_2) :\iff \exists t \in S : r_1 s_2 t = r_2 s_1 t$$

is an equivalence relation. The equivalence class of (r, s) will be denoted by $\frac{r}{s}$ and the set of equivalence classes by $S^{-1}R$. One has $\frac{rt}{st} = \frac{r}{s}$ for all $r \in R$ and all $s, t \in S$.

(b) *$S^{-1}R$ is a commutative ring under*

$$\frac{r_1}{s_1} + \frac{r_2}{s_2} := \frac{r_1 s_2 + r_2 s_1}{s_1 s_2}$$

and

$$\frac{r_1}{s_1} \cdot \frac{r_2}{s_2} := \frac{r_1 r_2}{s_1 s_2}$$

with 0*-element $\frac{0}{1}$ and* 1*-element $\frac{1}{1}$.*

(c) *The function $\iota\colon R \to S^{-1}R$, $r \mapsto \frac{r}{1}$, is a ring homomorphism with the property $\iota(S) \subseteq (S^{-1}R)^\times$.*

Proof (a) Reflexivity and symmetry clearly hold. To show transitivity, let $(r_1, s_1) \sim (r_2, s_2)$ and $(r_2, s_2) \sim (r_3, s_3)$. Then there exist $t_1, t_2 \in S$ with $r_1 s_2 t_1 = r_2 s_1 t_1$ and $r_2 s_3 t_2 = r_3 s_2 t_2$. Multiplying the first equation by $s_3 t_2$ and the second equation by $s_1 t_1$ yields $r_1 s_2 t_1 s_3 t_2 = r_2 s_1 t_1 s_3 t_2 = r_3 s_2 t_2 s_1 t_1$. This implies $(r_1, s_1) \sim (r_3, s_3)$, since $s_2 t_1 t_2 \in S$. Moreover, $\frac{rt}{st} = \frac{r}{s}$, since $rts1 = rst1$ with $1 \in S$.

(b) This is shown in the following steps, each of which is a straightforward verification:

(i) Addition is well-defined.
(ii) Multiplication is well-defined.
(iii) Addition is associative.
(iv) $\frac{0}{1}$ is an additive identity element.
(v) $\frac{-r}{s}$ is an additive inverse of $\frac{r}{s}$.
(vi) Addition is commutative.

(vii) Multiplication is associative.
(viii) $\frac{1}{1}$ is a multiplicative identity element.
(ix) Multiplication is commutative.
(x) Distributivity holds.

(c) First note that $\iota(1) = \frac{1}{1}$ which is the 1-element of $S^{-1}R$. Moreover, we have for $r, r' \in R$ and $s \in S$:

$$\begin{aligned} \iota(r + r') &= \frac{r + r'}{1} = \frac{r}{1} + \frac{r'}{1} = \iota(r) + \iota(r')\,, \\ \iota(rr') &= \frac{rr'}{1} = \frac{r}{1} \cdot \frac{r'}{1} = \iota(r)\iota(r')\,, \\ \iota(s) \cdot \frac{1}{s} &= \frac{s}{1} \cdot \frac{1}{s} = \frac{s}{s} = \frac{1}{1}\,. \end{aligned}$$

This completes the proof. □

13.2 Remark (a) $S^{-1}R$ is called the *localization of* R with respect to S.

(b) If $0 \in S$ then $S^{-1}R = \{0\}$ (see Exercise 2).

(c) It is not difficult to show that ι is injective if and only if S does not contain any zero-divisors of R (see Exercise 2). This is for example true when R is an integral domain and $0 \notin S$. In this case we can view R as a subring in $S^{-1}R$ by viewing the element r as $\frac{r}{1}$. Also, the notation $\frac{r}{s}$ is justified by noting that $\frac{r}{s} = \frac{r}{1} \cdot \frac{1}{s} = \frac{r}{1} \cdot (\frac{s}{1})^{-1} = \iota(r)\iota(s)^{-1} = r \cdot s^{-1}$ under this identification.

