Chapter 3
Algebraic Structures

An algebraic structure is a set with operations between its elements that follow certain rules. As an example of such a structure consider the integers and the operation '+.' What are the properties of this addition? Already in elementary school one learns that the sum $a + b$ of two integers a and b is another integer. Moreover, there is a number 0 such that $0 + a = a$ for every integer a, and for every integer a there exists an integer $-a$ such that $(-a) + a = 0$. The analysis of the properties of such concrete examples leads to definitions of abstract concepts that are built on a few simple axioms. For the integers and the operation addition, this leads to the algebraic structure of a group.

This principle of abstraction from concrete examples is one of the strengths and basic working principles of Mathematics. By "extracting and completely exposing the mathematical kernel" (David Hilbert) we also simplify our further work: Every proved assertion about an abstract concept automatically holds for all concrete examples. Moreover, by combining defined concepts we can move to further generalizations and in this way extend the mathematical theory step by step. Hermann Günther Graßmann (1809–1877) described this procedure as follows[1]: "... the mathematical method moves forward from the simplest concepts to combinations of them and gains via such combinations new and more general concepts."

3.1 Groups

We begin with a set and an operation with specific properties.

Definition 3.1 A *group* is a set G with a map, called *operation*,

$$\oplus : G \times G \to G, \quad (a, b) \mapsto a \oplus b,$$

[1] "... die mathematische Methode hingegen schreitet von den einfachsten Begriffen zu den zusammengesetzteren fort, and gewinnt so durch Verknüpfung des Besonderen neue and allgemeinere Begriffe."

J. Liesen and V. Mehrmann, *Linear Algebra*, Springer Undergraduate Mathematics Series, DOI 10.1007/978-3-319-24346-7_3

that satisfies the following:

(1) The operation $\oplus$ is associative, i.e., $(a \oplus b) \oplus c = a \oplus (b \oplus c)$ holds for all $a, b, c \in G$.
(2) There exists an element $e \in G$, called a *neutral element*, for which
   (a) $e \oplus a = a$ for all $a \in G$, and
   (b) for every $a \in G$ there exists an $\widetilde{a} \in G$, called an *inverse element* of a, with $\widetilde{a} \oplus a = e$.

If $a \oplus b = b \oplus a$ holds for all $a, b \in G$, then the group is called *commutative* or *Abelian*.[2]

As short hand notation for a group we use $(G, \oplus)$ or just G, if is clear which operation is used.

Theorem 3.2 *For every group $(G, \oplus)$ the following assertions hold:*

(1) If $e \in G$ is a neutral element and if $a, \widetilde{a} \in G$ with $\widetilde{a} \oplus a = e$, then also $a \oplus \widetilde{a} = e$.
(2) If $e \in G$ is a neutral element and if $a \in G$, then also $a \oplus e = a$.
(3) G contains exactly one neutral element.
(4) For every $a \in G$ there exists a unique inverse element.

Proof

(1) Let $e \in G$ be a neutral element and let $a, \widetilde{a} \in G$ satisfy $\widetilde{a} \oplus a = e$. Then by Definition 3.1 there exists an element $a_1 \in G$ with $a_1 \oplus \widetilde{a} = e$. Thus,

$$\begin{aligned} a \oplus \widetilde{a} = e \oplus (a \oplus \widetilde{a}) = (a_1 \oplus \widetilde{a}) \oplus (a \oplus \widetilde{a}) a_1 \oplus ((\widetilde{a} \oplus a) \oplus \widetilde{a}) \\ = a_1 \oplus (e \oplus \widetilde{a}) = a_1 \oplus \widetilde{a} = e. \end{aligned}$$

(2) Let $e \in G$ be a neutral element and let $a \in G$. Then there exists $\widetilde{a} \in G$ with $\widetilde{a} \oplus a = e$. By (1) then also $a \oplus \widetilde{a} = e$ and it follows that

$$a \oplus e = a \oplus (\widetilde{a} \oplus a) = (a \oplus \widetilde{a}) \oplus a = e \oplus a = a.$$

(3) Let $e, e_1 \in G$ be two neutral elements. Then $e_1 \oplus e = e$, since e_1 is a neutral element. Since e is also a neutral element, it follows that $e_1 = e \oplus e_1 = e_1 \oplus e$, where for the second identity we have used assertion (2). Hence, $e = e_1$.

