Introduction to Algebraic Structures

Lecture Notes 2019

Janko Böhm, Magdaleen Marais

November 6, 2019

Contents

List of Figures

List of Symbols

0

Introduction

In this course, we will focus on the foundations of algebra, including linear algebra. We will also discuss some very simple, but nevertheless fundamental facts from number theory. Algebra and number theory are very closely related areas of pure mathematics, complementing analysis, combinatorics[1], geometry and topology[2].

What is number theory? As the name says, number theory is studying the properties of the integer numbers $(..., -1, 0, 1, 2, 3, ...)$, in particular the relation of addition and multiplication. Many number theory problems are easy to formulate, but very difficult to solve. The most prominent example is Fermat's last theorem from 1637: For $n \geq 3$ there are no (non-trivial) integer solutions

[1] Using combinatorics one can, for example, compute that in the standard lotto game there are $\binom{49}{6} \approx 14\,000\,000$ possible results.

[2] In topology one can see, for example, that the knot in Figure 1 cannot be untangled without cutting the string.

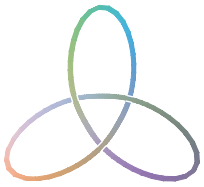


Figure 1: Knot

of the equation

$$x^n + y^n = z^n.$$

Fermat's last theorem was only proven 1995 (by A. Wiles) after 350 years of work of many mathematicians, which involved introducing various new concepts in mathematics. Today, there are close connections of number theory to, for example, algebraic geometry, combinatorics, cryptography and coding theory.

What is algebra? Algebra is a very diverse area of mathematics, which discusses basic structures which are of key importance in all fields of mathematics, like groups rings and fields. That is, algebra studies the question, how one can introduce operations on sets, like the addition and multiplication of integer numbers. By combining methods from algebra and number theory, one can construct, for example, public key cryptosystems. Another connection of algebra and number theory arises from algebraic geometry, which studies solution sets of polynomial systems of equations in several variables[3].

The simplest (but in practice the most important) special case are linear systems of equations over a field K (for example, $K = \mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ the field of rational, real or complex numbers), the

[3]For example, the common solution set of $x^2 + 2y^2 = 3$ and $2x^2 + y^2 = 3$, that is, the intersection of two ellipses, consists out of 4 points $(1,1), (-1,1), (1,-1), (-1,-1)$, see Figure 2.

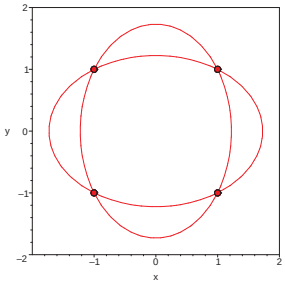


Figure 2: Four points.

core topic of linear algebra. Here, we solve systems

$$\begin{aligned} a_{1,1}x_1 + ... + a_{1,m}x_m &= b_1 \\ &\vdots \\ a_{n,1}x_1 + ... + a_{n,m}x_m &= b_n \end{aligned}$$

with $a_{ij} \in K$, $b_i \in K$ for $x_j \in K$ (with $i = 1, ..., n$ and $j = 1, ...m$). As an application of linear algebra, we will discuss the Google page rank algorithm.

Let us also comment on an other special case, which however goes beyond the topics discussed in this course, that is, polynomial equations of higher degree in a single variable x. For example, one can ask for the solution set of the quadratic equation

$$ax^2 + bx + c = 0.$$

The solutions can be described, using radicals, as

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

In a similar way, one can find expressions in terms of radicals for equations of degree $d = 3$ (Tartaglia 1535, Cardano 1545) and $d = 4$ (Ferrari 1522), for $d \geq 5$ the solutions can, in general, not be written in terms of radical any more. An important subtopic of algebra, the Galois theory, discusses when this is possible.

1

Fundamental constructions

In this section, we discuss fundamental construction, which are used to construct from given mathematical objects new mathematical objects. Starting out with the notation of a set, we discuss how two given sets can be related to each other. In particular, we will discuss maps and equivalence relations.

1.1 Sets

Definition 1.1.1 (Cantor) *A **set** is a collection of definite, distinct objects m, concrete or imaginary, thus forming a new object M.*

If m is an element of M, we write

$$m \in M,$$

if not, then $m \notin M$. We write the set M with elements $m_1, m_2, ...$ as

$$M = \{m_1, m_2, ...\}.$$

We call the set with no elements the **empty set** $\varnothing = \{\ \}$.

Remark 1.1.2 *The definition we interpret as follows: Objects are mathematical objects and the collection of objects into a set, is a new mathematical object. By the term distinct, we mean that we can decide for any two objects in the set, whether they are equal or not.*

Example 1.1.3 *The following sets of numbers are examples of sets: The numerical digits*

$$\{0, 1, 2, ..., 9\},$$

the natural numbers

$$\mathbb{N} = \{1, 2, 3, ...\}$$
$$\mathbb{N}_0 = \{0, 1, 2, 3, ...\},$$

the integers

$$\mathbb{Z} = \{0, 1, -1, 2, -2, ...\},$$

the rational numbers

$$\mathbb{Q} = \left\{ \frac{a}{b} \mid a, b \in \mathbb{Z},\ b \neq 0 \right\}.$$

The Symbol | is written in place of ***with****.*

Definition 1.1.4 *If every element of the set N is also an element of the set M (that is, $m \in N \Rightarrow m \in M$), then N is called a* ***subset*** *of M (we write $N \subset M$ or $N \subseteq M$). The symbol $\Rightarrow$ is used in place of* ***from which it follows that****.*

Two sets M_1 and M_2 are ***equal*** *(we write $M_1 = M_2$), when $M_1 \subset M_2$ and $M_2 \subset M_1$. That means $m \in M_1 \Leftrightarrow m \in M_2$. Here the symbol $\Leftrightarrow$ is written instead of* ***if and only if****, that is both $\Rightarrow$ as well as $\Leftarrow$ holds.*

Example 1.1.5 $\{0, ..., 9\} \subset \mathbb{N}_0$.

Definition 1.1.6 *Let M, N be sets. Then the* ***complement*** *of N in M is,*

$$M \backslash N = \{m \in M \mid m \notin N\}.$$

The complement $M \backslash N$ can be seen in terms of a so-called Venn-Diagram in Figure 1.1. Further we call

$$M \cup N = \{m \mid m \in M \text{ or } m \in N\}$$

the ***union*** *of M and N, see Figure 1.2, and*

$$M \cap N = \{m \mid m \in M \text{ und } m \in N\}$$

intersection *of M and N, see Figure 1.3.*

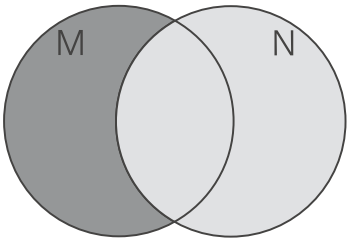


Figure 1.1: Complement

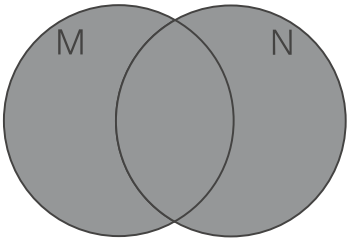


Figure 1.2: Union

Example 1.1.7 $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$.

Notation 1.1.8 *For an index set $I \neq \varnothing$ and sets M_i, $i \in I$, we write*

$$\bigcap_{i \in I} M_i = \{m \mid m \in M_i \text{ for all } i \in I\}$$

for the intersection of the M_i, $i \in I$, and

$$\bigcup_{i \in I} M_i = \{m \mid \text{there exists } i \in I \text{ with } m \in M_i\}$$

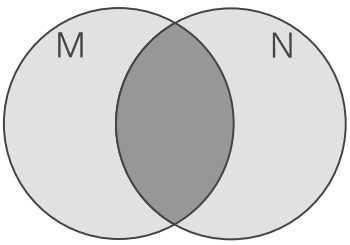


Figure 1.3: Intersection

for the union of the M_i, $i \in I$.

We abbreviate ***for all*** *by* $\forall$*, and* ***there exists*** *by* $\exists$*.*

Example 1.1.9 *For $I = \{1, 2\}$ and given sets M_1 and M_2*

$$\bigcap_{i \in I} M_i = M_1 \cap M_2.$$

Definition 1.1.10 *We write $|M|$ or $\#M$ for the* ***number of elements*** *of a finite set M and, $|M| = \infty$, if M has infinite many elements.*

Example 1.1.11 *That is $|\varnothing| = 0$, $|\{0, ..., 9\}| = 10$ and $|\{0\}| = 1$.*

Definition 1.1.12 *Let $M_1, ..., M_n$ be sets. Then the set*

$$M_1 \times ... \times M_n = \{(m_1, ..., m_n) \mid m_i \in M_i \ \forall i = 1, ..., n\}$$

of ordered tuples constructed from elements of $M_1, ..., M_n$, is called the ***cartesian product*** *of $M_1, ..., M_n$. For $n \in \mathbb{N}$ we write*

$$M^n = \underbrace{M \times ... \times M}_{n\text{-}times}.$$

The elements of M^n are lists $(m_1, ..., m_n)$ of length n with entries in M.

Example 1.1.13 *We have*

$$\{1, 2, 3\} \times \{3, 4\} = \{(1, 3), (1, 4), (2, 3), (2, 4), (3, 3), (3, 4)\}.$$

The chess board is the cartesian product

$$\{a, ..., h\} \times \{1, ..., 8\} = \{(a, 1), ...\},$$

the 3-dimensional space is

$$\mathbb{R}^3 = \mathbb{R} \times \mathbb{R} \times \mathbb{R},$$

and the set of 8-bit numbers is

$$\{0, 1\}^8 = \{(0, ..., 0, 0), (0, ..., 0, 1), ..., (1, ..., 1, 1)\}.$$

Definition 1.1.14 *Let M be a set. The* ***power set*** *of M is*

$$2^M = \mathfrak{P}(M) = \{A \mid A \subset M\}.$$

Theorem 1.1.15 *Let M be a finite set. Then*

$$\left|2^M\right| = 2^{|M|}.$$

Example 1.1.16 *Power sets:*

$$\begin{aligned} 2^{\varnothing} &= \{\varnothing\} \\ 2^{\{1\}} &= \{\varnothing, \{1\}\} \\ 2^{\{1,2\}} &= \{\varnothing, \{1\}, \{2\}, \{1,2\}\}. \end{aligned}$$

We use the following general principle for proofs to prove, for example, Theorem 1.1.15.

1.2 Mathematical induction

Suppose we have for every $n \in \mathbb{N}_0$ a given claim $A(n)$, and furthermore it is given that:

1) **Base case**: $A(0)$ is true.

2) **Induction step**: it follows for every $n > 0$ that

$$A(n-1) \text{ is true} \Rightarrow A(n) \text{ is true.}$$

Then $A(n)$ is true for all $n \in \mathbb{N}_0$. In fact we have the following chain of conclusions:

$$A(0) \text{ true } \Rightarrow A(1) \text{ true } \Rightarrow A(2) \text{ true } \Rightarrow \ldots$$

Remark 1.2.1 *Analogously, one can of course proceed to prove statements $A(n)$ for $n \geq n_0$ with $n_0 \in \mathbb{Z}$. One only has to make sure that the initial step $A(n_0)$ and all subsequent arrows used in the chain of conclusions*

$$A(n_0) \textit{ true } \Rightarrow A(n_0+1) \textit{ true } \Rightarrow A(n_0+2) \textit{ true } \Rightarrow \ldots$$

are proven.

Using induction, we now prove Theorem 1.1.15:

Proof. By numbering the elements of M we can assume without loss of generality (written in short WLOG) that $M = \{1, \dots, n\}$, using the convention that $\{1, \dots, 0\} = \varnothing$. So we have to show that the statement

$$\left|2^{\{1,\dots,n\}}\right| = 2^n$$

hold true for all $n \in \mathbb{N}_0$.

Initial step $n = 0$: It is $2^{\varnothing} = \{\varnothing\}$, and hence $|2^{\varnothing}| = 1 = 2^0$.

Inductive step $n-1$ to n: The union

$$\begin{aligned} 2^{\{1,\dots,n\}} &= \{A \subset \{1, \dots, n\} \mid n \notin A\} \dot\cup \\ &\quad \{A \subset \{1, \dots, n\} \mid n \in A\} \\ &= \{A \mid A \subset \{1, \dots, n-1\}\} \dot\cup \{A' \cup \{n\} \mid A' \subset \{1, \dots, n-1\}\} \end{aligned}$$

is disjoint, and therefore it follows from the **induction hypothesis**

$$\left|2^{\{1,\dots,n-1\}}\right| = 2^{n-1},$$

that

$$\left|2^{\{1,\dots,n\}}\right| = 2^{n-1} + 2^{n-1} = 2^n.$$

■

Next we discuss another typical example of a proof using induction.

Notation 1.2.2 *We write*

$$\sum_{k=1}^{n} a_k = a_1 + \dots + a_n$$

for the sum of the numbers $a_1, \dots, a_n$.

Similar we use

$$\prod_{k=1}^{n} a_k = a_1 \cdot \dots \cdot a_n$$

for their product.

When the numbers a_k *are represented by the elements* k *of the set* I*, we write*

$$\sum_{k \in I} a_k$$

for their sum and, analoguesly $\prod_{k \in I} a_k$ *for their product.*

Remark 1.2.3 *Given the list* $a = (a_1, ..., a_n)$ *the following computer program computes the sum* $s = \sum_{k=1}^{n} a_k$*:*

```
s:=0;
for k from 1 to n do
    s:=s+a[k];
od;
```

We use the syntax of MAPLE*, see [21], but the code will be similar in most programming language. See also Exercise 1.3.*

Using induction, we can prove the following general formula for the sum $\sum_{k=1}^{n} k$, which allows a much more efficient calculation for this specific sum:

Theorem 1.2.4 *For all* $n \in \mathbb{N}_0$*,*

$$\sum_{k=0}^{n} k = \frac{n(n+1)}{2}.$$

Proof. *Initial step* $n = 0$: We have

$$\sum_{k=0}^{0} k = 0 = \frac{0 \cdot (0+1)}{2}.$$

Inductive step n to $n+1$: We have

$$\sum_{k=1}^{n+1} k = \sum_{k=1}^{n} k + (n+1),$$

and hence it follows from the induction hypothesis that

$$\begin{aligned} \sum_{k=0}^{n+1} k &= \frac{n(n+1)}{2} + (n+1) \\ &= \frac{n(n+1) + 2(n+1)}{2} \\ &= \frac{(n+1)(n+2)}{2}. \end{aligned}$$

■

For a further example, see Exercise 1.4.

Remark 1.2.5 *The analogue to a proof by induction is in computer science the concept of a recursive algorithm. For example, the following recursive function calculates the sum* $\sum_{k=0}^{n} k$*:*

```
sumints:=proc(n)
    if n=0 then return(0);fi;
    return(sumints(n-1)+n);
end proc;
```

We can also write a recursive function that determines all subsets of $\{1, ..., n\}$ *from the proof of Theorem 1.1.15. For the implementation thereof, see Exercise 1.8. Another proof by induction, which provides a recursive algorithm, is discussed in Exercises 1.10 and 1.11.*

For further examples of induction, see the Exercises 1.5, 1.6, 1.7 and 1.12.