13.3 Examples (a) If R is an integral domain and $S = R \smallsetminus \{0\}$ then $S^{-1}R = \{\frac{r}{s} \mid r, s \in R, s \neq 0\}$ is a field. In fact, if $\frac{r}{s} \neq \frac{0}{1}$ then $r \neq 0$ and therefore $r \in S$. It follows that $\frac{r}{s} \cdot \frac{s}{r} = \frac{1}{1}$ so that $\frac{r}{s}$ is invertible with inverse $\frac{s}{r}$. In this case $S^{-1}R$ is called the *field of fractions* or *quotient field* of R. It is denoted by $\mathrm{Quot}(R)$. Note that $\mathrm{Quot}(R)$ contains R as a subring if one identifies the elements of R with elements in $\mathrm{Quot}(R)$ via $\iota\colon R \to \mathrm{Quot}(R)$.

(b) For any given element $f \in R$, the set $S := \{1, f, f^2, f^3, \ldots\}$ is multiplicatively closed. In this case the ring $S^{-1}R$ is also denoted by R_f.

(c) For any prime ideal P of R one can choose S to be $R \smallsetminus P$, the complement of P in R. In this case the ring $S^{-1}R$ is also denoted by R_P and called the *localization of* R *at the prime ideal* P. The ring R_P is a *local ring*, i.e., a ring T with the property that $T \smallsetminus T^\times$ is an ideal (the non-units form an ideal). A local ring has a unique maximal ideal, namely the set of non-units (see Exercise 3). In our example the unique maximal ideal of R_P is the set $P_P := \{\frac{r}{s} \mid r \in P, s \in R \smallsetminus P\}$ (see Exercise 3).

13.4 Theorem (Universal property of $\iota\colon R \to S^{-1}R$) *Let $1 \in S \subseteq R$ be multiplicatively closed, let T be a ring and let $f\colon R \to T$ be a ring homomorphism with $f(S) \subseteq T^\times$. Then there exists a unique ring homomorphism $\tilde{f}\colon S^{-1}R \to T$ such that $f = \tilde{f} \circ \iota$:*

$$\begin{tikzcd}
R \arrow[rr, "f"] \arrow[dr, "\iota"'] & & T \\
& S^{-1}R \arrow[ur, dotted, "\tilde{f}"'] &
\end{tikzcd}$$

Moreover, $\tilde{f}(\frac{r}{s}) = f(r)f(s)^{-1}$ for all $r \in R$ and $s \in S$.

Proof Uniqueness: If $\tilde{f}\colon S^{-1}R \to T$ is a ring homomorphism with $\tilde{f}(\iota(r)) = f(r)$ then $f(\frac{r}{1}) = f(r)$ for all $r \in R$ and $\tilde{f}(\frac{1}{s}) = \tilde{f}((\frac{s}{1})^{-1}) = \tilde{f}(\frac{s}{1})^{-1} = f(s)^{-1}$ for all $s \in S$. Hence, $\tilde{f}(\frac{r}{s}) = \tilde{f}(\frac{r}{1} \cdot \frac{1}{s}) = \tilde{f}(\frac{r}{1})\tilde{f}(\frac{1}{s}) = f(r)f(s)^{-1}$ for all $r \in R$ and all $s \in S$. This shows the uniqueness of $\tilde{f}$ and the last statement of the theorem.

Existence: We define $\tilde{f}(\frac{r}{s}) := f(r)f(s)^{-1}$ for $r \in R$ and $s \in S$. First we show that $\tilde{f}$ is well-defined. Assume that $\frac{r}{s} = \frac{r'}{s'}$ with $r' \in R$ and $s' \in S$. Then there exists $t \in S$ with $rs't = r'st$ and we obtain $f(r)f(s')f(t) = f(r')f(s)f(t)$. Since $f(t)$ is invertible in T, this implies $f(r)f'(s) = f(r')f(s')$. Multiplying both sides by $f(s)^{-1}f(s')^{-1}$ and noting that $\mathrm{im}(f)$ is commutative, we obtain $f(r)f(s)^{-1} = f(r')f(s')^{-1}$. Next we show that $\tilde{f}$ is additive and multiplicative. Let $r, r' \in R$ and let $s, s' \in S$. Then, noting again that $\mathrm{im}(f)$ is commutative, we have