(4) Let $\widetilde{a}, a_1 \in G$ be two inverse elements of $a \in G$ and let $e \in G$ be the (unique) neutral element. Then with (1) and (2) it follows that

$$\widetilde{a} = e \oplus \widetilde{a} = (a_1 \oplus a) \oplus \widetilde{a} = a_1 \oplus (a \oplus \widetilde{a}) = a_1 \oplus e = a_1. \qquad \square$$

[2]Named after Niels Henrik Abel (1802–1829), the founder of group theory.

Example 3.3

(1) $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$ and $(\mathbb{R}, +)$ are commutative groups. In all these groups the neutral element is the number 0 (zero) and the inverse of a is the number $-a$. Instead of $a + (-b)$ we usually write $a - b$. Since the operation is the addition, these groups are also called *additive groups*.

The natural numbers $\mathbb{N}$ with the addition do not form a group, since there is no neutral element in $\mathbb{N}$. If we consider the set $\mathbb{N}_0$, which includes also the number 0 (zero), then $0 + a = a + 0 = a$ for all $a \in \mathbb{N}_0$, but only $a = 0$ has an inverse element in $\mathbb{N}$. Hence also $\mathbb{N}_0$ with the addition does not form a group.

(2) The sets $\mathbb{Q} \setminus \{0\}$ and $\mathbb{R} \setminus \{0\}$ with the usual multiplication form commutative groups. In these *multiplicative groups*, the neutral element is the number 1 (one) and the inverse element of a is the number $\frac{1}{a}$ (or a^{-1}). Instead of $a \cdot b^{-1}$ we also write $\frac{a}{b}$ or a/b.
The integers $\mathbb{Z}$ with the multiplication do not form a group. The set $\mathbb{Z}$ includes the number 1, for which $1 \cdot a = a \cdot 1 = a$ for all $a \in \mathbb{Z}$, but no $a \in \mathbb{Z} \setminus \{-1, 1\}$ has an inverse element in $\mathbb{Z}$.

Definition 3.4 Let $(G, \oplus)$ be a group and $H \subseteq G$. If $(H, \oplus)$ is a group, then it is called a *subgroup* of $(G, \oplus)$.

The next theorem gives an alternative characterization of a subgroup.

Theorem 3.5 *$(H, \oplus)$ is a subgroup of the group $(G, \oplus)$ if and only if the following properties hold:*

(1) $\emptyset \neq H \subseteq G$.
(2) $a \oplus b \in H$ for all $a, b \in H$.
(3) For every $a \in H$ also the inverse element satisfies $\widetilde{a} \in H$.

Proof Exercise. □

The following definition characterizes maps between two groups which are compatible with the respective group operations.

Definition 3.6 Let $(G_1, \oplus)$ and $(G_2, \circledast)$ be groups. A map

$$\varphi : G_1 \to G_2, \quad g \mapsto \varphi(g),$$

is called a *group homomorphism*, if

$$\varphi(a \oplus b) \;=\; \varphi(a) \circledast \varphi(b) \quad \text{for all } a, b \in G_1.$$

A bijective group homomorphism is called a *group isomorphism*.

3.2 Rings and Fields

In this section we extend the concept of a group and discuss mathematical structures that are characterized by two operations. As motivating example consider the integers with the addition, i.e., the group $(\mathbb{Z}, +)$. We can multiply the elements of $\mathbb{Z}$ and this multiplication is associative, i.e., $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ for all $a, b, c \in \mathbb{Z}$. Furthermore the addition and multiplication satisfy the distributive laws $a \cdot (b + c) = a \cdot b + a \cdot c$ and $(a + b) \cdot c = a \cdot c + b \cdot c$ for all integers a, b, c. These properties make $\mathbb{Z}$ with addition and multiplication into a ring.

Definition 3.7 A *ring* is a set R with two operations

$$\begin{aligned} + &: R \times R \to R, & (a, b) &\mapsto a + b, & &(\textit{addition}) \\ * &: R \times R \to R, & (a, b) &\mapsto a * b, & &(\textit{multiplication}) \end{aligned}$$

that satisfy the following:

(1) $(R, +)$ is a commutative group.
We call the neutral element in this group *zero*, and write 0. We denote the inverse element of $a \in R$ by $-a$, and write $a - b$ instead of $a + (-b)$.
(2) The multiplication is associative, i.e., $(a * b) * c = a * (b * c)$ for all $a, b, c \in R$.
(3) The distributive laws hold, i.e., for all $a, b, c \in R$ we have

$$\begin{aligned} a * (b + c) &= a * b + a * c, \\ (a + b) * c &= a * c + b * c. \end{aligned}$$

A ring is called *commutative* if $a * b = b * a$ for all $a, b \in R$.
An element $1 \in R$ is called unit if $1 * a = a * 1 = a$ for all $a \in R$. In this case R is called a *ring with unit*.