1.3 Relations

In the following way we can describe relations between two sets:

Definition 1.3.1 *A* ***relation*** *relation between sets* M *and* N *is given by the subset* $R \subset M \times N$*.*

Example 1.3.2 *For* $M = \{2, 3, 7\}$*,* $N = \{4, 5, 6\}$ *and*

$$R = \{(m, n) \in M \times N \mid m \text{ divides } n\}$$

we have

$$R = \{(2, 4), (2, 6), (3, 6)\}\,.$$

The most important role is played by relations in which each element of M gets assigned exactly one element of N:

1.4 Maps

Definition 1.4.1 *A* ***map*** $f : M \to N$ *is a relation* $R \subset M \times N$*, such that for every* $m \in M$ *there is a unique element* $f(m) \in N$ *with* $(m, f(m)) \in R$*. We write*

$$\begin{array}{rccc} f: & M & \to & N \\ & m & \mapsto & f(m). \end{array}$$

*We call M the **source** and N the **target** of f.*
For a subset $A \subset M$

$$f(A) = \{f(m) \mid m \in A\} \subset N$$

*is called the **image** of A under f, and*

$$\text{Image}(f) := f(M)$$

is called the image of f.
For $B \subset N$

$$f^{-1}(B) = \{m \in M \mid f(m) \in B\} \subset M$$

*is called the **preimage** of B under f.*

Remark 1.4.2 *If a map is given by a mapping rule $f : M \to N$, $m \mapsto f(m)$, the representation of f as a relation is nothing else than the graph*

$$R = \text{Graph}(f) = \{(m, f(m)) \mid m \in M\} \subset M \times N$$

of f.

Example 1.4.3 *For*

$$\begin{array}{rccc} f: & \mathbb{R} & \to & \mathbb{R} \\ & x & \mapsto & f(x) = x^2 \end{array}$$

we have

$$R = \text{Graph}(f) = \left\{(x, x^2) \mid x \in \mathbb{R}\right\},$$

see Figure 1.4. The image of f is

$$f(\mathbb{R}) = \mathbb{R}_{\geq 0}$$

and we have

$$f^{-1}(\{1, 2\}) = \{-1, 1, -\sqrt{2}, \sqrt{2}\}.$$

Definition 1.4.4 *A map $f : M \to N$ is **surjective**, if for the image of f we have*

$$f(M) = N.$$

If for all $m_1, m_2 \in M$ we have, that

$$f(m_1) = f(m_2) \Longrightarrow m_1 = m_2,$$

*then f is **injective**.*
*A map that is both injective and surjective is **bijective**.*

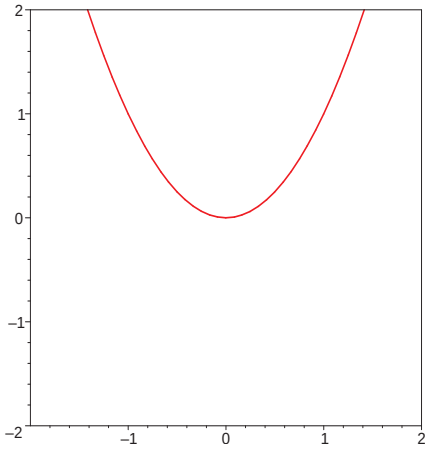


Figure 1.4: Graph of parabola.

Example 1.4.5 *The parabola function*

$$\mathbb{R} \to \mathbb{R},\ x \mapsto x^2$$

in Example 1.4.3 is neither injective or surjective. As a map onto its image

$$\mathbb{R} \to \mathbb{R}_{\geq 0},\ x \mapsto x^2$$

it becomes surjective. The map

$$\mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0},\ x \mapsto x^2$$

in which we also restrict the source is bijective. The hyperbola

$$\mathbb{R}\backslash\{0\} \to \mathbb{R},\ x \mapsto \frac{1}{x}$$

is injective, but not surjective (see Figure 1.5).

Theorem 1.4.6 (Pigeonhole principle) *If M, N are finite sets and if $f : M \to N$ is an injective mapping, then $|M| \leq |N|$.*

Example 1.4.7 *Let $M = \{1, 2, 3\}$ and $N = \{1, 2\}$. Since $|M| > |N|$ there is no injective mapping $f : M \to N$. Figure 1.6 shows an example of a map $f : M \to N$. Since $f(1) = f(3)$, it follows that f is not injective.*

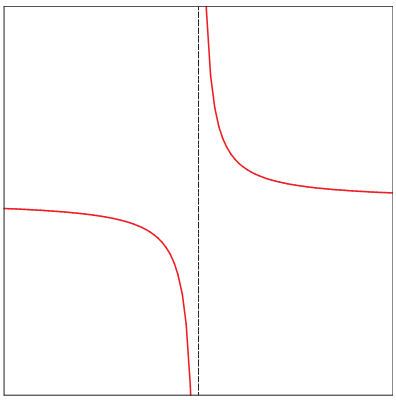


Figure 1.5: Hyperbola

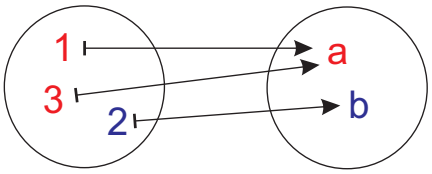


Figure 1.6: A non-injective map

We now prove Theorem 1.4.6:

Proof. We have

$$|N| = \sum_{n \in N} 1 \geq \sum_{n \in N} \left| f^{-1}(\{n\}) \right| = |M|,$$

since $f^{-1}(\{n\})$ has exactly 1 element, if n lies in the image of f (since f is injektive), and is empty otherwise. The second equality holds true, since M is the disjoint union

$$M = \dot{\bigcup_{n \in N}} f^{-1}(\{n\})$$

of the level sets $f^{-1}(\{n\})$ of the map f (which is analogous to the contour lines on a map giving the height of the respective point): A map assigns to each element m exactly one value n. We will come back to this idea in the context of equivalence relations. ■

Since a map assigns exactly one image element to each element of the source, the corresponding statement for surjective maps follows directly:

Theorem 1.4.8 *If M, N are finite sets and $f : M \to N$ a surjective map, then $|M| \geq |N|$.*

Combining Theorem 1.4.6 and Theorem 1.4.8, we have:

Corollary 1.4.9 *If M, N are finite sets and $f : M \to N$ a bijective map, then $|M| = |N|$.*

Definition and Theorem 1.4.10 *If $f : M \to N$ is bijective, then there is a unique* ***inverse map***

$$f^{-1} : N \to M,\ y \mapsto x \text{ if } f(x) = y.$$

We have

$$f^{-1}(f(x)) = x \qquad \text{and} \qquad f(f^{-1}(y)) = y$$

for all $x \in M$ and $y \in N$, respectively. Moreover, f^{-1} is bijective.

Proof. The inverse map is **well-defined** (that is, its definition assignes to every element of the source a unique element of the target): For every $y \in N$ there is exactly one $x \in M$ with $f(x) = y$. Since f is surjective there exists such an x, and since f is injective, this x is unique.

The two equalities are clear by definition of f^{-1}. On the bijectivity of f^{-1}: Since for every $x \in M$ we have $f^{-1}(f(x)) = x$, the map f^{-1} is surjective. For the injectivity, we use that f is a map: If $y_1, y_2 \in N$ and $x_i \in M$ with $y_i = f(x_i)$, then from

$$x_1 = f^{-1}(y_1) = f^{-1}(y_2) = x_2,$$

it follows, that $y_1 = f(x_1) = f(x_2) = y_2$. ■

For the term "there is a unique" used above, we also write the symbol $\exists_1$.

Remark 1.4.11 *The inverse map f^{-1} is the relation*

$$\{(f(x), x) \mid x \in M\} \subset N \times M.$$

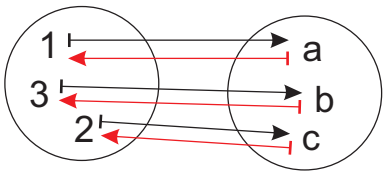


Figure 1.7: A bijektive map and its inverse map.

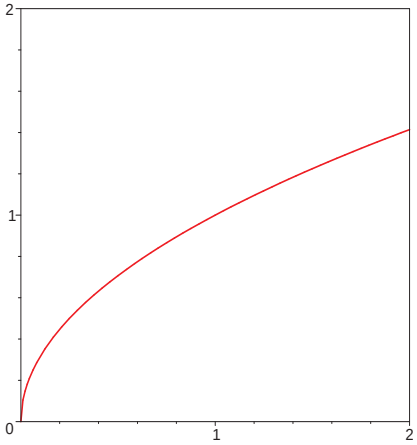


Figure 1.8: Square root

Example 1.4.12 *Figure 1.7 shows a bijective map* $f : \{1, 2, 3\} \to \{a, b, c\}$ *and its inverse map* f^{-1}*. The inverse of the bijective map*

$$\mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0},\ x \mapsto x^2$$

is

$$\mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0},\ y \mapsto \sqrt{y}$$

as shown in Figure 1.8.

See also the Exercises 1.14, 1.17, 1.18 and 1.19.

Definition 1.4.13 *Let* $f : M \to N$ *and* $g : N \to L$ *be maps. Then the composition of* f *and* g *is defined as*

$$\begin{array}{rccc} g \circ f : & M & \to & L \\ & m & \mapsto & g(f(m)) \end{array}$$

Lemma 1.4.14 *The composition of maps is associative, that is, for maps*

$$M \xrightarrow{f} N \xrightarrow{g} L \xrightarrow{h} K$$

we have

$$h \circ (g \circ f) = (h \circ g) \circ f.$$

For the proof see Exercise 1.15.

Example 1.4.15 *Even if $f : M \to M$ and $g : M \to M$, in general $f \circ g \neq g \circ f$. For example for*

$$f : \mathbb{R}^2 \to \mathbb{R}^2,\ (x, y) \mapsto (x + y, y)$$
$$g : \mathbb{R}^2 \to \mathbb{R}^2,\ (x, y) \mapsto (x, x + y)$$

we get

$$f \circ g : \mathbb{R}^2 \to \mathbb{R}^2,\ (x, y) \mapsto (2x + y, x + y)$$
$$g \circ f : \mathbb{R}^2 \to \mathbb{R}^2,\ (x, y) \mapsto (x + y, x + 2y).$$

Definition 1.4.16 *Let M be a set. The **identity map** on M is*

$$\begin{array}{rccc} \mathrm{id}_M : & M & \to & M \\ & m & \mapsto & m \end{array}$$

Example 1.4.17 *Figure 1.9 shows the graph of $\mathrm{id}_{\mathbb{R}}$.*

The equations in Definition and Theorem 1.4.10 can then be wirtten as follows:

Theorem 1.4.18 *If $f : M \to N$ is a bijective map, then*

$$f^{-1} \circ f = \mathrm{id}_M \qquad f \circ f^{-1} = \mathrm{id}_N$$

Indeed, these equalities characterize the property bijective and uniquely define the inverse map. For this see Exercise 1.16.

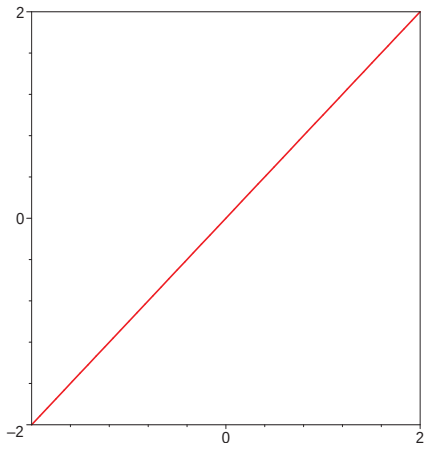


Figure 1.9: Identity map $\mathbb{R} \to \mathbb{R}$

1.5 Partial orderings and equivalence relations

Definition 1.5.1 *A relation $R \subset M \times M$ on a set M is called*

- ***reflexive**, if $(m, m) \in R$ for all $m \in M$,*
- ***transitive**, if*

$$(l, m) \in R \text{ and } (m, n) \in R \Longrightarrow (l, n) \in R,$$

- ***anti-symmetric**, if*

$$(n, m) \in R \text{ and } (m, n) \in R \Longrightarrow m = n.$$

*If R is reflexive, transitive, and anti-symmetric, then R is called a **partial ordering**. If, in addition, for all $m, n \in M$ we have $(m, n) \in R$ or $(n, m) \in R$, then R is called a **total ordering**.*

Example 1.5.2 *1) The inclusion $\subset$ of subsets of a set M is a partial ordering on the power set 2^M: For all $A, B, C \subset M$ we have*

- *$A \subset A$ (reflexive)*

- $A \subset B$ *and* $B \subset C \Longrightarrow A \subset C$ *(transitive)*
- $A \subset B$ *and* $B \subset A \Longrightarrow A = B$ *(anti-symmetric).*

In general $\subset$ *is not a total ordering, for example, for* $M = \{1, 2\}$ *neither* $\{1\} \subset \{2\}$ *nor* $\{2\} \subset \{1\}$.

2) In contrast, $\leq$ *on* $\mathbb{R}$ *is a total ordering.*

The concept of an equivalence relation relaxes the concept of equality.

Definition 1.5.3 *Let* M *be a set and* $R \subset M \times M$ *a reflexive and transitive relation. If* R *is in addition* ***symmetric****, that is,*

$$(m, n) \in R \Rightarrow (n, m) \in R,$$

then R *is called an* ***equivalence relation****.*

If we write $m \sim n$ for $(m, n) \in R$, then

- reflexive means, that $m \sim m$ for all $m \in M$,
- transitive means, that $m \sim l$ and $l \sim n \Rightarrow m \sim n$ for all $m, l, n \in M$ and
- symmetric means, that $m \sim n \Rightarrow n \sim m$ for all $m, n \in M$.

Example 1.5.4 *Equality is an equivalence relation.*

The property of two persons to be the same height, is an equivalence relation (in contrast, the property of being the same hight up to $1cm$ *difference is not an equivalence relation, since it is not transitive).*

More generally: Let $f : M \to N$ *be a map. Then*

$$m_1 \sim m_2 \Longleftrightarrow f(m_1) = f(m_2)$$

defines an equivalence relation on M.

Definition 1.5.5 *If* M *is a set and* $\sim$ *is an equivalence relation and* $m \in M$*, then*

$$[m] = \{n \in M \mid m \sim n\} \subset M$$

is called the ***equivalence class*** *of* m. *Every* $n \in [m]$ *is called a* ***representative*** *of* $[m]$.

Moreover, we write

$$M/\sim = \{[m] \mid m \in M\} \subset 2^M$$

for the set of equivalence classes of $\sim$ *and*

$$\begin{array}{rccc} \pi: & M & \to & M/\sim \\ & m & \mapsto & [m] \end{array}$$

for the ***canonical map***.

Theorem 1.5.6 *Given an equivalence relation, any two equivalence classes are equal or disjoint.*

Proof. Let $[m] \cap [n] \neq \varnothing$. We have to show that $[m] = [n]$. If $a \in [m] \cap [n]$, that is, $a \sim m$ and $a \sim n$, then, using symmetry and transitivity, it follows that $m \sim n$, that is, $m \in [n]$. Let $a \in [m]$ be any element. Then $a \sim m$ and $m \sim n$, hence $a \sim n$, that is, $a \in [n]$. So we have seen, that $[m] \subset [n]$. The other inclusion follows in the same way. ■

An equivalence relation paritions (subdivides) M in the equivalence classes.

Remark 1.5.7 *We have*

$$m_1 \sim m_2 \iff [m_1] = [m_2],$$

that is, equivalence translates into equality of equivalence classes.

Example 1.5.8 *The equivalence classes under the equivalence relation of being the same hight on a set* M *of persons (see Example 1.5.4) are the subsets of all persons with the same hight. So the set of equivalence classes* $M/\sim$ *is in bijection to the set of all occuring hights of persons. A cloths sales person is interested mainly in* $[m]$ *not in* m.