$$\begin{aligned}
\tilde{f}(\frac{r}{s} + \frac{r'}{s'}) &= \tilde{f}(\frac{rs' + r's}{ss'}) = f(rs' + r's)f(ss')^{-1} \\
&= (f(r)f(s') + f(r')f(s))f(s)^{-1}f(s')^{-1} \\
&= f(r)f(s)^{-1} + f(r')f(s')^{-1} = \tilde{f}(\frac{r}{s}) + \tilde{f}(\frac{r'}{s'})
\end{aligned}$$

and

$$\begin{aligned}\tilde{f}(\frac{r}{s}\cdot\frac{r'}{s'}) = \tilde{f}(\frac{rr'}{ss'}) &= f(rr')f(ss')^{-1} \\ &= f(r)f(r')f(s)^{-1}f(s')^{-1} = \tilde{f}(\frac{r}{s})\tilde{f}(\frac{r'}{s'})\,.\end{aligned}$$

Finally, $\tilde{f}(\frac{1}{1}) = f(1)f(1)^{-1} = 1_T$. This completes the proof. □

13.5 Remark Assume that R is an integral domain and that $f\colon R \to F$ is an injective ring homomorphism from R to a field F. By the universal property of $\iota\colon R \to S^{-1}R$, there exists a unique ring homomorphism $\tilde{f}\colon S^{-1}R \to F$ such that $\tilde{f}\circ\iota = f$:

$$\begin{tikzcd}
R \arrow[rr, "f"] \arrow[dr, "\iota"'] & & F \\
& S^{-1}R \arrow[ur, "\tilde{f}"'] &
\end{tikzcd}$$

Since f is injective, also $\tilde{f}$ is injective. In fact, if $\tilde{f}(\frac{r}{s}) = \tilde{f}(\frac{r'}{s'})$ then $f(r)f(s)^{-1} = f(r')f(s')^{-1}$ which implies $f(rs') = f(r's)$. Since f is injective we obtain $rs' = r's$ and $\frac{r}{s} = \frac{r'}{s'}$. Next, note that the image of $\tilde{f}$ is the set of elements of the form $f(r)f(s)^{-1}$ with $r \in R$ and $s \in S$. These elements form a subring E of F which is isomorphic to $S^{-1}R$ under $\tilde{f}$. Note that $f(R) \subseteq E$ and that we obtain a commutative diagram

$$\begin{tikzcd}
R \arrow[rr, "f"] \arrow[dr, "\iota"'] & & E \\
& S^{-1}R \arrow[ur, "\tilde{f}"'] &
\end{tikzcd}$$

where $\tilde{f}$ is now an isomorphism. Thus, we may always use the embedding $f\colon R \to E$ instead of $\iota\colon R \to S^{-1}R$ as the localization of R with respect to S. This applies in particular, if R is already contained in a field F and $f\colon R \to F$ is the inclusion. In this case, $E = \{rs^{-1} \mid r, s \in R, s \neq 0\} \subseteq F$.

13.6 Examples (a) Let p be a prime number. Since $\mathbb{Z}$ is a subset of $\mathbb{Q}$ we can write $\mathbb{Z}_{(p)}$ as the set of all fractions $\frac{r}{s}$ with $r, s \in \mathbb{Z}$ such that s is not divisible by p.

(b) Let $R := \mathbb{Z}[i]$ be the ring of Gaussian integers viewed as a subfield of the complex numbers. Then the field of Gaussian numbers, $\mathbb{Q}(i) = \{a + bi \mid a, b \in \mathbb{Q}\}$ can be viewed as the field of fractions of $\mathbb{Z}[i]$. In fact, every element of $\mathbb{Q}(i)$ can be written as a quotient of an element of R and a non-zero integer. Conversely, every quotient rs^{-1} with $r, s \in R$ and $s \neq 0$ lies in $\mathbb{Q}(i)$, since for $s = a + bi$ we have $s^{-1} = \frac{a}{a^2+b^2} - \frac{b}{a^2+b^2}i$.

Exercises

1. Prove the statement in Theorem 13.1(b).

2. Let R be a commutative ring and let S be a multiplicatively closed subset of R containing 1. Show the following statements:

(a) $S^{-1}R = \{0\}$ if and only if $0 \in S$.

(b) The map $\iota\colon R \to S^{-1}R$, $r \mapsto \frac{r}{1}$, is injective if and only if S does not contain a zero-divisor from R.