On the right hand side of the two distributive laws we have omitted the parentheses, since multiplication is supposed to bind stronger than addition, i.e., $a + (b * c) = a + b * c$. If it is useful for illustration purposes we nevertheless use parentheses, e.g., we sometimes write $(a * b) + (c * d)$ instead of $a * b + c * d$.

Analogous to the notation for groups we denote a ring with $(R, +, *)$ or just with R, if the operations are clear from the context.

In a ring with unit, the unit element is unique: If $1, e \in R$ satisfy $1 * a = a * 1 = a$ and $e * a = a * e = a$ for all $a \in R$, then in particular $e = e * 1 = 1$.

For $a_1, a_2, \ldots, a_n \in R$ we use the following abbreviations for the *sum* and *product* of these elements:

$$\sum_{j=1}^{n} a_j := a_1 + a_2 + \ldots + a_n \quad \text{and} \quad \prod_{j=1}^{n} a_j := a_1 * a_2 * \ldots * a_n.$$

Moreover, $a^n := \prod_{j=1}^{n} a$ for all $a \in R$ and $n \in \mathbb{N}$. If $\ell > k$, then we define the *empty sum* as

$$\sum_{j=\ell}^{k} a_j := 0.$$

In a ring with unit we also define for $\ell > k$ the *empty product* as

$$\prod_{j=\ell}^{k} a_j := 1.$$

Theorem 3.8 *For every ring R the following assertions hold:*

(1) $0 * a = a * 0 = 0$ *for all* $a \in R$.
(2) $a * (-b) = -(a * b) = (-a) * b$ *and* $(-a) * (-b) = a * b$ *for all* $a, b \in R$.

Proof

(1) For every $a \in R$ we have $0 * a = (0 + 0) * a = (0 * a) + (0 * a)$. Adding $-(0 * a)$ on the left and right hand sides of this equality we obtain $0 = 0 * a$. In the same way we can show that $a * 0 = 0$ for all $a \in R$.

(2) Since $(a*b)+(a*(-b)) = a*(b+(-b)) = a*0 = 0$, it follows that $a*(-b)$ is the (unique) additive inverse of $a * b$, i.e., $a * (-b) = -(a * b)$. In the same way we can show that $(-a) * b = -(a * b)$. Furthermore, we have

$$\begin{aligned} 0 = 0 * (-b) &= (a + (-a)) * (-b) = a * (-b) + (-a) * (-b) \\ &= -(a * b) + (-a) * (-b), \end{aligned}$$

and thus $(-a) * (-b) = a * b$. □

It is immediately clear that $(\mathbb{Z}, +, *)$ is a commutative ring with unit. This is the standard example, by which the concept of a ring was modeled.

Example 3.9 Let M be a nonempty set and let R be the set of maps $f : M \to \mathbb{R}$. Then $(R, +, *)$ with the operations

$$\begin{aligned} + &: R \times R \to R, \qquad (f, g) \mapsto f + g, \qquad (f + g)(x) := f(x) + g(x), \\ * &: R \times R \to R, \qquad (f, g) \mapsto f * g, \qquad (f * g)(x) := f(x) \cdot g(x), \end{aligned}$$

is a commutative ring with unit. Here $f(x) + g(x)$ and $f(x) \cdot g(x)$ are the sum and product of two real numbers. The zero in this ring is the map $0_R : M \to \mathbb{R}$, $x \mapsto 0$, and the unit is the map $1_R : M \to \mathbb{R}$, $x \mapsto 1$, where 0 and 1 are the real numbers zero and one.

In the definition of a ring only additive inverse elements occur. We will now formally define the concept of a multiplicative inverse.

Definition 3.10 Let $(R, +, *)$ be a ring with unit. An element $b \in R$ is called an *inverse* of $a \in R$ (with respect to $*$), if $a * b = b * a = 1$. An element of R that has an inverse is called *invertible*.

It is clear from the definition that $b \in R$ is an inverse of $a \in R$ if and only if $a \in R$ is an inverse of $b \in R$. In general, however, not every element in a ring must be (or is) invertible. But if an element is invertible, then it has a unique inverse, as shown in the following theorem.