Example 1.5.9 *Consider the equivalence relation* $\sim$ *on* $\mathbb{R}^2$ *given by*

$$(x_1, y_1) \sim (x_2, y_2) \iff f(x_1, y_1) = f(x_2, y_2)$$

with

$$f(x,y) = x^2 + y^2.$$

The equivalence classes are the concentric circles

$$K_s = \left\{(x,y) \in \mathbb{R}^2 \mid x^2 + y^2 = s\right\}$$

for $s \in \mathbb{R}_{\geq 0}$*, and the point* $(0,0)$*, which is a degenerate form of a circle, the circle with radius* 0*. For example,*

$$[(1,2)] = \left\{(x,y) \in \mathbb{R}^2 \mid x^2 + y^2 = 5\right\}.$$

Hence

$$M/\sim \; = \{K_s \mid s \in \mathbb{R}_{\geq 0}\},$$

and the map $\mathbb{R}_{\geq 0} \to M/\sim$*,* $s \mapsto K_s$ *is bijective. See Figure 1.10.*

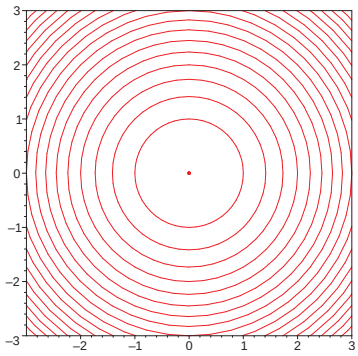


Figure 1.10: Equivalence classes

1.6 Exercises

Exercise 1.1 *Let* M *be a set. Show that for subsets* $A, B, C \subset M$ *(using, for example, Venn diagrams):*

1) *For* $\cap$ *we have:*

   (a) *Commutativity* $A \cap B = B \cap A$*,*

   (b) *Identity* $A \cap M = A$*,*

   (c) *Assoziativity* $A \cap (B \cap C) = (A \cap B) \cap C$*.*

2) For $\cup$ we have:

(a) Commutativity $A \cup B = B \cup A$,

(b) Identity $A \cup \varnothing = A$,

(c) Assoziativity $A \cup (B \cup C) = (A \cup B) \cup C$.

3) For $\cap$ and $\cup$ the distributive laws hold:

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$$
$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$$

4) Compare with the arithmetic rules for integers.

Exercise 1.2 *Show for finite sets M and N that*

$$|M \cup N| = |M| + |N| - |M \cap N|$$

and

$$|M \times N| = |M| \cdot |N| .$$

Exercise 1.3 *Write a program, that computes for a list $a = (a_1, ..., a_n) \in \mathbb{Z}^n$ the sum*

$$\sum_{k=1}^{n} a_k .$$

Exercise 1.4 *Prove, using induction, that*

$$\sum_{k=1}^{n} k^2 = \frac{n\,(n+1)\,(2n+1)}{6}$$

for alle $n \in \mathbb{N}$.

Exercise 1.5 *Find a formula for*

$$\sum_{k=1}^{n} (2k-1)$$

and prove your claim using induction.

Exercise 1.6 *Find a formula for*

$$\sum_{k=1}^{n} k^3$$

and prove your claim using induction.

Exercise 1.7 *Show, using induction, that for $q \in \mathbb{R}$, $q \neq 1$ we have*

$$\sum_{k=0}^{n} q^k = \frac{1 - q^{n+1}}{1 - q}$$

Exercise 1.8 *Implement a function, which enumerates recursively all subsets of $\{1, ..., n\}$.*

Exercise 1.9 *Let $0 \leq k \leq n$. Prove that for the number $\binom{n}{k}$ of k-element subsets of an n-element set we have*

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}$$

with $n! = 1 \cdot 2 \cdot ... \cdot n$.

Exercise 1.10 *The game "Towers of Hanoi" consists out of 3 fields, on which n discs with pairwise different radius can be stacked (see Figure 1.11). At the start of the game all discs are stacked on one field, sorted by increasing size, thus forming a tower. The goal of the game is to move the original stack to a different field. To do so, in every move of the game, one can shift the top disc on an arbitrary tower to any other tower, provided this tower does not contain a smaller disc.*

Describe an algorithm, which solves the game, find a formula for the required number of moves, and prove this formula using induction.

Exercise 1.11 *Write a recursive program, which solve the game "Towers of Hanoi".*

Exercise 1.12 *In an american city map with n avenues and m streets (see Figure 1.12) we want to move from point A to point B. How many shortest paths are there?*

Prove your formula using induction on $n + m$.

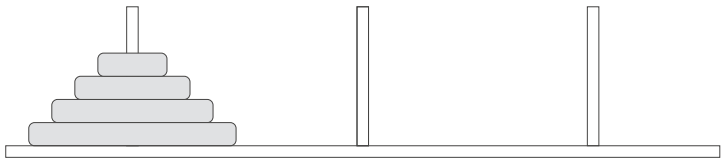


Figure 1.11: Towers of Hanoi

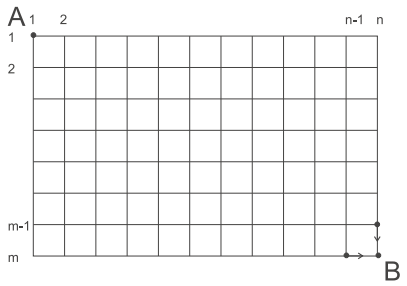


Figure 1.12: How many shortest paths are there from A to B.

Exercise 1.13 *Give an example for a map $\mathbb{N} \to \mathbb{N}$, which is*

1) injective but not surjective,

2) surjective but not injective.

Exercise 1.14 *At a party n persons meet. Prove that two of them know the same number of persons at the party.*

Exercise 1.15 *The composition of maps is associative, that is, for maps*

$$M \xrightarrow{f} N \xrightarrow{g} L \xrightarrow{h} K$$

we have

$$h \circ (g \circ f) = (h \circ g) \circ f.$$

Exercise 1.16 *Let $f : M \to N$ be a map. Prove:*

1) f is injective if and only if there is a map $g : f(M) \to M$ with $g \circ f = \mathrm{id}_M$.

2) f is surjective if and only if there is a map $g : N \to M$ with $f \circ g = \mathrm{id}_N$.

3) *f ist bijective if and only if there is a map $g : N \to M$ with $g \circ f = \mathrm{id}_M$ and $f \circ g = \mathrm{id}_N$.*

Moreover, $g = f^{-1}$ is the inverse map.

Exercise 1.17 *Let M, N be finite sets with $|M| = |N|$ and $f : M \to N$ a map. Prove that the following are equivalent:*

1) *f is bijective,*

2) *f is injective,*

3) *f is surjective.*

Exercise 1.18 *Suppose the numbers $1, ..., 101$ are given in any order. Prove that 11 of them (not necessarily consecutive) are in an increasing or decreasing order.*

Hint: Consider a suitable set of paris and use the pigeon hole principle.

Exercise 1.19 *Let $n \in \mathbb{N}$ and suppose there are $n^2 + 1$ points given in the square*

$$\{(x, y) \mid 0 \le x < n,\ 0 \le y < n\} \subset \mathbb{R}^2.$$

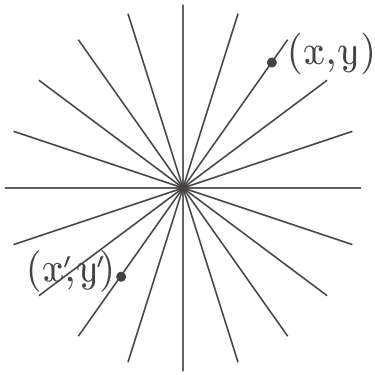
Show that among these points there are two which have distance $\le \sqrt{2}$.

Exercise 1.20 *Let M be an **infinite** set. Prove:*

1) *There is no surjective map $\varphi : M \to 2^M$.*
2) *There is no injective map $\psi : 2^M \to M$.*

Exercise 1.21 *Let $M := \mathbb{R}^2 \setminus \{(0, 0)\}$ be the set of points in the real plane without the 0-point. On M define $(x, y) \sim (x', y')$ if*

and only if there is a line through $(0,0) \in \mathbb{R}^2$ *which contains both the point* (x,y) *and the point* (x',y').



1) *Prove that* $\sim$ *is an equivalence relation.*

2) *Find a geometric representation of* $M/\sim$ *by assigning to any equivalence class a suitable representative.*

2

Numbers

In this section, as a start into algebra, we discuss the key properties of numbers. All these properties serve as role models for more general classes of rings.

2.1 The integers and division with remainder

On the natural numbers $\mathbb{N}_0 = \{0, 1, 2, 3, ...\}$ there are operations $+$ and $\cdot$, which obey the associative laws

$$a + (b + c) = (a + b) + c$$
$$a \cdot (b \cdot c) = (a \cdot b) \cdot c$$

the commutative laws

$$a + b = b + a$$
$$a \cdot b = b \cdot a$$

and the distributive law

$$a \cdot (b + c) = a \cdot b + a \cdot c$$

for alle $a, b, c \in \mathbb{N}_0$. We will not discuss the axiomatic definition of the natural numbers, but we remark that their key property is that for any number there is a number which is larger by one. As an exercise read up in a book or seach engine of your choice about the Peano axioms.

In $\mathbb{N}_0$ there is no number a with

$$1 + a = 0.$$

In practice this means: We can describe assets on an account, but no debt.

From the natural numbers, one constructs the integers $\mathbb{Z} = \{0, 1, -1, 2, -2, ...\}$ as follows:

Remark 2.1.1 *The basic idea of the construction is: The net worth of a bank account one can write as the difference of assets and depts. Different tuples of* (*assets, debt*) *lead to the same net worth of the account, for example,*

$$5 - 1 = 1000006 - 1000002$$

that is, the net worth of an account with $5 €$ *assets and* $1 €$ *debt is the same as that of one with* $1000006 €$ *assets and* $1000002 €$ *debt. The represent the net worth, we have to consider equivalence classes with respect to an appropriate equivalence relation. The account in the example have the same net worth, since*

$$5 + 1000002 = 1000006 + 1.$$

One hence defines

$$\mathbb{Z} := (\mathbb{N}_0 \times \mathbb{N}_0) / \sim$$

with the equivalence relation

$$(a, b) \sim (c, d) \Leftrightarrow a + d = b + c,$$

and considers the equivalence classes

$$[(a, b)] = \{(c, d) \mid (c, d) \sim (a, b)\}.$$

We think of $[(a, b)]$ *as the integer* $a - b$. *This motivates the following (well defined) operations* $+$ *and* $\cdot$ *on* $\mathbb{Z}$

$$\begin{aligned} [(a, b)] + [(c, d)] &:= [(a + c, b + d)] \\ [(a, b)] \cdot [(c, d)] &:= [(a \cdot c + b \cdot d, a \cdot d + b \cdot c)], \end{aligned}$$

which obey the associative, commutative and distributive laws (see also Exercise 2.2). We then have

$$[(a,b)] + [(b,a)] = [(0,0)]$$

for all $[(a,b)] \in \mathbb{Z}$*, in particular,*

$$[(1,0)] + [(0,1)] = [(0,0)]\,.$$

Moreover

$$[(0,0)] + [(a,b)] = [(a,b)]$$
$$[(1,0)] \cdot [(a,b)] = [(a,b)]\,.$$

A set with such operations is called a commutative ring with 1*. The integers are sorted by the total ordering* $\leq$*.*

Every account $[(a,b)]$ *is equivalent to a unique account with either no assets or no debt: For* $a \geq b$ *let* $c \in \mathbb{N}_0$ *with* $a = b + c$*. Then* $(a,b) \sim (c,0)$*. For* $a < b$ *let* $c \in \mathbb{N}$ *with* $b = a + c$*. Then* $(a,b) \sim (0,c)$*. We write short*

$$c := [(c,0)]$$

and

$$-c := [(0,c)]\,.$$

We then have

$$c + (-c) = 0$$

for all $c \in \mathbb{Z}\backslash\{0\}$*, since* $c + (-c) = [(c,c)] = [(0,0)] = 0$*.*

In a similar way, one can construct $\mathbb{Q}$ *from* $\mathbb{Z}$ *as*

$$\mathbb{Q} = (\mathbb{Z} \times \mathbb{Z}\backslash\{0\}) \,/\, \sim$$

with the equivalence relation

$$(a,b) \sim (c,d) \Leftrightarrow ad = bc,$$

where we write the equivalence classes as

$$\frac{a}{b} := [(a,b)].$$

The real numbers $\mathbb{R}$ *one can again construct from* $\mathbb{Q}$ *using a suitable equivalence relation.*

In $\mathbb{Q}$ every number a can be divided by any number $b \neq 0$. In many problems of daily life and mathematics this does not make sense, since the smallest useable unit is 1. If we want to distribute 1000 passengers uniformly on 3 airplanes, then $\frac{1000}{3}$ is not a resonable solution, we rather want

$$1000 = 3 \cdot 333 + 1,$$

so one person has to stay behind (or one of the airplanes will have to take the extra passenger). This process is called division with remainder (then 1 left-over passenger is the remainder):

Lemma 2.1.2 (Division with remainder) *Given $a, b \in \mathbb{Z}$, $b \neq 0$, there are uniquely defined $q, r \in \mathbb{Z}$ with*

$$a = b \cdot q + r$$

and $0 \leq r < |b|$.

Example 2.1.3 *In the above example, $a = 1000$ and $b = 3$, and we have*

$$1000 = 3 \cdot 333 + 1,$$

that is, $q = 333$ and $r = 1$.

We prove Lemma 2.1.2:

Proof. Existence: Without loss of generality $b > 0$. The set

$$\{w \in \mathbb{Z} \mid b \cdot w > a\} \neq \varnothing$$

has a smallest element w. We set

$$q := w - 1 \qquad r := a - qb.$$

Obviously $a = qb + r$, moreover $qb + b > a$, hence,

$$r < b$$

and, since w was chosen minimal, also $bq \leq a$, hence,

$$r \geq 0.$$

Uniqueness: If we have two representations

$$b \cdot q_1 + r_1 = a = b \cdot q_2 + r_2$$

and without loss of generality $r_2 \leq r_1$, then

$$0 \leq \underbrace{r_1 - r_2}_{b \cdot (q_2 - q_1)} < |b| ,$$

hence, $q_1 = q_2$ and $r_1 = r_2$. ■

The proof gives an explicit (but very inefficient) algorithm for division with remainder (scan through the w, starting with a random number, decreasing w iteratively by 1 if $b \cdot w > a$, and increasing w iteratively by 1 if $b \cdot w < a$ until the respective condition is not satisfied any more). In practice, one rather proceeds as follows:

Remark 2.1.4 *School book division without digits after the decimal point iteratively determines q (starting with the largest digit), thus yielding an algorithm for division with remainder.*

Example 2.1.5 *For $a = 2225$ and $b = 7$ write*

$$\begin{array}{rl} 2225 & = 7 \cdot 317 + 6 \\ -21 & \\ \hline 12 & \\ -7 & \\ \hline 55 & \\ -49 & \\ \hline 6 & \end{array}$$

hence $q = 317$ and $r = 6$.

Using division with remainder, we can algorithmically decide divisibility.

Definition 2.1.6 *Let $a, b \in \mathbb{Z}$. We say that b **divides** a*

$$b \mid a$$

if there is a $q \in \mathbb{Z}$ with $a = b \cdot q$. This means the division of a by b yields remainder $r = 0$.

Two numbers $a, b \in \mathbb{Z}$ are called ***coprime****, if for any $t \in \mathbb{N}$ with $t \mid a$ and $t \mid b$ it follows that $t = 1$.*

Let $m \in \mathbb{N}$ and $a, b \in \mathbb{Z}$. Then a is ***congruent*** *to b modulo m*

$$a \equiv b \bmod m$$

if $m \mid (a - b)$.