3. (a) A ring T is called *local* if the set $M := T \smallsetminus T^\times$ of non-units is an ideal of T. Show that in this case M is the unique maximal ideal of T and that T/M is a division ring.

(b) Let R be a commutative ring and let P be a prime ideal of R. Show that the localization R_P is a local ring with maximal ideal $P_P := \{\frac{r}{s} \mid r \in P, s \in R \smallsetminus P\}$.

4. Let p be a prime number and let $R := \mathbb{Z}_{(p)} = \{\frac{r}{s} \mid r \in \mathbb{Z}, s \in \mathbb{Z} \smallsetminus (p)\}$ be the localization of $\mathbb{Z}$ at the prime ideal (p).

(a) Show that $R^\times = \{\frac{a}{b} \mid a, b \in \mathbb{Z} \smallsetminus (p)\}$.

(b) Show that, up to associates, p is the only prime element of R.

(c) Show that every non-zero element a of R can be written as $a = up^n$ with unique $u \in R^\times$ and $n \in \mathbb{N}_0$.

(d) Show that every non-zero ideal of R is of the form (p^n) for a unique $n \in \mathbb{N}_0$.

5. This exercise gives a geometric explanation of the origin of the notion of a *local ring*. Let $x \in \mathbb{R}^n$ and consider all pairs (U, f), where U is an open neighborhood of x and $f\colon U \to \mathbb{R}$ is a continuous function. For two such pairs (U, f) and (V, g) we write $(U, f) \sim (V, g)$ if there exists an open subset W of $U \cap V$ containing x such that $f|_W = g|_W$ (their restrictions to W coincide).

(a) Show that $\sim$ is an equivalence relation. Denote the equivalence class of (U, f) by $[U, f]$ and let C_x denote the set of these equivalence classes. The elements of C_x are called *germs at* x and C_x is called the *stalk at* x.

(b) Show that C_x is a ring with respect to

$$[U, f] + [V, g] := [U \cap V, f|_U + g|_V] \quad \text{and} \quad [U, f] \cdot [V, g] := [U \cap V, f|_U \cdot g|_V] \,.$$

(You don't have to verify the ring axioms, but show that addition and multiplication are well-defined.)

(c) Show that C_x is a local ring and that $M_x := \{[U, f] \in C_x \mid f(x) = 0\}$ is its unique maximal ideal.

(d) Show that C_x/M_x is isomorphic to $\mathbb{R}$.

6. Let R be an integral domain and let S be a multiplicatively closed subset of R with $1 \in S$. View R as a subring of $R' := S^{-1}R$ via the canonical map $\iota\colon R \to R'$, $r \mapsto \frac{r}{1}$.

(a) Let $\mathcal{I}$ denote the set of ideals of R and denote by $\mathcal{I}'$ the set of ideals of R'. Consider the maps $\alpha\colon \mathcal{I}' \to \mathcal{I}$, $I' \mapsto I' \cap R$, and $\beta\colon \mathcal{I} \to \mathcal{I}'$, $I \mapsto (I)_{R'}$. Show that $\beta \circ \alpha = \mathrm{id}_{\mathcal{I}'}$. (Note that this implies that α is injective.)

(b) Let $\mathcal{P}'$ denote the set of prime ideals of R'. Show that α defines a bijection between $\mathcal{P}'$ and the set of prime ideals of R whose intersection with S is empty.

14 Polynomial Rings

Throughout this section, R denotes a UFD and K denotes its field of fractions. We view R as a subring of K via the canonical embedding $\iota\colon R \to K$, $r \mapsto \frac{r}{1}$.

14.1 Proposition *Let k be a commutative ring, let $\mathcal{X} = \{X_1, \ldots, X_n\}$ be a family of indeterminates, and let $i\colon \mathcal{X} \to k[\mathcal{X}] = k[X_1, \ldots, X_n]$ be the function defined by $i(X_1) = X_1$, …, $i(X_n) = X_n$. This function has the following universal property: For every k-algebra (A, η) and every function $f\colon \mathcal{X} \to A$, there exists a unique k-algebra homomorphism $\tilde{f}\colon k[\mathcal{X}] \to A$ such that $\tilde{f} \circ i = f$:*

$$\begin{tikzcd}
\mathcal{X} \arrow[r, "f"] \arrow[d, "i"'] & A \\
k[\mathcal{X}] \arrow[ur, dotted, "\tilde{f}"'] &
\end{tikzcd}$$