Theorem 3.11 *Let $(R, +, *)$ be a ring with unit.*

(1) If $a \in R$ is invertible, then the inverse is unique and we denote it by a^{-1}.
(2) If $a, b \in R$ are invertible then $a * b \in R$ is invertible and $(a * b)^{-1} = b^{-1} * a^{-1}$.

Proof

(1) If $b, \widetilde{b} \in R$ are inverses of $a \in R$, then $b = b * 1 = b * (a * \widetilde{b}) = (b * a) * \widetilde{b} = 1 * \widetilde{b} = \widetilde{b}$.

(2) Since a and b are invertible, $b^{-1} * a^{-1} \in R$ is well defined and

$$(b^{-1} * a^{-1}) * (a * b) = ((b^{-1} * a^{-1}) * a) * b = (b^{-1} * (a^{-1} * a)) * b = b^{-1} * b = 1.$$

In the same way we can show that $(a * b) * (b^{-1} * a^{-1}) = 1$, and thus $(a * b)^{-1} = b^{-1} * a^{-1}$. □

From an algebraic point of view the difference between the integers on the one hand, and the rational or real numbers on the other, is that in the sets $\mathbb{Q}$ and $\mathbb{R}$ every element (except for the number zero) is invertible. This "additional structure" makes $\mathbb{Q}$ and $\mathbb{R}$ into fields.

Definition 3.12 A commutative ring R with unit is called a *field*, if $0 \neq 1$ and every $a \in R \setminus \{0\}$ is invertible.

By definition, every field is a commutative ring with unit, but the converse does not hold. One can also introduce the concept of a field based on the concept of a group (cp. Exercise 3.15).

Definition 3.13 A *field* is a set K with two operations

$$\begin{aligned} &+ : K \times K \to K, && (a, b) \mapsto a + b, && \text{(addition)} \\ &* : K \times K \to K, && (a, b) \mapsto a * b, && \text{(multiplication)} \end{aligned}$$

that satisfy the following:

(1) $(K, +)$ is a commutative group.
We call the neutral element in this group *zero*, and write 0. We denote the inverse element of $a \in K$ by $-a$, and write $a - b$ instead of $a + (-b)$.
(2) $(K \setminus \{0\}, *)$ is a commutative group.
We call the neutral element in this group *unit*, and write 1. We denote the inverse element of $a \in K \setminus \{0\}$ by a^{-1}.
(3) The distributive laws hold, i.e., for all $a, b, c \in K$ we have

$$a * (b + c) = a * b + a * c,$$
$$(a + b) * c = a * c + b * c.$$

We now show a few useful properties of fields.

Lemma 3.14 *For every field K the following assertions hold:*

(1) K has at least two elements.
(2) $0 * a = a * 0 = 0$ for all $a \in K$.
(3) $a * b = a * c$ and $a \neq 0$ imply that $b = c$ for all $a, b, c \in K$.
(4) $a * b = 0$ imply that $a = 0$ or $b = 0$ for all $a, b \in K$.

Proof

(1) This follows from the definition, since $0, 1 \in K$ with $0 \neq 1$.
(2) This has already been shown for rings (cp. Theorem 3.8).
(3) Since $a \neq 0$, we know that a^{-1} exists. Multiplying both sides of $a * b = a * c$ from the left with a^{-1} yields $b = c$.
(4) Suppose that $a * b = 0$. If $a = 0$, then we are finished. If $a \neq 0$, then a^{-1} exists and multiplying both sides of $a * b = 0$ from the left with a^{-1} yields $b = 0$. □

For a ring R an element $a \in R$ is called a *zero divisor*,[3] if a $b \in R \setminus \{0\}$ exists with $a * b = 0$. The element $a = 0$ is called the trivial zero divisor. Property (4) in Lemma 3.14 means that fields contain only the trivial zero divisor. There are also rings in which property (4) holds, for instance the ring of integers $\mathbb{Z}$. In later chapters we will encounter rings of matrices that contain non-trivial zero divisors (see e.g. the proof of Theorem 4.9 below).

The following definition is analogous to the concepts of a subgroup (cp. Definition 3.4) and a subring (cp. Excercise 3.14).

Definition 3.15 Let $(K, +, *)$ be a field and $L \subseteq K$. If $(L, +, *)$ is a field, then it is called a *subfield* of $(K, +, *)$.

As two very important examples for algebraic concepts discussed above we now discuss the *field of complex numbers* and the *ring of polynomials*.

[3]The concept of zero divisors was introduced in 1883 by Karl Theodor Wilhelm Weierstraß (1815–1897).