Example 2.1.7 $1 \equiv 7 \bmod 3$.

Being congruent modulo m is an equivalence relation, see Exercise 2.3. There we will also implement a function, which decides congruence modulo m using division with remainder.

For fixed m we write the equivalence class (called **residue class**) of a as

$$\begin{aligned} \overline{a} &= \{b \in \mathbb{Z} \mid a \equiv b \bmod m\} \\ &= \{a + k \cdot m \mid k \in \mathbb{Z}\}. \end{aligned}$$

Hence, $a \equiv b \bmod m$ if and only if $\overline{a} = \overline{b}$.

Example 2.1.8 *Congruence modulo 3 partitions $\mathbb{Z}$ in 3 residue classes*

$$\begin{aligned} \overline{0} &= \{..., -3, 0, 3, 6, ...\} \\ \overline{1} &= \{..., -2, 1, 4, 7, ...\} \\ \overline{2} &= \{..., -1, 2, 5, 8, ...\}, \end{aligned}$$

since division with remainder by 3 can give the remainders $0, 1$ and 2.

Residue classes play an important role in many public-key crypto systems.

2.2 Fundamental theorem of arithmetic

Definition 2.2.1 *An element $p \in \mathbb{N}$, $p \geq 2$ is called a* ***prime number****, if $p = a \cdot b$, $a, b \in \mathbb{N}$ implies $a = 1$ or $b = 1$.*

Example 2.2.2 $2, 3, 5, 7, 11, 13, 17, 19, 23...$

How to find all prime numbers up to a given bound will be discussed in the next section.

Theorem 2.2.3 (Fundamental theorem of arithmetic) *Every number $n \in \mathbb{Z}\backslash\{0,-1,1\}$ has a unique representation*

$$n = \pm\, p_1^{r_1} \cdot \ldots \cdot p_s^{r_s}$$

with prime numbers $p_1 < \ldots < p_s$ and $r_i \in \mathbb{N}$. The p_i are called the ***prime factors*** *of n.*

Proof. Existence of prime factorization using induction on n:

$n = 2$ is a prime number. If $n > 2$ and not prime, then $n = a \cdot b$ with $a, b \neq 1$. Since $a, b < n$, both a and b by the induction hypothesis have factorizations, and by sorting by the prime factors we obtain a prime factorization of $n = a \cdot b$.

Proof of uniqueness, using induction on n:

For $n = 2$, then n is prime, and the claim is clear. Suppose $n > 2$ and

$$n = p_1 \cdot \ldots \cdot p_s = q_1 \cdot \ldots \cdot q_t$$

with $p_1 \leq \ldots \leq p_s$ and $q_1 \leq \ldots \leq q_t$. If $s = 1$ or $t = 1$, then again n is prime, and the claim is clear. So suppose now that $s, t \geq 2$.

If $p_1 = q_1$ then

$$p_2 \cdot \ldots \cdot p_s = q_2 \cdot \ldots \cdot q_t < n$$

has, by the induction hypothesis, a unique prime factorization and die claim follows.

Assume now that $p_1 < q_1$. Then

$$n > \underbrace{p_1 \cdot (p_2 \cdot \ldots \cdot p_s - q_2 \cdot \ldots \cdot q_t)}_{=:N_1} = \underbrace{(q_1 - p_1) \cdot q_2 \cdot \ldots \cdot q_t}_{=:N_2} \geq 2,$$

so $N_1 = N_2$, by the induction hypothesis, has a unique prime factorization. Since $p_1 < q_1 \leq \ldots \leq q_t$ we have $p_1 \neq q_i$ for $i \geq 1$. Moreover, p_1 is not a divisor of $q_1 - p_1$, since otherwiese p_1 would divide the prime q_1. Hence p_1 is a prime factor of N_1, but not one of N_2, a contradiction. ■

Example 2.2.4 $24 = 2^3 \cdot 3$.

In MAPLE *we can compute a prime factorization by:*

```
ifactor(24);
```

$(2)^3(3)$

The proof of the fundamental theorem only shows the existence of a (unique) prime factorization. We will come back to the question, how to compute such a factorization.

From the fundamental theorem we conclude:

Corollary 2.2.5 (Euklid's first theorem) *If $p \in \mathbb{Z}$ is prime and $a, b \in \mathbb{Z}$ with $p \mid ab$, then $p \mid a$ or $p \mid b$.*

Proof. The prime factorization of ab is obtained by combining the factorizations of a and b. ■

Corollary 2.2.6 (Euklid's second theorem) *There are infinitely many prime numbers.*

Proof. Let $M = \{p_1, ..., p_r\}$ be a finite set of prime numbers. We show, that there is a prime number, which is not in M. The number $N = p_1 \cdot ... \cdot p_r + 1$ is not divisible by any of the primes p_i, since otherwise also 1 would be divisible by p_i. Hence, there is a prime factor p of N, which is not in M. ■

Without proof we mention the following theorem on the density of the prime numbers:

Theorem 2.2.7 (Prime number theorem) *Setting*

$$\pi(x) = \left|\{p \leq x \mid p \in \mathbb{N} \text{ prime}\}\right|.$$

for $x \in \mathbb{R}_{>0}$, we have

$$\lim_{x \to \infty} \frac{\pi(x)}{\frac{x}{\ln(x)}} = 1.$$

Example 2.2.8 *The following program (in the syntax of* MAPLE*) computes $\pi(x)$:*

```
pi:=proc(x)
local p,N;
p:=2;
N:=0:
while p<=x do
    p:=nextprime(p);
    N:=N+1;
od;
return(N);
end proc:
```

We obtain, for example,

```
pi(100000);
```

9592

So about 10% *of the numbers* ≤ 100000 *are prime numbers.*

See also Exercise 2.5.

2.3 Greatest common divisor and Euclidean algorithm

Definition 2.3.1 *If* $a_1, ..., a_t \in \mathbb{Z}$*, then* $d \in \mathbb{N}$ *is called* ***greatest common divisor*** *of* $a_1, ..., a_t$*, written* $d = \gcd(a_1, ..., a_t)$*, if we have*

1) $d \mid a_j$ *for all* $j = 1, ..., t$*, that is,* d *is a divisor of all* a_j*, and*

2) *if* $\tilde{d} \in \mathbb{Z}$ *is a divisor of all* a_j*, that is* $\tilde{d} \mid a_j$ *for all* $j = 1, ..., t$*, then* $\tilde{d} \mid d$*.*

Furthermore the number $m \in \mathbb{N}$ *is called* ***least common multiple*** *of* $a_1, ..., a_t$*, written* $m = \operatorname{lcm}(a_1, ..., a_t)$*, if we have*

1) $a_j \mid m$ *for all* $j = 1, ..., t$*, that is,* m *is a multiple of all* a_j*, and*

2) *if* $\tilde{m} \in \mathbb{Z}$ *is a multiple of all* a_j*, that is,* $a_j \mid \tilde{m}$ *for all* $j = 1, ..., t$*, then* $m \mid \tilde{m}$*.*

Example 2.3.2 *The common divisors of* $18 = 2 \cdot 3^2$ *and* $66 = 2 \cdot 3 \cdot 11$ *are* $1, 2, 3$ *and* 6*, hence*

$$\gcd(18, 66) = 6.$$

Remark 2.3.3 *If we write*

$$a_j = \pm 1 \cdot \prod_{i=1}^{s} p_i^{r_{ji}}$$

with p_i *prime and* $r_{ji} \geq 0$*, then*

$$\gcd(a_1, ..., a_t) = \prod_{i=1}^{s} p_i^{\min\{r_{ji} | j\}} \tag{2.1}$$

(and for lcm *the corresponding formula replacing the minimum with the maximum holds true). Using these formulas, we get:*

1) Two numbers $a, b \in \mathbb{Z}$ are coprime if and only if

$$\gcd(a, b) = 1.$$

2) For $a, b \in \mathbb{N}$,

$$\gcd(a, b) \cdot \operatorname{lcm}(a, b) = a \cdot b.$$

Example 2.3.4 *For $18 = 2 \cdot 3^2$ and $66 = 2 \cdot 3 \cdot 11$ we have*

$$\gcd(18, 66) = 6.$$

A much more efficient way for determining the greatest common divisor (and thus also the least common multiple) is provided by the Euclidean algorithm:

Theorem 2.3.5 (Euclidean algorithm) *Let $a_1, a_2 \in \mathbb{Z}\backslash\{0\}$. Then the successive division with remainder*

$$\begin{aligned} a_1 &= q_1 a_2 + a_3 \\ &\vdots \\ a_j &= q_j a_{j+1} + a_{j+2} \\ &\vdots \\ a_{n-2} &= q_{n-2} a_{n-1} + a_n \\ a_{n-1} &= q_{n-1} a_n + 0 \end{aligned}$$

terminates with remainder zero, and

$$\gcd(a_1, a_2) = a_n.$$

Backsubstiution of these equalities

$$\begin{aligned} a_n &= a_{n-2} - q_{n-2} a_{n-1} \\ &\vdots \\ a_3 &= a_1 - q_1 a_2 \end{aligned}$$

yields a representation of the greatest common divisor as

$$\gcd(a_1, a_2) = u \cdot a_1 + v \cdot a_2$$

with $u, v \in \mathbb{Z}$. Computing this representation is referred to as the ***extended Euclidean algorithm****.*

Proof. We have $|a_{i+1}| < |a_i|$ for all $i \geq 2$, hence, after finitely many iterations, $a_i = 0$. Then a_n is a divisor of a_{n-1}, hence also of $a_{n-2} = q_{n-2}a_{n-1} + a_n$ and inductively of $a_{n-1}, ..., a_1$. If t is an arbitrary divisor of a_1 and a_2, then also of $a_3 = a_1 - q_1 a_2$ and inductively of $a_1, ..., a_n$. ■

Example 2.3.6 *We compute the gcd of* 66 *and* 18 *using the Euclidean algorithm, that is, by successive division with remainder:*

$$66 = 3 \cdot 18 + 12$$
$$18 = 1 \cdot 12 + 6$$
$$12 = 2 \cdot 6 + 0$$

Hence $\gcd(66, 18) = 6$, *since reading the equaltities backwards, we have*

$$6 \mid 12 \text{ hence } 6 \mid 18 \text{ hence } 6 \mid 66$$

and reading them top-to-bottom, if t *is a divisor of* 66 *and* 18, *then*

$$t \mid 12 \text{ hence } t \mid 6.$$

Moreover, we obtain a representation of $\gcd(36, 15)$ *as a* $\mathbb{Z}$*-linear combination of* 66 *and* 18

$$6 = 18 - 1 \cdot 12 = 18 - 1 \cdot (66 - 3 \cdot 18) = 4 \cdot 18 + (-1) \cdot 66.$$

In MAPLE *we can execute the extended Euclidean algorithm by:*

```
igcdex(66,18,'u','v');
6
```

Here the command stores in x *and* y *the coefficients in the representation of the ggT as a linear combintation:*

```
u;
-1
v;
4
u*66+v*18;
6
```

Note that u *and* v *are not unique. We could also choose, for example,* $u = -19$ *and* $v = 70$.

One key applicaiton of the representation of 1 as a $\mathbb{Z}$-linear combination of two coprime numbers is solving of simultaneous congruences. This will be addressed in the next section on the Chinese remainder theorem.

2.4 The Chinese remainder theorem

Theorem 2.4.1 (Chinese remainder theorem in $\mathbb{Z}$) *If $n_1, ..., n_r \in \mathbb{N}$ are pairwise coprime and $a_1, ..., a_r \in \mathbb{Z}$, then the* ***simultaneous congruences***

$$\begin{aligned} x &\equiv a_1 \bmod n_1 \\ &\vdots \\ x &\equiv a_r \bmod n_r \end{aligned}$$

have a solution. The solution is unique up to multiples of $n = n_1 \cdot ... \cdot n_r$.

Proof. Set

$$\hat{n}_i = \frac{n}{n_i}$$

and find, using the extended Euclidean algorithm, $x_i, y_i \in \mathbb{Z}$ with

$$1 = \gcd(n_i, \hat{n}_i) = x_i n_i + y_i \hat{n}_i.$$

Then

$$\begin{aligned} y_i \hat{n}_i &\equiv 0 \bmod n_j \ \forall j \neq i \\ y_i \hat{n}_i &\equiv 1 \bmod n_i. \end{aligned}$$

hence,

$$z = \sum_{i=1}^{r} a_i y_i \hat{n}_i$$

satisfies the congruences, similarly all $z + k \cdot n$ with $k \in \mathbb{Z}$ do. If x and x' are solutions, then $n_i \mid (x - x')$ for all i. Hence, also $\operatorname{lcm}(n_1, ..., n_r) \mid (x - x')$. Since the n_i are pairwise coprime, $\operatorname{lcm}(n_1, ..., n_r) = n_1 \cdot ... \cdot n_r$, that is,

$$n \mid (x - x').$$

■

The Chinese remainder theorem allows us, to replace an arbitrary number of congruences by a single congruence. We can also iteratively combine pairs of two congruences into one. We hence formulate the solution algorithm in the special case $r = 2$:

Remark 2.4.2 *Given coprime numbers $n_1, n_2 \in \mathbb{N}$ and $a_1, a_2 \in \mathbb{Z}$, we find a solution of the simultaneous congruences*

$$x \equiv a_1 \bmod n_1$$
$$x \equiv a_2 \bmod n_2$$

The extended Euclidean algorithm finds $u, v \in \mathbb{Z}$ with

$$1 = \gcd(n_1, n_2) = u \cdot n_1 + v \cdot n_2$$

Since

$$un_1 \equiv 0 \bmod n_1$$
$$un_1 \equiv 1 \bmod n_2$$
$$vn_2 \equiv 1 \bmod n_1$$
$$vn_2 \equiv 0 \bmod n_2$$

for

$$z := a_2 \cdot u \cdot n_1 + a_1 \cdot v \cdot n_2$$

we have

$$z \equiv a_1 \bmod n_1$$
$$z \equiv a_2 \bmod n_2$$

If x another solution, then $n_i \mid (x - z)$ for $i = 1, 2$, and hence $n_1 n_2 \mid (x - z)$.

So we obtain

$$\left.\begin{array}{l} x \equiv a_1 \bmod n_1 \\ x \equiv a_2 \bmod n_2 \end{array}\right\} \Longleftrightarrow x \equiv z \bmod n_1 n_2$$

If we apply this method iteratively, we get another proof of Theorem 2.4.1.

We note that the Chinese remainder theorem can be formulated in a much more general setting.