Moreover, one has

$$\tilde{f}\Big(\sum_{(i_1,\ldots,i_n)\in\mathbb{N}_0^n} \alpha_{i_1,\ldots,i_n} X_1^{i_1}\cdots X_n^{i_n}\Big) = \sum_{(i_1,\ldots,i_n)\in\mathbb{N}_0^n} \eta(\alpha_{i_1,\ldots,i_n}) f(X_1)^{i_1}\cdots f(X_n)^{i_n}\,. \tag{14.1.a}$$

Here $\alpha_{i_1,\ldots,i_n} \in k$ is equal to 0 for all but finitely many $(i_1, \ldots, i_n) \in \mathbb{N}_0^n$.

Proof The uniqueness statement is clear, since every element of $k[X]$ is a sum of products of elements from k and from $\mathcal{X}$.

We define the homomorphism $\tilde{f}$ as in (14.1.a). It is a straightforward computation that $\tilde{f}$ is a ring homomorphism. Clearly, $\tilde{f}$ satisfies $\tilde{f}(i(X_j)) = f(X_j)$ for $j = 1, \ldots, n$. □

14.2 Definition A polynomial $f(X) \in R[X]$ is called *primitive*, if the coefficients of $f(X)$ are coprime. For example, $6X^2 + 15X - 10$ is primitive in $\mathbb{Z}[X]$.

14.3 Lemma (Gauss' Lemma, 1777–1855) *Let $f, g \in R[X]$. Then, f and g are primitive if and only if fg is primitive.*

Proof "$\Rightarrow$": Assume that fg is not primitive and let $p \in R$ be a prime element dividing all the coefficients of fg. Let $\nu \colon R \to R/(p)$ denote the canonical epimorphism. Note that $(R/(p)[X], \nu)$ is an R-algebra. Then, by Proposition 14.1 applied to the function $\phi \colon \{X\} \to R/(p)[X]$, $X \mapsto X$, the map $\tilde{\varphi} \colon R[X] \to R/(p)[X]$, $\sum_i a_i X^i \mapsto \sum_i \nu(a_i) X^i$, is an R-algebra homomorphism with $\tilde{\varphi}(fg) = 0$. This implies $\tilde{\varphi}(f)\tilde{\varphi}(g) = 0$. Since $R/(p)$ is an integral domain, also $R/(p)[X]$ is. Therefore, $\tilde{\varphi}(f) = 0$ or $\tilde{\varphi}(g) = 0$. But if $\tilde{\varphi}(f) = 0$, then every coefficient of f is divisible by p and f is not primitive (and similarly for g). This is a contradiction.

"$\Leftarrow$": Assume that f is not primitive and let $p \in R$ be a prime element dividing all the coefficients of f. Then p divides all the coefficients of fg. This is a contradiction. In the same way one treats the case that g is not primitive. □

14.4 Theorem (Eisenstein's Irreducibility Criterion, 1823–1852) *Assume that* $f(X) = a_n X^n + \cdots + a_1 X + a_0 \in R[X]$ *is primitive with* $\deg(f) \geqslant 1$ *and assume that* $p \in R$ *is a prime element such that*

$$p \mid a_0,\ p \mid a_1,\ \ldots,\ p \mid a_{n-1},\ p \nmid a_n \text{ and } p^2 \nmid a_0\,.$$

Then f *is irreducible in* $R[X]$.

Proof Obviously, $f \neq 0$ and f is not a unit in $R[X]$. Assume that $f = gh$ with $g = b_k X^k + \cdots + b_1 X + b_0 \in R[X]$ and $h = c_l X^l + \cdots c_1 X + c_0 \in R[X]$ and $b_k \neq 0 \neq c_l$. Since $p \mid a_0 = b_0 c_0$, and $p^2 \nmid a_0$, we have $p \mid b_0$ or $p \mid c_0$, but not both. Without loss of generality assume that $p \mid b_0$ and $p \nmid c_0$. Since $p \nmid a_n = b_k c_l$, we have $p \nmid b_k$. Therefore, there exists $j \in \{1, \ldots, k\}$ such that $p \mid b_0, \ldots, p \mid b_{j-1}$, and $p \nmid b_j$. Since $a_j = b_j c_0 + b_{j-1} c_1 + \cdots b_0 c_j$ (with $c_i := 0$ if $i > l$), we obtain $p \nmid a_j$. This implies $j = n$. But $j \leqslant k$ and $k + l = n$ then implies that $k = n$ and $l = 0$. Thus, $h \in R$. Since f is primitive, also h is (by Gauss' Lemma 14.3). This implies that h is a unit in R and also in $R[X]$. Thus, f is irreducible in $R[X]$. □