Example 3.16 The set of *complex numbers* is defined as

$$\mathbb{C} := \{ (x, y) \mid x, y \in \mathbb{R} \} = \mathbb{R} \times \mathbb{R}.$$

On this set we define the following operations as addition and multiplication:

$$\begin{aligned} + &: \mathbb{C} \times \mathbb{C} \to \mathbb{C}, \quad (x_1, y_1) + (x_2, y_2) := (x_1 + x_2, y_1 + y_2), \\ \cdot &: \mathbb{C} \times \mathbb{C} \to \mathbb{C}, \quad (x_1, y_1) \cdot (x_2, y_2) := (x_1 \cdot x_2 - y_1 \cdot y_2, x_1 \cdot y_2 + x_2 \cdot y_1). \end{aligned}$$

On the right hand sides we here use the addition and the multiplication in the field $\mathbb{R}$. Then $(\mathbb{C}, +, \cdot)$ is a field with the neutral elements with respect to addition and multiplication given by

$$\begin{aligned} 0_{\mathbb{C}} &= (0, 0), \\ 1_{\mathbb{C}} &= (1, 0), \end{aligned}$$

and the inverse elements with respect to addition and multiplication given by

$$\begin{aligned} -(x, y) &= (-x, -y) \quad \text{for all } (x, y) \in \mathbb{C}, \\ (x, y)^{-1} &= \left(\frac{x}{x^2 + y^2}, -\frac{y}{x^2 + y^2} \right) \quad \text{for all } (x, y) \in \mathbb{C} \setminus \{(0, 0)\}. \end{aligned}$$

In the multiplicative inverse element we have written $\frac{a}{b}$ instead of $a \cdot b^{-1}$, which is the common notation in $\mathbb{R}$.

Considering the subset $L := \{(x, 0) \mid x \in \mathbb{R}\} \subset \mathbb{C}$, we can identify every $x \in \mathbb{R}$ with an element of the set L via the (bijective) map $x \mapsto (x, 0)$. In particular, $0_{\mathbb{R}} \mapsto (0, 0) = 0_{\mathbb{C}}$ and $1_{\mathbb{R}} \mapsto (1, 0) = 1_{\mathbb{C}}$. Thus, we can interpret $\mathbb{R}$ as subfield of $\mathbb{C}$ (although $\mathbb{R}$ is not really a subset of $\mathbb{C}$), and we do not have to distinguish between the zero and unit elements in $\mathbb{R}$ and $\mathbb{C}$.

A special complex number is the *imaginary unit* $(0, 1)$, which satisfies

$$(0, 1) \cdot (0, 1) = (0 \cdot 0 - 1 \cdot 1, 0 \cdot 1 + 0 \cdot 1) = (-1, 0) = -1.$$

Here again we have identified the real number -1 with the complex number $(-1, 0)$. The imaginary unit is denoted by $\mathbf{i}$, i.e.,

$$\mathbf{i} := (0, 1),$$

and hence we can write $\mathbf{i}^2 = -1$. Using the identification of $x \in \mathbb{R}$ with $(x, 0) \in \mathbb{C}$ we can write $z = (x, y) \in \mathbb{C}$ as

$$(x, y) = (x, 0) + (0, y) = (x, 0) + (0, 1) \cdot (y, 0) = x + \mathbf{i}y = \mathrm{Re}(z) + \mathbf{i}\,\mathrm{Im}(z).$$

In the last expression $\mathrm{Re}(z) = x$ and $\mathrm{Im}(z) = y$ are the abbreviations for *real part* and *imaginary part* of the complex number $z = (x, y)$. Since $(0, 1) \cdot (y, 0) = (y, 0) \cdot (0, 1)$, i.e., $\mathbf{i}y = y\mathbf{i}$, it is justified to write the complex number $x + \mathbf{i}y$ as $x + y\mathbf{i}$.

For a given complex number $z = (x, y)$ or $z = x + \mathbf{i}y$ the number $\overline{z} := (x, -y)$, respectively $\overline{z} := x - \mathbf{i}y$, is called the associated *complex conjugate* number. Using the (real) square root, the *modulus* or *absolute value* of a complex number is defined as

$$|z| := (z\overline{z})^{1/2} = \big((x + \mathbf{i}y)\,(x - \mathbf{i}y)\big)^{1/2} = \big(x^2 - \mathbf{i}xy + \mathbf{i}yx - \mathbf{i}^2y^2\big)^{1/2} = (x^2 + y^2)^{1/2}.$$

(Again, for simplification we have omitted the multiplication sign between two complex numbers.) This equation shows that the absolute value of a complex number is a nonnegative real number. Further properties of complex numbers are stated in the exercises at the end of this chapter.