Example 2.4.3 *We solve the simultaneous congruences*

$$x \equiv -28 \bmod 30$$
$$x \equiv 5 \bmod 7.$$

Since $\gcd(30,7) = 1$*, it follows there is a solution. With the extended Euclidean algorithm, we find* u *and* v *with*

$$u \cdot 30 + v \cdot 7 = 1,$$

for example, $u = -3$*,* $v = 13$*. Then we have*

$$\begin{aligned}(-3) \cdot 30 &\equiv 0 \bmod 30\\ (-3) \cdot 30 &\equiv 1 \bmod 7\\ 13 \cdot 7 &\equiv 1 \bmod 30\\ 13 \cdot 7 &\equiv 0 \bmod 7\end{aligned}$$

hence

$$z = (-28) \cdot (13 \cdot 7) + 5 \cdot (-3 \cdot 30) = -2998$$

is a solution (which is unique modulo 210*). The Chinese remainder theorem thus replaces the two congruences by a single one:*

$$\left.\begin{aligned}x &\equiv -28 \bmod 30\\ x &\equiv 5 \bmod 7\end{aligned}\right\} \Leftrightarrow x \equiv -2998 \equiv 152 \bmod 210.$$

For the single congruence, it is easy to write down the solution set

$$152 + 210 \cdot \mathbb{Z} = \{152 + k \cdot 210 \mid k \in \mathbb{Z}\},$$

which indeed is the residue class $\overline{152}$*.*

If the moduli n_i are not coprime, we can find a similar solution formula, however, simultaneous congruences may not be solveable. The following theorem gives a criterion:

Theorem 2.4.4 *Let* $a_1, a_2 \in \mathbb{Z}$ *and* $n_1, n_2 \in \mathbb{N}$*. Then the simultaneous congruences*

$$\begin{aligned}x &\equiv a_1 \bmod n_1\\ x &\equiv a_2 \bmod n_2\end{aligned}$$

are solveable if and only if

$$a_1 - a_2 \equiv 0 \bmod \gcd(n_1, n_2).$$

The solutions are unique up to the addition of multiples of $\operatorname{lcm}(n_1, n_2)$*.*

The proof is Exercise 2.12, where we also describe a method to find the solutions.

2.5 Prime factorization

There is a very straight-forward method to prime factorization: trial division Although there are much more powerful algorithms, for rather small numbers up to 10^6 trial division is the best choice.

Algorithm 2.5.1 (Trial division) *Let $n \in \mathbb{N}$ be composite (that is, not prime). The smallest prime divisor p of n satisfies*

$$p \leq m := \left\lfloor \sqrt{n} \right\rfloor .$$

If we know all prime numbers $p \leq m$, then we test $p \mid n$ using division with remainder. In this way, we can factorize n.

Proof. Write $n = p \cdot q$. Then $p^2 \leq p \cdot q = n$, hence $p \leq \sqrt{n}$. Since $p \in \mathbb{N}$, it follows that $p \leq \left\lfloor \sqrt{n} \right\rfloor$. ∎

Example 2.5.2 *In order to factorize 234 via trial division, we first test, whether n is divisible by a prime number $p \leq \left\lfloor \sqrt{234} \right\rfloor = 15$. We find*

$$234 = 2 \cdot 117.$$

If 117 is not prime, then it must have a prime divisor $p \leq \left\lfloor \sqrt{117} \right\rfloor = 10$. We find that

$$117 = 3 \cdot 39.$$

If 39 is not prime, then it must have a prime divisor $p \leq \left\lfloor \sqrt{39} \right\rfloor = 6$. We find that

$$39 = 3 \cdot 13.$$

Finally we observe that 13 is prime, since 13 is not divisible by any prime number $p \leq \left\lfloor \sqrt{13} \right\rfloor = 3$.

Trial division allows us to enumerate all prime numbers $\leq n$ in an inductive way: If we know all prime numbers $p \leq \left\lfloor \sqrt{n} \right\rfloor < n$, then we can decide whether n is prime.

Example 2.5.3 *We enumerate all prime numbers* ≤ 11. *Since for the smallest prime divisor of* n *we have* $p \leq m$, *wa can conlude that*

n	m		
2	1		$\Rightarrow 2$ *prime*
3	1		$\Rightarrow 3$ *prime*
4	2	$4 = 2 \cdot 2$	$\Rightarrow 4$ *not prime*
5	2	$2 \nmid 5$	$\Rightarrow 5$ *prime*
6	2	$6 = 2 \cdot 3$	$\Rightarrow 6$ *not prime*
7	2	$2 \nmid 7$	$\Rightarrow 7$ *prime*
8	2	$8 = 2 \cdot 4$	$\Rightarrow 8$ *not prime*
9	3	$9 = 3 \cdot 3$	$\Rightarrow 9$ *not prime*
10	3	$10 = 2 \cdot 5$	$\Rightarrow 10$ *not prime*
11	3	$2 \nmid 11$ *and* $3 \nmid 11$	$\Rightarrow 11$ *prime*

Practically one proceeds the opposite way, and rules out multiples of prime numbers, which already have been conputed.:

Algorithm 2.5.4 (Sieve of Eratosthenes) *We obtain a list of all primes up to* $N \in \mathbb{N}$, $N \geq 4$ *as follows:*

1) *Make a boolean list* L *with one entry for every number* $2, ..., N$. *Mark all numbers as prime (true). Set* $p = 2$.

2) *Mark all* $j \cdot p$ *with* $j \geq p$ *as not prime (false).*

3) *Find the smallest* $q > p$, *which ist marked as prime (true). If* $q > \sqrt{N}$ *return* L. *Set* $p := q$, *goto* (2).

Proof. In step (2) all $j \cdot p$ with $2 \leq j < p$ are already marked as $false$ from previous steps, since they have a prime divisor $< p$. Hence all true multiples of p are marked as $false$. The number q in step (3) is always prime, since p is the largest prime number $< q$, and hence from previous steps all multiples $j \cdot x$ of all prime numbers $x < q$ are marked as $false$. Once the algorithm terminates, all numbers are marked as $false$, which have a prime number $p \leq \sqrt{N}$ as a true divisor, that is which are not prime. ■

Example 2.5.5 *We find all primes* ≤ 15 *and give in ever iteration the list of all* j *with* $L_j = true$*:*

	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$p=2$	2	3		5		7		9		11		13		15
$p=3$	2	3		5		7				11		13		

In the first iteration, we delete all multiples of 2*, in the second iteration all multiples of* 3*. All remaining numbers are prime, since* $p = 5 > \sqrt{15}$*.*

For large numbers, there are much more efficient ways than trial division to find a prime divisor of a given number.

2.6 Exercises

Exercise 2.1 *Let* $n \in \mathbb{N}$ *and* $M \subset \{1, \dots, 2n\}$ *a set of integers with* $|M| = n+1$ *elements. Show that in* M *there are two different integers such that the one divides the other.*

Exercise 2.2 *Show:*

1) On $M = \mathbb{N}_0 \times \mathbb{N}_0$ *by*

$$(a,b) \sim (c,d) \Leftrightarrow a + d = b + c$$

we can define an equivalence relation.

2) The operations addition and multiplication

$$[(a,b)] + [(c,d)] = [(a+c, b+d)]$$
$$[(a,b)] \cdot [(c,d)] = [(a \cdot c + b \cdot d, a \cdot d + b \cdot c)]$$

on

$$\mathbb{Z} = (\mathbb{N}_0 \times \mathbb{N}_0) \,/\, \sim$$

are well-defined, associative, commutative and distributiv.

More generally, these properties play an important role in the context of groups and rings.

Exercise 2.3 *1) Let $m \in \mathbb{N}$ and $a, b \in \mathbb{Z}$. Then we say that a is congruent to b modulo m*

$$a \equiv b \bmod m$$

if $m \mid (a-b)$. Prove that "being congruent modulo m" is an equivalence relation.

2) Write a function, which decides $a \equiv b \bmod m$.

Exercise 2.4 *Show:*

1) If $r \in \mathbb{N}$ and $p = 2^r - 1$ is prime, then r is prime.

2) If $r \in \mathbb{N}$ and $p = 2^r + 1$ is prime, then $r = 2^k$ with $k \in \mathbb{N}_0$.

Exercise 2.5 *Test the prime number theorem experimentally in* MAPLE*:*

1) Write a procedure, which computes

$$\pi(x) = |\{p \leq x \mid p \in \mathbb{N} \text{ prime}\}|$$

for $x > 0$.

2) Compare the function $\frac{\pi(x)}{x}$ with $\frac{1}{\ln(x)-a}$ for $a \in \mathbb{Z}_{\geq 0}$, in particular for large x. For which a do you get the best approximation?

3) Visualize your observations using MAPLE*.*

Hint: Use the MAPLE*-function* nextprime*.*

Exercise 2.6 *Let P_N be the probability, that two randomly chose natural numbers $n, m \leq N$ are coprime. Determine P_N for $N = 10^6, 10^{12}$ and 10^{18} approximatively by samples of 10^2, 10^4 and 10^6 generated with a computer algebra system. Check experimentally, that P_N for large values of N takes the value*

$$\frac{6}{\pi^2} \approx 60.7\%.$$

Exercise 2.7 *Implement the extended Euclidean algorithm. Test your implementation at examples.*

Exercise 2.8 *Reduce*

$$\frac{90297278063}{18261358091}$$

to smallest terms.

Exercise 2.9 *Into an originally empty accout there regularily get paid in* $2809\,€$*, and occasionally there get drawn* $10403\,€$ *from the account. Is it possible that the account at some point has the balance of* $1\,€$*?*

Exercise 2.10 *Implement*

1) *the sieve of Erathosthenes.*
2) *the factorization of integers via trial division.*
3) *Find the prime factorization of*

$$116338867864982351.$$

Exercise 2.11 *Find the set* $L \subset \mathbb{Z}$ *of all solutions* x *of the simultaneous congruences*

$$\begin{aligned} x &\equiv 2 \bmod 3 \\ x &\equiv 2 \bmod 7 \\ x &\equiv 3 \bmod 10 \end{aligned}$$

Exercise 2.12 *Let* $a_1, a_2 \in \mathbb{Z}$ *and* $n_1, n_2 \in \mathbb{Z}_{>0}$*. Show that the simultaneous congruences*

$$\begin{aligned} x &\equiv a_1 \bmod n_1 \\ x &\equiv a_2 \bmod n_2 \end{aligned}$$

are solveable if and only if

$$a_1 - a_2 \equiv 0 \bmod \gcd(n_1, n_2).$$

Show that the solution is unique modulo $\operatorname{lcm}(n_1, n_2)$*.*

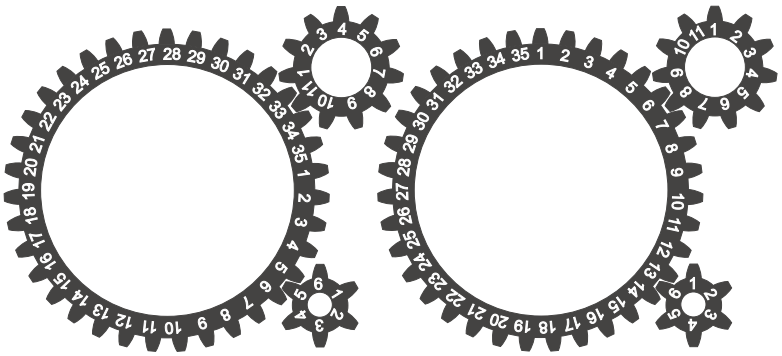


Figure 2.1: Two configurations of gearwheels.

Exercise 2.13 *Is it possible for the two configurations of gearwheels in Figure 2.1 to transform the one into the other by rotation? If possible, by how many ticks we have to turn?*

Exercise 2.14 *Find the set $L \subset \mathbb{Z}$ of all solutions x of the simultaneous congruences*

$$x \equiv 1 \bmod 108$$
$$x \equiv 25 \bmod 80$$

Exercise 2.15 *Using your implementation of the extended Euclidean algorithm (or any other available implementation like the* MAPLE*-function* igcdex*) write a procedure, which determines the solution set of the simultaneous congruences*

$$x \equiv a_1 \bmod n_1$$
$$x \equiv a_2 \bmod n_2$$

for given $a_1, a_2 \in \mathbb{Z}$ and $n_1, n_2 \in \mathbb{Z}_{>0}$ with $\gcd(n_1, n_2) = 1$. Compare with the MAPLE*-function* chrem*.*

Extend your implementation such that it works correctly also for n_1, n_2 not coprime.

3

Groups

3.1 Overview

In this chapter we discuss the foundations of group theory, which will have various applications in the chapters of rings, fields and vector spaces. As and example for groups we consider symmetry groups of subsets of $\mathbb{R}^n$, for example, the sets of rotations and (roto-) reflections, which map a Platonic solid (tetrahedron, cube, octahedron, dodecahedron and icosahedron) to itself (see Figure 3.1).The group property arises here from the fact, that the composition of two symmetries is again a symmetry and any symmetry can be undone by a symmetry. For example in the symmetry group of the tetrahedron the 120° rotation is equal to the composition of two reflections, see Figure 3.2.

In general, we have: The composition of two symmetries is again a symmetry. For every symmetry there is an inverse symmetry, such that the composition gives the identity map.

In the context of symmetry groups, the concept of an action of a group G on a set M plays an important role. For example, we can consider for G the symmetry group of the tetrahedron and for M the tetrahedron or the sets of vertices or edges or faces of the tetrahedron. A group action is then a map (satisfying a couple of obvious additional conditions)

$$\begin{array}{ccc} G \times M & \longrightarrow & M \\ (g, m) & \longmapsto & g \cdot m \end{array}$$

that is a group element g maps an element $m \in M$ to another

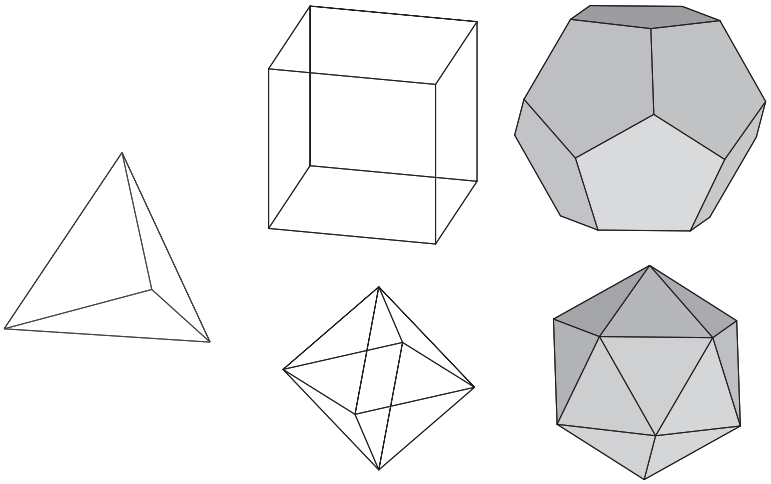


Figure 3.1: The Platonic solids

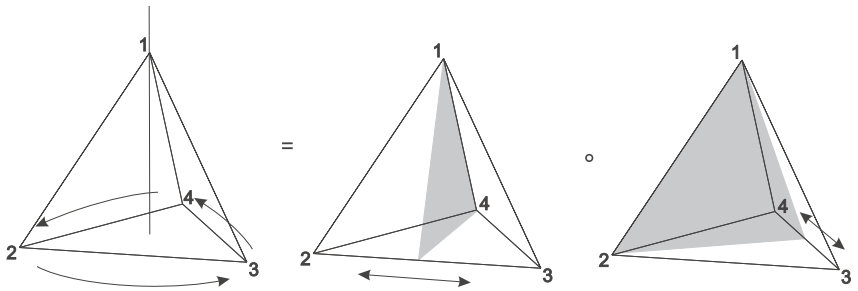


Figure 3.2: Composition of two symmetries of the tetrahedron.

element of M, which we call $g \cdot m$. If we start with some m and apply all elements of G, then we obtain the so-called orbit of m, for example, we can map any vertex of a tetrahedron to any other vertex by applying a symmetry. In general, M will decompose into disjoint orbit. One of the key theorems in this context is the orbit counting formula.

The two most important examples of operations for the construction and classification of groups is that of a subgroup $H \subset G$ by

$$\begin{array}{ccc} H \times G & \longrightarrow & G \\ (h, g) & \longmapsto & hg \end{array}$$

and of G on itself by conjugation

$$\begin{array}{ccc} G \times G & \longrightarrow & G \\ (a,b) & \longmapsto & aba^{-1} \end{array}$$

The translation we will study in detail, the conjugation will be discussed in the exercises.