14.5 Remark Let p be a prime number and let $i \in \{1, \ldots, p-1\}$. Then, the binomial coefficient $\binom{p}{i}$ is divisible by p, because it is equal to $\frac{p!}{i!(p-i)!}$ and it is a natural number.

The following theorem illustrates how Eisenstein's Irreducibility Criterion can be applied.

14.6 Theorem *Let $p \in \mathbb{N}$ be a prime number. Then the polynomial*

$$\Phi_p(X) := 1 + X + \cdots + X^{p-1}$$

*is irreducible in $\mathbb{Z}[X]$. ($\Phi_p(X)$ is called the p-*th cyclotomic polynomial.*)*

Proof By Proposition 14.1, applied to the functions $\{X\} \to \mathbb{Z}[X]$ which map X to $X+1$ and to $X-1$, we obtain ring homomorphisms $\varepsilon\colon \mathbb{Z}[X] \to \mathbb{Z}[X]$, $f(X) \mapsto f(X+1)$, and $\delta\colon \mathbb{Z}[X] \to \mathbb{Z}[X]$, $f(X) \mapsto f(X-1)$. It is easy to see that they are inverses of each other and therefore ring isomorphisms. In order to see that Φ_p is irreducible in $\mathbb{Z}[X]$ it suffices to show that $\varepsilon(\Phi_p)$ is irreducible in $\mathbb{Z}[X]$. Note that $\Phi_p \cdot (X-1) = X^p - 1$. Applying ε to this equation yields

$$\begin{aligned} \varepsilon(\Phi_p) \cdot X &= (X+1)^p - 1 = X^p + \binom{p}{p-1} X^{p-1} + \cdots + \binom{p}{1} X + 1 - 1 \\ &= \left[X^{p-1} + \binom{p}{p-1} X^{p-2} + \cdots \binom{p}{2} X + \binom{p}{1} \right] \cdot X\,, \end{aligned}$$

and we obtain

$$\varepsilon(\Phi_p) = X^{p-1} + \binom{p}{p-1} X^{p-2} + \cdots + \binom{p}{2} X + p\,.$$

This polynomial is primitive in $\mathbb{Z}[X]$, and, by Eisenstein's irreducibility criterion for the prime p, it is irreducible in $\mathbb{Z}[X]$. □

Assume that $f(X) \in R[X]$. Next we want to understand how irreducibility of $f(X)$ in $R[X]$ is related to its irreducibility in $K[X]$. Theorem 14.8 will give a complete answer and will imply that the cyclotomic polynomial $\Phi_p(X)$ is also irreducible in $\mathbb{Q}[X]$. But first we need the following proposition.

14.7 Proposition *For every $f \in K[X] \smallsetminus \{0\}$ there exists an element $a \in K \smallsetminus \{0\}$ and a primitive polynomial $g \in R[X]$ such that $f = ag$. If also $f = bh$ with $b \in K$ and a primitive polynomial $h \in R[X]$, then there exists $u \in U(R)$ with $h = ug$ and $b = au^{-1}$.*

Proof *Existence:* Write $f = \frac{r_0}{s_0} + \frac{r_1}{s_1}X + \cdots + \frac{r_n}{s_n}X^n$ with $r_i \in R$, $0 \neq s_i \in R$, and set $s := s_0 s_1 \cdots s_n$. Then $s \neq 0$ and $sf \in R[X]$. Thus we can write $sf = t_0 + t_1 X + \cdots + t_n X^n$ with $t_i \in R$. Let $d \in \gcd(t_0, \ldots, t_n)$. Then $d \neq 0$,

$\frac{t_0}{d}, \ldots, \frac{t_n}{d}$ are coprime in R, and $g := \frac{s}{d} f$ is primitive in $R[X]$. Thus, $f = ag$ with $a = \frac{d}{s}$, as desired.