Example 3.17 Let $(R, +, \cdot)$ be a commutative ring with unit. A *polynomial over* R and in the indeterminate or variable t is an expression of the form

$$p = \alpha_0 \cdot t^0 + \alpha_1 \cdot t^1 + \ldots + \alpha_n \cdot t^n,$$

where $\alpha_0, \alpha_1, \ldots, \alpha_n \in R$ are the *coefficients* of the polynomial. Instead of $\alpha_0 \cdot t^0$, t^1 and $\alpha_j \cdot t^j$ we often just write α_0, t and $\alpha_j t^j$. The set of all polynomials over R is denoted by $R[t]$.

Let

$$p \;=\; \alpha_0 + \alpha_1 \cdot t + \ldots + \alpha_n \cdot t^n, \quad q \;=\; \beta_0 + \beta_1 \cdot t + \ldots + \beta_m \cdot t^m$$

be two polynomials in $R[t]$ with $n \geq m$. If $n > m$, then we set $\beta_j = 0$ for $j = m + 1, \ldots, n$ and call p and q *equal*, written $p = q$, if $\alpha_j = \beta_j$ for $j = 0, 1, \ldots, n$. In particular, we have

$$\begin{aligned} \alpha_0 + \alpha_1 \cdot t + \ldots + \alpha_n \cdot t^n &= \alpha_n \cdot t^n + \ldots + \alpha_1 \cdot t + \alpha_0, \\ 0 + 0 \cdot t + \ldots + 0 \cdot t^n &= 0. \end{aligned}$$

The *degree* of the polynomial $p = \alpha_0 + \alpha_1 \cdot t + \ldots + \alpha_n \cdot t^n$, denoted by $\deg(p)$, is defined as the largest index j, for which $\alpha_j \neq 0$. If no such index exists, then the polynomial is the *zero polynomial* $p = 0$ and we set $\deg(p) := -\infty$.

Let $p, q \in R[t]$ as above have degrees n, m, respectively, with $n \geq m$. If $n > m$, then we again set $\beta_j = 0$, $j = m + 1, \ldots, n$. We define the following operations on $R[t]$:

$$p + q := (\alpha_0 + \beta_0) + (\alpha_1 + \beta_1) \cdot t + \ldots + (\alpha_n + \beta_n) \cdot t^n,$$
$$p * q := \gamma_0 + \gamma_1 \cdot t + \ldots + \gamma_{n+m} \cdot t^{n+m}, \quad \gamma_k := \sum_{i+j=k} \alpha_i \beta_j.$$

With these operations $(R[t], +, *)$ is a commutative ring with unit. The zero is given by the polynomial $p = 0$ and the unit is $p = 1 \cdot t^0 = 1$. But $R[t]$ it is not a field, since not every polynomial $p \in R[t] \setminus \{0\}$ is invertible, not even if R is a field. For example, for $p = t$ and any other polynomial $q = \beta_0 + \beta_1 t + \ldots + \beta_m t^m \in R[t]$ we have

$$p * q = \beta_0 t + \beta_1 t^2 + \ldots + \beta_m t^{m+1} \neq 1,$$

and hence p is not invertible.

In a polynomial we can "substitute" the variable t by some other object when the resulting expression can be evaluated algebraically. For example, we may substitute t by any $\lambda \in R$ and interpret the addition and multiplication as the corresponding operations in the ring R. This defines a map from R to R by

$$\lambda \mapsto p(\lambda) = \alpha_0 \cdot \lambda^0 + \alpha_1 \cdot \lambda^1 + \ldots + \alpha_n \cdot \lambda^n, \quad \lambda^k := \underbrace{\lambda \cdot \ldots \cdot \lambda}_{\text{k times}}, \quad k = 0, 1, \ldots, n,$$

where $\lambda^0 = 1 \in R$ (this is an empty product). Here one should not confuse the ring element $p(\lambda)$ with the polynomial p itself, but rather think of $p(\lambda)$ as an *evaluation* of p at λ. We will study the properties of polynomials in more detail later on, and we will also evaluate polynomials at other objects such as matrices or endomorphisms.