3.2 Groups and actions

3.2.1 Basics

Definition 3.2.1 *A **group** $(G, \circ)$ is a set G together with a map*

$$\begin{array}{rccc} \circ : & G \times G & \longrightarrow & G \\ & (a,b) & \mapsto & a \circ b \end{array}$$

*called **operation**, which satisfies the following axioms:*

(G1) Associativity

$$a \circ (b \circ c) = (a \circ b) \circ c \ \forall a, b, c \in G$$

(G2) There exist a neutral element , that is an

$$e \in G$$

with

$$e \circ a = a \circ e = a \ \forall a \in G$$

(G3) Existence of inverses, that is $\forall a \in G \ \exists a^{-1} \in G$ with

$$a^{-1} \circ a = a \circ a^{-1} = e$$

If in addition the commutative law

$$a \circ b = b \circ a \ \forall a, b \in G,$$

*is obeyed, we call G **abelian**.*

A set G together with an operation

$$\begin{array}{rccc} \circ : & G \times G & \longrightarrow & G \end{array}$$

*which obeys $(G1)$, is called a **semigroup**.*

*$(G, \circ)$ with $(G1)$ and $(G2)$ is called a **monoid**.*

*The number of elements $|G|$ of G is called the **order** of G (which can be ∞).*

Remark 3.2.2 *If in the definition of a group G we only require the existence of a left-neutral element $e \in G$ with $e \circ a = a \ \forall a \in G$ and left-inverse elements a^{-1} for every $a \in G$ with $a^{-1} \circ a = e$, then e is also right-neutral and the elements a^{-1} right-inverses:*

1) For $a, b \in G$ we have: If $a \circ b = e$, then also $b \circ a = e$.

2) We have that $a \circ e = a$ for all $a \in G$.

Remark 3.2.3 *If G is a group then:*

1) The neutral element of G is unique.

2) The inverses of the elements of G are unique.

3) For $a, b \in G$ we have $(a \circ b)^{-1} = b^{-1} \circ a^{-1}$.

4) For $a \in G$ we have $(a^{-1})^{-1} = a$.

These statements are shown in Exercise 3.2.

Appart from the symmetry groups mentioned in Section 3.1, we discuss the following central examples of groups:

Example 3.2.4 *1) The set of integers with addition*

$$(\mathbb{Z}, +)$$

is a group. The neutral element is 0.

2) The set of integers with multiplication

$$(\mathbb{Z}, \cdot)$$

is a monoid. The neutral element is 1.

3) The set of non-zero rational numbers together with multiplication

$$(\mathbb{Q}\backslash\{0\}, \cdot)$$

is a group.

4) Let X be an arbitrary set. The set of self-mappings of X

$$S(X) = \{f : X \longrightarrow X \mid f \text{ bijective}\}$$

together with composition is a group.

In particular, for

$$X = \{1, ..., n\},$$

the set of ***permutations*** *of n elements*

$$S_n := S(\{1, ..., n\})$$

is called the ***symmetric group****. Obviously, we have that*

$$|S_n| = n \cdot (n-1) \cdot ... \cdot 2 \cdot 1 = n!$$

For $\sigma \in S_n$ we also write

$$\sigma = \begin{pmatrix} 1 & \cdots & n \\ \sigma(1) & \cdots & \sigma(n) \end{pmatrix}$$

An element of S_n is called a ***transposition****, if it interchanges two unique elements.*

Through numbering the corners of the tetrahedron in Figure 3.3 the rotation in Figure 3.3 can be identified by the permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix} \in S_4$$

and the reflexion in Figure 3.4 with the transposisiton

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \end{pmatrix} \in S_4.$$

5) Let

$$A = \{\alpha, \beta, \gamma, ...\}$$

be a finite set. A ***word*** *over the alphabet A is a finite sequence*

$$w = b_1 b_2 ... b_n$$

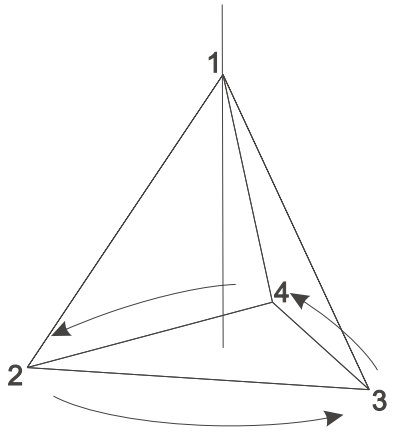


Figure 3.3: Rotational symmetry of the tetrahedron

with $b_i \in A$. Given another word $v = a_1...a_m$, we define the operation "writtenaftereachother" by

$$w \circ v = b_1...b_n a_1...a_m.$$

The set

$$G = \{w \mid w \text{ a word over } A\}$$

together with $\circ$ form a semigroup.

If we allow the empty word e in G, then $(G, \circ)$ becomes a monoid.

6) *If we add the letters $\alpha^{-1}, \beta^{-1}, ...$ with the calculation rule*

$$\alpha\alpha^{-1} = \alpha^{-1}\alpha = e,$$

then we get the free group generated by A.

7) *If G_1, G_2 are groups, then the **cartesian product** $G_1 \times G_2$ of G_1 and G_2 with the operation*

$$(a_1, b_1) \circ (a_2, b_2) := (a_1 \circ a_2, b_1 \circ b_2)$$

is again a group.

Definition and Theorem 3.2.5 (subgroup criterion) *Let $(G, \circ)$ be a group. A subset $H \subset G$ is called a **subgroup**, if the following two equivalent conditions are satisfied:*

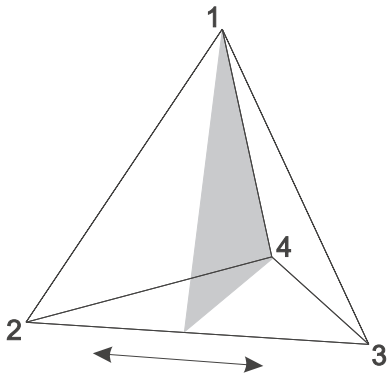


Figure 3.4: Reflection symmetry of the tetrahedron

1) $(H, \circ)$ *is a group (that is,* $e \in H$ *and* $a, b \in H \Longrightarrow a \circ b \in H$, $b^{-1} \in H$*)*

2) $H \neq \varnothing$*, and* $a, b \in H \Longrightarrow a \circ b^{-1} \in H$.

Proof. (1) ⇒ (2) is obvious. Is on the other hand $H \neq \varnothing$, then there is an $a \in H$. For this element we have $e = a \circ a^{-1} \in H$, and thus for all $a \in H$, that $a^{-1} = e \circ a^{-1} \in H$. Also for all $a, b \in H$ we have $b^{-1} \in H$, and hence

$$a \circ b = a \circ \left(b^{-1}\right)^{-1} \in H.$$

■

Example 3.2.6 *Let* G *be the symmetry group of the tetraederon,* r_{120} *the rotation in Figure 3.3 and* s_{23} *the reflection in Figure 3.4. Then*

$$\{id, r_{120}, (r_{120})^2\} \subset G$$
$$\{id, s_{23}\} \subset G$$

are subgroups.

Example 3.2.7 *The subgroups of* $(\mathbb{Z}, +)$ *are of the form*

$$n\mathbb{Z} := \{n \cdot k \mid k \in \mathbb{Z}\}$$

where $n \in \mathbb{Z}_{\geq 0}$.

Proof. Using the subgroup criterion, we see that $n\mathbb{Z} \subset \mathbb{Z}$ is.a subgroup. Suppose, on the other hand, that $H \subset \mathbb{Z}$ is a subgroup. Then either $H = \{0\}$ or there is a smallest element $n > 0$ in H. We show that then $H = n\mathbb{Z}$: Let $m \in H$. Division with remainder yields a representation of m

$$m = qn + r$$

with $0 \leq r < n$ and $r \in H$. By definition of n it follows that $r = 0$, hence $m \in n\mathbb{Z}$. ■

Example 3.2.8 *Let $n \in \mathbb{N}$ and $a \in \mathbb{Z}$. The equivalence class (residue class) of a modulo n can be expressed by using the subgroup $n\mathbb{Z} \subset \mathbb{Z}$ as*

$$\begin{aligned}\overline{a} &= \{b \in \mathbb{Z} \mid a \equiv b \bmod n\} \\ &= a + n\mathbb{Z} := \{a + b \mid b \in n\mathbb{Z}\} = \{a + k \cdot n \mid k \in \mathbb{Z}\} \subset \mathbb{Z}\end{aligned}$$

(see also Exercise 2.3).

The set of residue classes

$$\mathbb{Z}_n := \mathbb{Z}/n := \left\{\overline{0}, \overline{1}, \overline{2}, ..., \overline{n-1}\right\}$$

is together with the operation

$$\overline{a} + \overline{b} := \overline{a + b}$$

a group, the ***group of residue classes modulo n*** *(with neutral element $\overline{0}$ and inverse $-\overline{a} = \overline{-a}$ of $\overline{a} \in \mathbb{Z}/n$).*

Since $\overline{a} + \overline{b} := \overline{a + b}$ is not defined in terms of $\overline{a}$ and $\overline{b}$, but in terms of representatives a and b, we have to show that $\overline{a}+\overline{b}$ is well-defined, that is, does not depend on the choice of represenatives of a and b:

If $\overline{a_1} = \overline{a_2}$ and $\overline{b_1} = \overline{b_2}$, that is, $a_1 - a_2 = n \cdot k_1$ and $b_1 - b_2 = n \cdot k_2$ with numbers k_1, k_2, then

$$\overline{a_1} + \overline{b_1} = \overline{a_1 + b_1} = \overline{a_2 + b_2 + n \cdot (k_1 + k_2)} = \overline{a_2 + b_2} = \overline{a_2} + \overline{b_2}.$$

Example 3.2.9 *For $n = 3$ we get $\mathbb{Z}/3 = \{\overline{0}, \overline{1}, \overline{2}\}$ with*

$$\begin{aligned}\overline{0} &= \{..., -3, 0, 3, 6, ...\} = 3\mathbb{Z} \\ \overline{1} &= \{..., -2, 1, 4, 7, ...\} = 1 + 3\mathbb{Z} \\ \overline{2} &= \{..., -1, 2, 5, 8, ...\} = 2 + 3\mathbb{Z}\end{aligned}$$

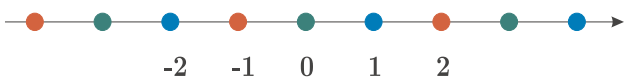


Figure 3.5: residue classes modulo 3

see also Figure 3.5.

The operation can be described in terms of the ***group table***

+	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{0}$	$\overline{1}$

for example, we see that $\overline{2}+\overline{2}=\overline{2+2}=\overline{4}=\overline{1}$.

Example 3.2.10 *For every divisor* a *of* n*, and* $d=\frac{n}{a}$ *the subset*

$$\left\{\overline{0},\overline{a},\overline{2a},...,\overline{(d-1)a}\right\}\subset\mathbb{Z}/n$$

is a subgroup (exercise).

For example, for $n=6$ *and* $a=2$ *we ge the subgroup*

$$\left\{\overline{0},\overline{2},\overline{4}\right\}\subset\mathbb{Z}/6.$$

If we compare the group table

+	$\overline{0}$	$\overline{2}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{2}$	$\overline{4}$
$\overline{2}$	$\overline{2}$	$\overline{4}$	$\overline{0}$
$\overline{4}$	$\overline{4}$	$\overline{0}$	$\overline{2}$

of this group with that of $\mathbb{Z}/3$, we observe, that the elements of the two groups have different names, but obey the same calculation rules.

The identification of the subgroup $\left\{\overline{0},\overline{2},\overline{4}\right\}\subset\mathbb{Z}/6$ with $\mathbb{Z}/3$ is an example of a group isomorphism, that is, a bijective map, which is compatible with the group structures. The group isomorphism

$$\begin{array}{rccc}\varphi: & \mathbb{Z}/3 & \longrightarrow & \left\{\overline{0},\overline{2},\overline{4}\right\}\\ & 0+3\mathbb{Z} & \longmapsto & 0+6\mathbb{Z}\\ & 1+3\mathbb{Z} & \longmapsto & 2+6\mathbb{Z}\\ & 2+3\mathbb{Z} & \longmapsto & 4+6\mathbb{Z}\end{array}$$

satisfies, for example,

$$\varphi\left(\overline{1}+\overline{1}\right)=\varphi\left(\overline{2}\right)=\overline{4}=\overline{2}+\overline{2}=\varphi\left(\overline{1}\right)+\varphi\left(\overline{1}\right).$$

We write then

$$\mathbb{Z}/3\cong\left\{\overline{0},\overline{2},\overline{4}\right\}$$

and more generally we have

$$\mathbb{Z}/d\cong\left\{\overline{0},\overline{a},\overline{2a},...,\overline{(d-1)a}\right\}.$$

Definition 3.2.11 *A **group homomorphism** φ between two groups G_1 and G_2 is a map*

$$\varphi:G_1\longrightarrow G_2$$

which satisfies

$$\varphi\left(a\circ b\right)=\varphi\left(a\right)\circ\varphi\left(b\right)\quad\forall a,b\in G_1$$

that is, which is compatible with the group structures.

Note that $\circ$ on the left side is the operation in G_1, and on the right side is the operation in G_2.

Remark 3.2.12 *If $\varphi:G_1\longrightarrow G_2$ is a group homomomorphism, then*

$$\varphi\left(e_1\right)=e_2$$

where $e_i\in G_i$ denotes the respective neutral element.

*The **kernel** of φ*

$$\operatorname{Ker}\varphi=\left\{a\in G_1\mid\varphi\left(a\right)=e_2\right\}$$

*and the **image** of φ*

$$\operatorname{Im}\varphi=\varphi\left(G_1\right)$$

are subgroups of G_1 and G_2, respectively.

For the proof see Exercise 3.4.

For example, for the above group homomorphismus $\varphi:\mathbb{Z}/3\to\mathbb{Z}/6$ given by $\overline{1}\mapsto\overline{2}$, we have

$$\operatorname{Im}\varphi=\left\{\overline{0},\overline{2},\overline{4}\right\}$$
$$\operatorname{Ker}\varphi=\left\{\overline{0}\right\}.$$

Lemma 3.2.13 *A group homomorphism $\varphi : G_1 \longrightarrow G_2$ is injective if and only if*

$$\operatorname{Ker}\varphi = \{e_1\},$$

that is, the kernel contains only the neutral element e_1 of G_1.

Proof. We first remark, that for $b \in G_1$

$$(\varphi(b))^{-1} = \varphi\left(b^{-1}\right)$$

since

$$\varphi(b) \circ \varphi\left(b^{-1}\right) = \varphi(b \circ b^{-1}) = \varphi(e_1) = e_2,$$

and the inverse is unique. For $a, b \in G_1$ we hence have

$$\varphi(a) = \varphi(b) \Longleftrightarrow \varphi\left(a \circ b^{-1}\right) = e_2 \Longleftrightarrow a \circ b^{-1} \in \operatorname{Ker}\varphi.$$

using that

$$\varphi(a) \circ (\varphi(b))^{-1} = \varphi(a) \circ \varphi\left(b^{-1}\right) = \varphi(a \circ b^{-1})$$

Hence if $\operatorname{Ker}\varphi = \{e_1\}$, then $\varphi(a) = \varphi(b)$ implies, that $a = b$.

Is on the other hand φ injective, then it follows from

$$\varphi(a) = e_2 = \varphi(e_1)$$

that $a = e_1$. ■

Definition 3.2.14 *Injective group homomorphisms are called (group-) **monomorphisms**,surjective (group-)homomorphisms (group-) **epimorphisms**.*

*A (group-) **isomorphism***

$$\varphi : G_1 \longrightarrow G_2$$

ia a bijective homomorphism. The inverse map

$$\varphi^{-1} : G_2 \longrightarrow G_1$$

is then also a isomorphism. We write $G_1 \cong G_2$.