Uniqueness: Assume that (a, g) and (b, h) are as in the statement of the proposition. We can write $b = \frac{e}{t}$ with $e, t \in R$, $t \neq 0$. Then $tdg = seh$. Since g and h are primitive, this implies $(td) = (se)$. Thus, $td = use$ for some $u \in U(R)$ and we obtain $a = \frac{d}{s} = u\frac{e}{t} = ub$ and $h = b^{-1}f = ua^{-1}f = ug$. □

14.8 Theorem *For $f \in R[X]$ the following are equivalent:*

(i) *f is irreducible in $R[X]$.*

(ii) *Either (f is constant and irreducible in R) or (f is primitive in $R[X]$ and irreducible in $K[X]$).*

Proof (i)⇒(ii): We have $f \neq 0$ and $f \notin U(R[X]) = U(R)$. If $\deg(f) = 0$, then clearly f is irreducible in R, since $U(R[X]) = U(R)$. So assume that $\deg(f) > 0$. Then $f \notin U(K[X]) = K \smallsetminus \{0\}$ and clearly, f is primitive in $R[X]$. We show that f is irreducible in $K[X]$. So let $g, h, \in K[X]$ with $f = gh$. We need to show that g or h is a constant polynomial. By Proposition 14.7, there exist $a, b \in K$ and primitive polynomials $g_1, h_1 \in R[X]$ such that $g = ag_1$ and $h = bh_1$. We have $1 \cdot f = gh = (ab)(g_1h_1)$ with g_1h_1 primitive by Gauss' Lemma 14.3. Now the uniqueness part of Proposition 14.7 implies that $ab = u$ for some unit u of R. This implies $f = (ug_1)h_1$. Since f is irreducible in $R[X]$, we can conclude that ug_1 or h_1 is a unit in $R[X]$ and therefore constant. This implies that g or h is a constant polynomial.

(ii)⇒(i): Assume that f is constant and irreducible in R. Then clearly, f is irreducible in $R[X]$. Next assume that f is irreducible in $K[X]$ and primitive in $R[X]$ and assume that $f = gh$ for some $g, h \in R[X]$. Note that $\deg(f(X)) > 0$, since f is irreducible in $K[X]$. For the same reason, g or h is a unit in $K[X]$ and therefore constant. Thus, $g \in R$ or $h \in R$, say $g \in R$. Then g divides all the coefficients of f. Since f is primitive, $g \in U(R) = U(R[X])$. □

14.9 Corollary *Let $f \in K[X]$ with $\deg(f) \geqslant 1$ and write $f = a \cdot g$ with $0 \neq a \in K$ and primitive $g \in R[X]$ according to Proposition 14.7. Then, f is irreducible in $K[x]$ if and only if g is irreducible in $R[X]$. In particular, $\Phi_p(X)$ is irreducible in $\mathbb{Q}[X]$.*

Proof By Theorem 14.8, since g is primitive and $\deg(g(X)) > 0$, we have:

$$\begin{aligned} & g \text{ is irreducible in } R[X] \\ \Longleftrightarrow\ & g \text{ is irreducible in } K[X] \\ \Longleftrightarrow\ & f \text{ is irreducible in } K[X] \end{aligned}$$

□

14.10 Theorem *If R is a UFD, then $R[X]$ is a UFD.*

Proof By Proposition 13.2 and Theorem 14.8 it suffices to show that

(i) every $f \in R[X]$, which is non-zero and not a unit, is a product of irreducible elements, and

(ii) whenever $r_1 \cdots r_m p_1 \cdots p_n = s_1 \cdots s_k q_1 \cdots q_l$ with irreducible elements $r_1, \dots, r_m, s_1, \dots, s_k$ of R and primitive elements $p_1, \dots, p_n, q_1, \dots, q_l$ of $R[X]$ which are irreducible in $K[X]$, then $m = k$, $n = l$, r_i is associate to s_i in R, and p_j is associate to q_j in $R[X]$ (after reordering if necessary).