Exercises

3.1 Determine for the following $(M, \oplus)$ whether they form a group:

(a) $M = \{x \in \mathbb{R} \mid x > 0\}$ and $\oplus : M \times M \to M$, $(a, b) \mapsto a^b$.
(b) $M = \mathbb{R} \setminus \{0\}$ and $\oplus : M \times M \to M$, $(a, b) \mapsto \frac{a}{b}$.

3.2 Let $a, b \in \mathbb{R}$, the map

$$f_{a,b} : \mathbb{R} \times \mathbb{R} \to \mathbb{R} \times \mathbb{R}, \quad (x, y) \mapsto (ax - by, ay),$$

and the set $G = \{f_{a,b} \mid a, b \in \mathbb{R}, \ a \neq 0\}$ be given. Show that $(G, \circ)$ is a commutative group, when the operation $\circ : G \times G \to G$ is defined as the composition of two maps (cp. Definition 2.18).

3.3 Let $X \neq \emptyset$ be a set and let $S(X) = \{f : X \to X \mid f \text{ is bijective}\}$. Show that $(S(X), \circ)$ is a group.

3.4 Let $(G, \oplus)$ be a group. For $a \in G$ denote by $-a \in G$ the (unique) inverse element. Show the following rules for elements of G:

(a) $-(-a) = a$.
(b) $-(a \oplus b) = (-b) \oplus (-a)$.
(c) $a \oplus b_1 = a \oplus b_2 \Rightarrow b_1 = b_2$.
(d) $a_1 \oplus b = a_2 \oplus b \Rightarrow a_1 = a_2$.

3.5 Prove Theorem 3.5.

3.6 Let $(G, \oplus)$ be a group and for a fixed $a \in G$ let $Z_G(a) = \{g \in G \mid a \oplus g = g \oplus a\}$. Show that $Z_G(a)$ is a subgroup of G.
(This subgroup of all elements of G that commute with a is called *centralizer* of a.)

3.7 Let $\varphi : G \to H$ be a group homomorphism. Show the following assertions:

(a) If $U \subseteq G$ is a subgroup, then also $\varphi(U) \subseteq H$ is a subgroup. If, furthermore, G is commutative, then also $\varphi(U)$ is commutative (even if H is not commutative).
(b) If $V \subseteq H$ is a subgroup, then also $\varphi^{-1}(V) \subseteq G$ is a subgroup.

3.8 Let $\varphi : G \to H$ be a group homomorphism and let e_G and e_H be the neutral elements of the groups G and H, respectively.

(a) Show that $\varphi(e_G) = e_H$.
(b) Let $\ker(\varphi) := \{g \in G \mid \varphi(g) = e_H\}$. Show that φ is injective if and only if $\ker(\varphi) = \{e_G\}$.

3.9 Show the properties in Definition 3.7 for $(R, +, *)$ from Example 3.9 in order to show that $(R, +, *)$ is a commutative ring with unit. Suppose that in Example 3.9 we replace the codomain $\mathbb{R}$ of the maps by a commutative ring with unit. Is $(R, +, *)$ then still a commutative ring with unit?

3.10 Let R be a ring and $n \in \mathbb{N}$. Show the following assertions:

(a) For all $a \in R$ we have $(-a)^n = \begin{cases} a^n, & \text{if } n \text{ is even,} \\ -a^n, & \text{if } n \text{ is odd.} \end{cases}$
(b) If there exists a unit in R and if $a^n = 0$ for $a \in R$, then $1 - a$ is invertible.
(An element $a \in R$ with $a^n = 0$ for some $n \in \mathbb{N}$ is called *nilpotent*.)

3.11 Let R be a ring with unit. Show that $1 = 0$ if and only if $R = \{0\}$.

3.12 Let $(R, +, *)$ be a ring with unit and let $R^\times$ denote the set of all invertible elements of R.

(a) Show that $(R^\times, *)$ is a group (called the *group of units* of R).
(b) Determine the sets $\mathbb{Z}^\times$, $K^\times$, and $K[t]^\times$, when K is a field.

3.13 For fixed $n \in \mathbb{N}$ let $n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\}$ and $\mathbb{Z}/n\mathbb{Z} = \{[0], [1], \ldots, [n-1]\}$ be as in Example 2.29.