Proof of (i): If $f \in R$, then the assertion is clear. Assume $\deg(f) > 0$. Let d be a greatest common divisor of the coefficients of f and write $f = dg$ with $g \in R[X]$ primitive. We may write $f = f_1 \cdots f_r$ with $f_1, \dots, f_r$ irreducible in $K[X]$, since $K[X]$ is a Euclidean domain. For $i = 1, \dots, r$, write $f_i = a_i g_i$ with $0 \neq a_i \in K$ and $g_i \in R[X]$ primitive, according to Proposition 14.7. Then $f = a_1 \cdots a_r g_1 \cdots g_r$ with $g_1 \cdots g_r$ primitive in $R[X]$, by Gauss' Lemma 14.3. By Proposition 14.7, there exists a unit u of R such that $g = (ug_1)g_2 \cdots g_r$ and $ud = a_1 \cdots a_r$. With $f_1, \dots, f_r$ also $ug_1, g_2, \dots, g_r$ are irreducible in $K[X]$, and then by Theorem 14.8 also in $R[X]$. Now write d as a product of irreducible elements of R (if d is not a unit of R). If d is a unit in R, then $f = (dug_1)g_2 \cdots g_r$. In both cases we are done.

Proof of (ii): By Proposition 14.7 and Gauss' Lemma 14.3, there exists a unit u of R with $r_1 \cdots r_m = s_1 \cdots s_k u^{-1}$ and $p_1 \cdots p_n = q_1 \cdots q_l u$. Since R is a UFD, it follows that $m = k$ and r_i is associate to s_i in R for all $i = 1, \dots m$ (after reordering if necessary). Since $K[X]$ is a UFD, $n = l$ and p_j is associate to q_j in $K[X]$ for $j = 1, \dots, n$ (after reordering if necessary). Thus, $p_j = x_j q_j$ with some non-zero $x_i \in K$, for all $j = 1, \dots, n$. Since p_j and q_j are primitive in $R[X]$, Proposition 14.7 implies that x_j is a unit in R. Therefore, p_j is associate to q_j in $R[X]$ for each $j = 1, \dots, n$. □

14.11 Remark The statements "R is a PID $\Rightarrow$ $R[X]$ is a PID" and "R is a Euclidean domain $\Rightarrow$ $R[X]$ is a Euclidean domain" are false in general. A counterexample to both is the ring $R = \mathbb{Z}$, since $\mathbb{Z}$ is a Euclidean domain, but $\mathbb{Z}[X]$ is not a PID. In fact, the ideal $(2, X)$ is not a principal ideal of $Z[X]$ (see Exercise 1).

Exercises

1. Show that the ideal $(2, X)$ of $\mathbb{Z}[X]$ is not principal.

2. Let $F := \mathbb{Z}/2\mathbb{Z}$.

(a) Show that $X^2 + X + 1$ is the only irreducible polynomial of degree 2 in $F[X]$.

(b) Show that $X^4 + X^3 + 1$ is irreducible in $F[X]$.

(c) Show that $X^4 + X^3 + 1$ is irreducible in $\mathbb{Q}[X]$.

3. Let F be a field, let $f(X) \in F[X]$ be a polynomial of degree $n \geqslant 1$, and let $I = (f(X))$ denote the ideal of $F[X]$ generated by $f(X)$.

(a) Show that the natural epimorphism $\nu\colon F[X] \to F[X]/I$, $a(X) \mapsto a(X) + I$, defines a bijection between the subset $\{r(X) \mid \deg(r) < n\}$ of $F[X]$ and $F[X]/I$. (This function is also an isomorphism of F-vector spaces.)

(b) Assume that F is a finite field with q elements and that $f(X)$ is irreducible. Then $E := F[X]/I$ is a field. How many elements does E have?

(c) Assume $F = \mathbb{Z}/2\mathbb{Z}$ and $f(X) = X^4 + X^3 + 1$ (see Exercise 2). Find a generator of the unit group of E.

4. Show that the polynomial $X^4 + 7X^3 + 15X^2 + 10X + 7$ is irreducible in $\mathbb{Q}[X]$.

5. Let $F := \mathbb{Z}/2\mathbb{Z}$. Decompose the polynomial $X^5 - 1$ into irreducible factors in $F[X]$.