(a) Show that $n\mathbb{Z}$ is a subgroup of $\mathbb{Z}$.
(b) Define by

$$\oplus : \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}, \quad ([a], [b]) \mapsto [a] \oplus [b] = [a + b],$$
$$\odot : \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}, \quad ([a], [b]) \mapsto [a] \odot [b] = [a \cdot b],$$

an addition and multiplication in $\mathbb{Z}/n\mathbb{Z}$, (with $+$ and $\cdot$ being the addition and multiplication in $\mathbb{Z}$). Show the following assertions:

(i) $\oplus$ and $\odot$ are well defined.
(ii) $(\mathbb{Z}/n\mathbb{Z}, \oplus, \odot)$ is a commutative ring with unit.
(iii) $(\mathbb{Z}/n\mathbb{Z}, \oplus, \odot)$ is a field if and only if n is a prime number.

3.14 Let $(R, +, *)$ be a ring. A subset $S \subseteq R$ is called a *subring* of R, if $(S, +, *)$ is a ring. Show that S is a subring of R if and only if the following properties hold:

(1) $S \subseteq R$.
(2) $0_R \in S$.
(3) For all $r, s \in S$ also $r + s \in S$ and $r * s \in S$.
(4) For all $r \in S$ also $-r \in S$.

3.15 Show that the Definitions 3.12 and 3.13 of a field describe the same mathematical structure.

3.16 Let $(K, +, *)$ be a field. Show that $(L, +, *)$ is a subfield of $(K, +, *)$ (cp. Definition 3.15), if and only if the following properties hold:

(1) $L \subseteq K$.
(2) $0_K, 1_K \in L$.
(3) $a + b \in L$ and $a * b \in L$ for all $a, b \in L$.
(4) $-a \in L$ for all $a \in L$.
(5) $a^{-1} \in L$ for all $a \in L \setminus \{0\}$.

3.17 Show that in a field $1 + 1 = 0$ holds if and only if $1 + 1 + 1 + 1 = 0$.

3.18 Let $(R, +, *)$ be a commutative ring with $1 \neq 0$ that does not contain non-trivial zero divisors. (Such a ring is called an *integral domain*.)

(a) Define on $M = R \times R \setminus \{0\}$ a relation by

$$(x, y) \sim (\widehat{x}, \widehat{y}) \quad \Leftrightarrow \quad x * \widehat{y} = y * \widehat{x}.$$

Show that this is an equivalence relation.

(b) Denote the equivalence class $[(x, y)]$ by $\frac{x}{y}$. Show that the following maps are well defined:

$$\oplus : (M/\sim) \times (M/\sim) \to (M/\sim) \quad \text{with} \quad \frac{x}{y} \oplus \frac{\widehat{x}}{\widehat{y}} := \frac{x * \widehat{y} + y * \widehat{x}}{y * \widehat{y}},$$

$$\odot : (M/\sim) \times (M/\sim) \to (M/\sim) \quad \text{with} \quad \frac{x}{y} \odot \frac{\widehat{x}}{\widehat{y}} := \frac{x * \widehat{x}}{y * \widehat{y}},$$

where $M/\sim$ denotes the quotient set with respect to $\sim$ (cp. Definition 2.27).

(c) Show that $(M/\sim, \oplus, \odot)$ is a field. (This field is called the *quotient field* associated with R.)

(d) Which field is $(M/\sim, \oplus, \odot)$ for $R = \mathbb{Z}$?

3.19 In Exercise 3.18 consider $R = K[t]$, the ring of polynomials over the field K, and construct in this way the field of *rational functions*.

3.20 Let $a = 2 + \mathbf{i} \in \mathbb{C}$ and $b = 1 - 3\mathbf{i} \in \mathbb{C}$. Determine $-a, -b, a + b, a - b$, $a^{-1}, b^{-1}, a^{-1}a, b^{-1}b, ab, ba$.

3.21 Show the following rules for the complex numbers:

(a) $\overline{z_1 + z_2} = \overline{z}_1 + \overline{z}_2$ and $\overline{z_1 z_2} = \overline{z}_1\,\overline{z}_2$ for all $z_1, z_2 \in \mathbb{C}$.
(b) $\overline{z^{-1}} = (\overline{z})^{-1}$ and $\mathrm{Re}(z^{-1}) = \frac{1}{|z|^2}\mathrm{Re}(z)$ for all $z \in \mathbb{C} \setminus \{0\}$.

3.22 Show that the absolute value of complex numbers satisfies the following properties:

(a) $|z_1 z_2| = |z_1|\,|z_2|$ for all $z_1, z_2 \in \mathbb{C}$.
(b) $|z| \geq 0$ for all $z \in \mathbb{C}$ with equality if and only if $z = 0$.
(c) $|z_1 + z_2| \leq |z_1| + |z_2|$ for all $z_1, z_2 \in \mathbb{C}$.