See also Exercise 3.4.

Example 3.2.15 *1) The inclusion of a subgroup $H \hookrightarrow G$ is a monomorphism.*

2) The map

$$\begin{array}{ccc} \mathbb{Z} & \longrightarrow & n\mathbb{Z} \\ k & \longmapsto & n \cdot k \end{array}$$

is for $n \geq 1$ an isomorphism.

*3) The **exponential function***

$$\begin{array}{ccc} (\mathbb{R}, +) & \longrightarrow & (\mathbb{R}_{>0}, \cdot) \\ x & \longmapsto & \exp(x) = e^x \end{array}$$

in Figure 3.6 is a homomorphism, since by the functional equation of the exponential function $e^{x_1+x_2} = e^{x_1} \cdot e^{x_2}$ for all $x_i \in \mathbb{R}$. Since the exponential function is continuous and strictly monotone with $\lim_{x \mapsto \infty} e^x = \infty$ and $\lim_{x \mapsto -\infty} e^x = 0$, it defines even an Isomorphismus.

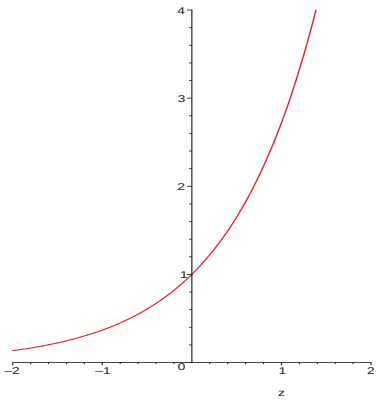


Figure 3.6: Exponential function

4) In contrast, with $\mathbb{C}^* = \mathbb{C} \backslash \{0\}$ the map

$$\begin{array}{ccc} (\mathbb{C}, +) & \longrightarrow & (\mathbb{C}^*, \cdot) \\ z & \longmapsto & \exp(z) = e^z \end{array}$$

is an epimorphism, but not an isomorphism. The kernel is

$$\operatorname{Ker}(\exp : \mathbb{C} \longrightarrow \mathbb{C}^*) = 2\pi i\mathbb{Z} := \{2\pi i n \mid n \in \mathbb{Z}\}.$$

5) Let $n \geq 2$. The ***signatur*** *or the* ***signum***

$$\begin{array}{rccl} \operatorname{sign}: & S_n & \longrightarrow & (\{\pm 1\}, \cdot) \\ & \sigma & \longmapsto & \operatorname{sign}(\sigma) = \prod\limits_{\substack{i,j=1 \\ i<j}}^{n} \frac{\sigma(i)-\sigma(j)}{i-j} \end{array}$$

is an epimorphism and

$$\operatorname{Ker}(\operatorname{sign}) = A_n$$

is called ***alternating group****.*

The definition of sign *translates into the following program (in the Syntax of* MAPLE*):*

```
sgn:=proc(sigma)
local s,j,i;
s:=1;
for j from 1 to nops(sigma) do
    for i from 1 to j-1 do
        s:=s*(sigma[i]-sigma[j])/(i-j);
    od;
od;
return(s);
end proc:
```

where we represent the permutation σ by the list $(\sigma(1), \ldots, \sigma(n))$.

As an example, we consider the permutation from Figure 3.2. For the rotation

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix}$$

using the above formula we obtain

$$\begin{aligned} \operatorname{sign}(\sigma) &= \frac{1-3}{1-2} \cdot \frac{1-4}{1-3} \cdot \frac{1-2}{1-4} \cdot \frac{3-4}{2-3} \cdot \frac{3-2}{2-4} \cdot \frac{4-2}{3-4} \\ &= \frac{3-2}{2-3} \cdot \frac{4-2}{2-4} = (-1)^2 = 1 \end{aligned}$$

and for the two reflections

$$\tau_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \end{pmatrix} \qquad \tau_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{pmatrix}$$

that $\operatorname{sign}(\tau_i) = -1$. *Indeed we have for all transpositions* τ, *that* $\operatorname{sign}(\tau) = -1$. *We will prove this below.*

Since sign *is a group homomorphism, it follows from* $\sigma = \tau_1 \cdot \tau_2$ *directly that*

$$\operatorname{sign}(\sigma) = \operatorname{sign}(\tau_1) \cdot \operatorname{sign}(\tau_2) = 1.$$

As we will see , one can easily compute the signum via the homomorphismu-property, by writing a permutation as a product of permutations with known signum.

See also Exercise 3.5.

6) If $a, b \in \mathbb{N}$ *and* $\gcd(a, b) = 1$. *Then*

$$\mathbb{Z}/ab \cong \mathbb{Z}/a \times \mathbb{Z}/b$$

This is a reformulation of the Chinese remainder theorem.

In practice, groups are often specified in terms of generators:

Definition 3.2.16 *Let* E *be a subset of a group* G. *Then* $\langle E \rangle$ *is the smallest subgroup of* G, *which contains all elements of* E. *Equivalently* $\langle E \rangle$ *is the intersection of all subgroups* U *with* $E \subset U \subset G$ *(since the intersection of subgroups is again a subgroup).*

We call $\langle E \rangle$ *the* ***subgroup generated by E****.*

A group G *is called* ***cyclic****, if there is a* $g \in G$ *with*

$$G = \langle g \rangle .$$

For $g \in G$ we obviously have

$$\langle g \rangle = \{ g^r \mid r \in \mathbb{Z} \}$$

with

$$g^r = \underbrace{g \circ \ldots \circ g}_{r}$$

and $g^r = (g^{-1})^{-r}$ for $r < 0$. If the operation is written additively as $+$ we write $r \cdot g$ instead of g^r.

Example 3.2.17 *1) The residue class group* $\mathbb{Z}/n$ *is cyclic generated by* $\overline{1}$.

2) The group $(\mathbb{Z}, +)$ *cyclic generated by* 1.

3) The subgroup $n\mathbb{Z} \subset (\mathbb{Z}, +)$ *is cyclic generated by* n*, so* $n\mathbb{Z} = \langle n \rangle$*. According to Example 3.2.15 we have* $n\mathbb{Z} \cong \mathbb{Z}$*.*

We will prove later, that all cyclic groups are up to isomorphism of the form $\mathbb{Z}$ or $\mathbb{Z}/n$ (see Example 3.3.13).

Definition 3.2.18 *Let* $g \in G$ *be an element of a group. Then*

$$\operatorname{ord}(g) = |\langle g \rangle|$$

is called the ***order*** *of* g*.*

See also Exercise 3.9.

Example 3.2.19 *For the rotation of the tetrahedron by* 120°

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix}$$

we have

$$\langle \sigma \rangle = \left\{ \mathrm{id} = \sigma^0, \sigma^1, \sigma^2 \right\} \cong \mathbb{Z}/3$$

and hence $\operatorname{ord}(\sigma) = 3$.

3.2.2 Group actions

Groups are considered in mathematics mainly since they can be used to describe symmetries. In order to interpret groups as groups of symmetries, the effect of the elements of a group on the elements of a set are specified through the notion of a group action:

Definition 3.2.20 *Let* $(G, \circ)$ *be a group and* M *a set. An* ***action*** *of* G *on* M *(from the left) is a map*

$$\begin{array}{rccc} \cdot : & G \times M & \longrightarrow & M \\ & (g, m) & \longmapsto & g \cdot m \end{array}$$

which satisfies the following conditions:

1)

$$e \cdot m = m$$

for all $m \in M$.

2)

$$(a \circ b) \cdot m = a \cdot (b \cdot m)$$

for all $a, b \in G$ *and* $m \in M$.

Remark 3.2.21 *In an analogous way, one can specify operatons from the right*

$$\begin{array}{rccc} \cdot : & M \times G & \longrightarrow & M \\ & (m, g) & \longmapsto & m \cdot g \end{array}$$

with $m \cdot e = m$ *and* $(m \cdot a) \cdot b = m \cdot (a \circ b)$.

It seems to be superfluous to have both notations, however there are settings, where there are two distinct canonical definitions for an action from the left and from the right, and where both definitions are used at the same time. An example is the action of a subgroup $H \subset G$ *on* G *by* $H \times G \to G$, $(h, g) \mapsto h \circ g$ *from the left, and by* $G \times H \to G$, $(g, h) \mapsto g \circ h$ *from the right, which we will later discuss in detail.*

Remark 3.2.22 *To put it differently, an action of* G *on* M *is a group homomorphism*

$$\begin{array}{rccc} \varphi : & G & \longrightarrow & S(M) \\ & g & \mapsto & \varphi(g) := \begin{pmatrix} M & \longrightarrow & M \\ m & \mapsto & g \cdot m \end{pmatrix} \end{array}$$

of G *into the group of self-mappings of* M.

Proof. We check whether $\varphi(g)$ for alle $g \in G$ is bijective and whether φ is a homomorphism: Let $g \cdot m_1 = g \cdot m_2$ for $m_1, m_2 \in M$. Then

$$\begin{aligned} m_1 = e \cdot m_1 &= \left(g^{-1} \circ g\right) \cdot m_1 = g^{-1} \cdot (g \cdot m_1) \\ &= g^{-1} \cdot (g \cdot m_2) = \left(g^{-1} \circ g\right) \cdot m_2 = e \cdot m_2 = m_2. \end{aligned}$$

Each $m \in M$ is in the image of $\varphi(g)$, since $m = e \cdot m = g \cdot (g^{-1} \cdot m)$. Moreover,

$$\begin{aligned} \varphi(g \circ h) &= (m \mapsto (g \circ h) \cdot m) = (m \mapsto g \cdot (h \cdot m)) \\ &= (m \mapsto g \cdot m) \circ (m \mapsto h \cdot m) = \varphi(g) \circ \varphi(h). \end{aligned}$$

■

Example 3.2.23 *S_n acts on $\{1,...,n\}$ by*

$$\begin{array}{ccc} S_n \times \{1,...,n\} & \longrightarrow & \{1,...,n\} \\ (\sigma,\, j) & \longmapsto & \sigma(j) \end{array}$$

Another key example is the action of the group of motions of $\mathbb{R}^n$:

Definition 3.2.24 *A Euclidean **motion** $f : \mathbb{R}^n \to \mathbb{R}^n$ is a map, which respects the Euclidean distance*

$$\|x\| := \sqrt{\textstyle\sum_{i=1}^{n} x_i^2}$$

that is, with

$$\|x - y\| = \|f(x) - f(y)\|$$

for all $x, y \in \mathbb{R}^n$. Figure 3.7 shows a motion, which is the composition of a translation and a roto-reflection. The set $\mathrm{E}(n)$ of

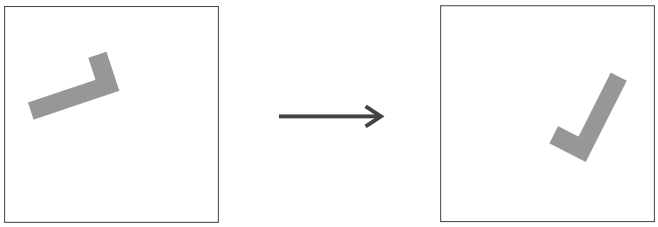


Figure 3.7: Example of a motion of $\mathbb{R}^2$.

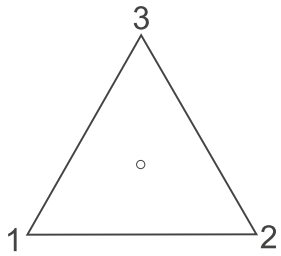
*Euclidean motions of $\mathbb{R}^n$ is with the composition a group, the **group of motions**.*

Let $M \subset \mathbb{R}^n$ be a subset. The group

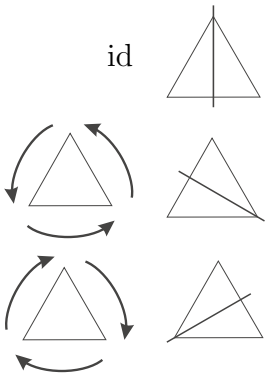
$$\mathrm{Sym}(M) = \{A \in \mathrm{E}(n) \mid A(M) = M\}$$

*is called the **symmetry group** of M.*

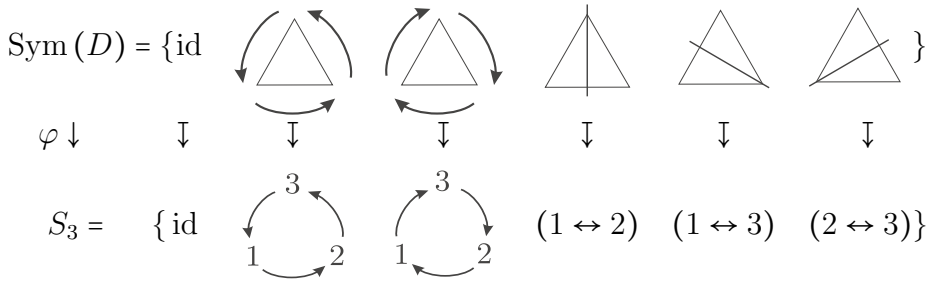
Example 3.2.25 (Symmetry group) *We describe the symmetry group $\mathrm{Sym}(D)$ of the equilateral triangle D.*



Every symmetry is a rotation or reflection



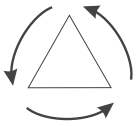
Every symmetry is uniquely determined by its action on the vertices of the triangle. By numbering the vertices, we can consider every symmetry as a bijective map $\{1,2,3\} \to \{1,2,3\}$. *Indeed, we have a group isomorphism* φ



which is induced by the action of $\mathrm{Sym}\,(D)$ *on the vertices of the triangle*

$$\mathrm{Sym}\,(D) \times \{1,2,3\} \longrightarrow \{1,2,3\}\,.$$

Is, for example,

$r_{120} =$ 

the rotation by $120°$*, then the operation gives a map*

$$(r_{120}, 1) \mapsto 2,\ (r_{120}, 2) \mapsto 3,\ (r_{120}, 3) \mapsto 1$$

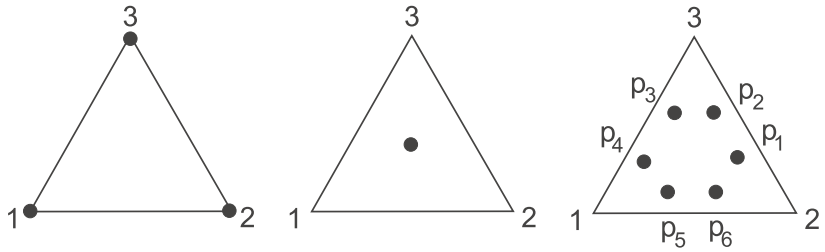
hence

$$\varphi(r_{120}) = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

Example 3.2.26 (Orbit and Stabilizer) *Given a point of the equilateral triangle D, we want to investigate on which other points under the operation*

$$\mathrm{Sym}\,(D) \times D \longrightarrow D$$

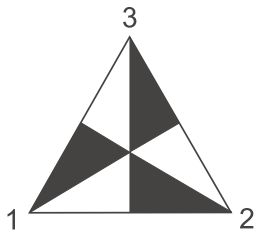
this point can map. This set is called the orbit, the number of elements the lenght of the orbit. Examples of orbits are



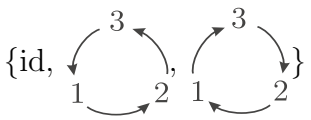
The operation on D induce an operation

$$\mathrm{Sym}\,(D) \times 2^D \longrightarrow 2^D$$

of the set of all subsets of D. In the orbit of the black subset is also the white subset:



Otherwise one can consider the set of all elements of $\mathrm{Sym}\,(D)$*, that keep a given point (or a subset) fixed. The corner* 1 *is fixed by* $\{\mathrm{id}, (2 \leftrightarrow 3)\}$*, the middlepoint* m *by* $\mathrm{Sym}\,(D)$ *and the point* p_1 *only by the identity. The black subset is fixed by*



We observe that these sets are subgroups of $\mathrm{Sym}\,(D)$*, and that the product of the group orders with length the respective orbits,*

in each case $|\mathrm{Sym}(D)| = 6$*, give.*

	Orbit	*fixed by*	
1	$\{1,2,3\}$	$\{\mathrm{id}, (2 \leftrightarrow 3)\}$	$3 \cdot 2 = 6$
m	$\{m\}$	$\mathrm{Sym}(D)$	$1 \cdot 6 = 6$
p_1	$\{p_1, ..., p_6\}$	$\{\mathrm{id}\}$	$6 \cdot 1 = 6$

This is true in general, and is called the orbit counting theorem (see Section **??***).*

We first formalize the ideas of orbit and stabilizer:

Definition 3.2.27 *Let* $G \times M \to M$ *be an action. For* $m \in M$ *we call*

$$Gm = \{g \cdot m \mid g \in G\} \subset M$$

the ***orbit*** *of* m*. If* $N \subset M$ *is any subset, then*

$$\mathrm{Stab}(N) = \{g \in G \mid gN = N\},$$

where $gN = \{g \cdot n \mid n \in N\}$*, is called the* ***stabilizer*** *of* N*.*

The most important case is that of the stabilizer of a 1*-element set: For an element* $m \in M$ *let*

$$\mathrm{Stab}(m) = \{g \in G \mid g \cdot m = m\} = \mathrm{Stab}(\{m\}).$$

Remark 3.2.28 *Two orbits* Gm_1 *and* Gm_2 *are either equal or disjoint. To be in the same orbit is, hence, an equivalence relation.*

Proof. If there exists an

$$m_3 \in Gm_1 \cap Gm_2$$

then there are $g_1, g_2 \in G$ with

$$m_3 = g_1 \cdot m_1 = g_2 \cdot m_2$$

hence

$$m_2 = g_2^{-1} \cdot (g_1 \cdot m_1).$$

For every $g \in G$ we hence have

$$g \cdot m_2 = g \cdot (g_2^{-1} \cdot (g_1 \cdot m_1)) = (g \circ g_2^{-1} \circ g_1) \cdot m_1 \in Gm_1$$

that is

$$Gm_2 \subset Gm_1.$$

Similarily we have the other inclusion, that is $Gm_2 = Gm_1$.

The second claim one easily checks using the definition of an equivalence relation. ■

Definition 3.2.29 *The set of orbits we denote by M/G (**quotient** of M by G). Every element $m \in Gm_1$ we call a **representative** of the orbit, since $Gm = Gm_1$. Morover,*

$$\begin{array}{rccc} \pi: & M & \longrightarrow & M/G \\ & m & \longmapsto & Gm \end{array}$$

*is called the **quotient map**.*

With the above remark we see:

Definition and Theorem 3.2.30 *Let $G \times M \to M$ be an action. A **complete set of representatives** of the orbits is a subset $R \subset M$, such that every orbit Gm contains exactly one element of R.*

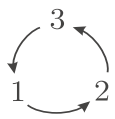
Then M is the disjoint union

$$M = \dot{\bigcup_{r \in R}} G \cdot r$$

The representation of permutations in mapping notation is not efficient: For the permutation

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

we do not have to remember the images of $4, \ldots, 7$. The images of $1, 2, 3$ we can encode in a diagram



This is the idea of a so-called cycle:

Definition 3.2.31 *If $\sigma \in S_n$, then the action of $\langle\sigma\rangle$ on the set $\{1,...,n\}$ decomposes the set into orbits*

$$\langle\sigma\rangle x = \left\{x, \sigma(x), \sigma^2(x), ..., \sigma^{t-1}(x)\right\}$$

*and t minimal with $\sigma^t(x) = x$. If there is only one orbit of length $t > 1$ (that is, all others have length 1), then σ is called a **cycle** of order t, and we write*

$$\sigma = \left(x, \sigma(x), \sigma^2(x), ..., \sigma^{t-1}(x)\right),$$

*that is we code, in addition to the orbit, also the order in which we go through the orbit by iteratively applyíng σ. **Transpositions** are cycles of length 2. For the neutral element we write $()$.*

One could also use for a cycle a circle notation as above, but that would use a bit too much space, and would not be easy to enter on a computer console.

Remark 3.2.32 *The cycle*

$$\sigma = (a_1, \dots, a_t) \in S_n$$

is thus the map

$$\begin{aligned} \{1,\dots,n\} &\longrightarrow \{1,\dots,n\} \\ a_1 &\longmapsto a_2 \\ a_2 &\longmapsto a_3 \\ &\vdots \\ a_{t-1} &\longmapsto a_t \\ a_t &\longmapsto a_1 \\ a &\longmapsto a \quad \textit{otherwise,} \end{aligned}$$

and $\mathrm{ord}(\sigma) = t$.

Example 3.2.33 *For the rotation*

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix}$$

of the tetrahedron by $120°$ *(see also Example 3.2.19) we obtian the decomposition into orbits*

$$\{1,2,3,4\} = \{1\} \dot\cup \{2,3,4\}\,.$$

Hence σ *is a cycle and by remembering the order in which we go through the orbit by iteratively applying* σ*, we get*

$$\sigma = (2,3,4),$$

that is, $2 \mapsto 3$*,* $3 \mapsto 4$*,* $4 \mapsto 2$*. The notation of a cycle one can open up at any point, hence*

$$\sigma = (2,3,4) = (3,4,2) = (4,2,3).$$

The rotation

$$\sigma^2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix}$$

of the tetrahedron by $240°$ *gives the same decomposition into orbits* $\{1,2,3,4\} = \{1\} \dot\cup \{2,3,4\}$*, but*

$$\sigma^2 = (2,4,3).$$

Note that it is easy to compute square of cycles σ*: We just have to go two steps in the cycle to get the image of an element (and similarly for higher powers).*

Not every permutation is a cycle: Under the action of

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

there are two orbits of length 4 and

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

is the product of two cycles. Since orbits are disjoint, we can always decompose a permutation into disjoint cycles:

Theorem 3.2.34 *We have:*

1) Every element of S_n *is a product of disjoint cycles.*

2) Ever element of S_n is a product of transpositions.

Proof. Let $\sigma \in S_n$.

1) Let $\{x_1, ..., x_r\}$ be a complete set of representatives of the orbits of the operation of $\langle\sigma\rangle$ on $\{1, ..., n\}$. If we restrict σ as a map on the orbit $\langle\sigma\rangle x_i$, then we obtain a cycle σ_i and

$$\sigma = \sigma_1 \circ ... \circ \sigma_r$$

2) Using 1) we may assume, that σ is a cycle $(y_0, ..., y_{t-1})$. Then, as one easily checks,

$$(y_0, ..., y_{t-1}) = (y_0, y_1) \circ ... \circ (y_{t-2}, y_{t-1}) .$$

■

In the cycle notation of permuations, one usually leaves the symbol $\circ$ away.

Example 3.2.35 *Let*

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

The operation of $\langle\sigma\rangle$ decomposes

$$\{1, ..., 9\} = \{1, 2, 3, 4\} \dot\cup \{5, 9\} \dot\cup \{6, 8\} \dot\cup \{7\}$$

in disjoint orbits

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

See also Exercise 3.7.

Remark 3.2.36 *If $\sigma = \tau_1 \circ ... \circ \tau_r$ with transpositions τ_i, then we can compute the signum of σ directly as*

$$\operatorname{sign}(\sigma) = (-1)^r,$$

since sign *is a group homomorphism and* $\operatorname{sign}\tau = -1$ *for all transpositions τ.*

Proof. For a transposition τ, we compute

$$\operatorname{sign}(\tau) = \prod_{i<j} \frac{\tau(i) - \tau(j)}{i - j}.$$

Assume $\tau = (k, l)$ and $k < l$.Then

$$\frac{\tau(i) - \tau(j)}{i - j} = \begin{cases} -1 & \text{for } i = k \text{ and } j = l \\ 1 & \text{for } i, j \notin \{k, l\} \\ \frac{l-j}{k-j} & \text{for } i = k \text{ and } j \neq l \\ \frac{i-k}{i-l} & \text{for } i \neq k \text{ and } j = l. \end{cases}$$

If we further split up the last two cases into the j with $k = i < j < l$ or $l < j$, and into the i with $k < i < j = l$ or $i < k$, respectively, then we get

$$\operatorname{sign}(\tau) = -\underbrace{\prod_{\substack{j \text{ with} \\ l<j}} \frac{l-j}{k-j}}_{>0} \cdot \underbrace{\prod_{\substack{j \text{ with} \\ k<j<l}} \frac{l-j}{k-j} \cdot \prod_{\substack{i \text{ with} \\ k<i<l}} \frac{i-k}{i-l}}_{1} \cdot \underbrace{\prod_{\substack{i \text{ with} \\ i<k}} \frac{i-k}{i-l}}_{>0}.$$

The second and the third product cancel, and all numerators an denominators of the first and last product are negative. Hence $\operatorname{sign}\tau < 0$ so $\operatorname{sign}\tau = -1$. ■

Example 3.2.37 *For*

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

we obtain

$$\operatorname{sign}(\sigma) = (-1)^5 = -1.$$

Remark 3.2.38 *For a representation of a permutation $\sigma = c_1 \circ \ldots \circ c_r$ as a product of disjoint cycles c_i of length m_i one can compute the order of σ as*

$$\operatorname{ord}(\sigma) = \operatorname{lcm}(m_1, \ldots, m_r).$$

For the proof see Exercise 3.9.

Example 3.2.39 *For* $\sigma = (1,4,3,2)\,(5,9)\,(6,8)$ *we get*

$$\operatorname{ord}(\sigma) = \operatorname{lcm}(4,2,2) = 4.$$

We can check this also by a direct calculation

$$\begin{aligned}\sigma^2 &= (1,4,3,2)^2(5,9)^2(6,8)^2 = (1,3)(2,4)\\ \sigma^3 &= (1,2,3,4)(5,9)(6,8)\\ \sigma^4 &= \mathrm{id}\,.\end{aligned}$$

For subgroups of S_n the computer algebra system GAP [13] algorithms for computing essentially all object introduced in this chapter.

Example 3.2.40 *We determine* $\operatorname{ord}(\sigma)$ *for*

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

using GAP*:*

```
sigma:=(1,4,3,2)(5,9)(6,8);
```
$(1,4,3,2)(5,9)(6,8)$
```
sigma^2;
```
$(1,3)(2,4)$
```
sigma^3;
```
$(1,2,3,4)(5,9)(6,8)$
```
sigma^4;
```
$()$

Hence $\operatorname{ord}(\sigma) = 4$*. To apply Remark 3.2.38, instead, we use:*

```
Order(sigma);
```
4

Note that, in contrast to the usual convention, to compute $\sigma \circ \tau$ *for* $\sigma, \tau \in S_n$ *we have to enter* $\tau * \sigma$ *in* GAP *(that is, maps take their argument on the left hand side). We check in* GAP*, that with* $\tau = (2,5)$ *we get*

$$\begin{aligned}\sigma \circ \tau &= (1,4,3,2)\,(5,9)\,(6,8) \circ (2,5)\\ &= (1,4,3,2,9,5)(6,8).\end{aligned}$$

```
tau:=(2,5);;
tau*sigma;
```
$(1,4,3,2,9,5)(6,8)$

Remark 3.2.41 *The symmetric group S_3 is generated by $(1,2)$ and $(2,3)$*

$$S_3 = \langle (1,2), (2,3) \rangle$$

since $(1,2)(2,3) = (1,2,3)$ and $(1,2)(2,3)(1,2) = (1,3)$. In general, we have

$$S_n = \langle (1,2), (2,3), ..., (n-1,n) \rangle,$$

see also die Exercises 3.21 and 3.22.

Example 3.2.42 *In* GAP *we can define a group via a generating system as follows:*

```
G:=Group((1,2),(2,3));
```

Group$([(1,2),(2,3)])$

```
Elements(G);
```

$[(), (2,3), (1,2), (1,2,3), (1,3,2), (1,3)]$

3.2.3 Action by translation

So far, we have considered the action of $\mathrm{Sym}(M)$ on a set M and of S_n on $\{1, ..., n\}$. A further very important example is the action of a group $(G, \circ)$ on itself

$$\begin{aligned} G \times G &\longrightarrow G \\ (g,h) &\mapsto g \circ h \end{aligned}$$

given by the group operation (this gives an action both from the left and from the right). The action plays in important role in the proof of the following theorem, which is of key importance for practical calculations with groups: It allows to consider any finite group as a subgroup of S_n. In this representation, the group can then be handled by the computer.

Theorem 3.2.43 (Cayley) *Every group G is isomorphic to a subgroup of the group of self-mappings $S(G)$.*

In particular for $n := |G| < \infty$, we can consider G as a subgroup of $S_n \cong S(G)$.

Proof. The map

$$\begin{array}{rccc} \varphi: & G & \to & S(G) \\ & g & \mapsto & \begin{pmatrix} G & \to & G \\ h & \mapsto & g \circ h \end{pmatrix} \end{array}$$

is a group homomorphism and

$$\operatorname{Ker}\varphi = \{g \in G \mid g \circ h = h \ \forall h \in G\} = \{e\}$$

(using the uniqueness of the neutral element), hence φ is injective. Hence,

$$G \cong \operatorname{Im}(\varphi) \subset S(G).$$

■

For finite groups one can specify the action

$$\begin{aligned} G \times G &\longrightarrow G \\ (g,h) &\mapsto g \circ h \end{aligned}$$

via a table, the **group table**.

Example 3.2.44 *The group*

$$G = \mathbb{Z}/4 = \left\{\overline{0}, \overline{1}, \overline{2}, \overline{3}\right\}$$

has the group table

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{0}$	$\overline{1}$	$\overline{2}$

In ever row or column, every element of the group occurs exactly once.

The rows of the table specify $\varphi(g)$, in the example we have

$$\varphi(\overline{0}) = \begin{pmatrix} \overline{0} & \overline{1} & \overline{2} & \overline{3} \\ \overline{0} & \overline{1} & \overline{2} & \overline{3} \end{pmatrix}$$

$$\varphi(\overline{1}) = \begin{pmatrix} \overline{0} & \overline{1} & \overline{2} & \overline{3} \\ \overline{1} & \overline{2} & \overline{3} & \overline{0} \end{pmatrix}$$

$$\varphi(\overline{2}) = \begin{pmatrix} \overline{0} & \overline{1} & \overline{2} & \overline{3} \\ \overline{2} & \overline{3} & \overline{0} & \overline{1} \end{pmatrix}$$

$$\varphi(\overline{3}) = \begin{pmatrix} \overline{0} & \overline{1} & \overline{2} & \overline{3} \\ \overline{3} & \overline{0} & \overline{1} & \overline{2} \end{pmatrix}$$

where we use the map notation introduced for elements of S_n also for elements of $S(G)$.

Finally, we can number the elements of G to do the identification $S(G) \cong S_4$.

A group is abelian if and only if its group table is symmetric with respect to the diagonal. The associaticity law one cannot see in any obvious way from the table.

Analogous to the action of a group on itself, one can also consider the action of a subgroup on the group:

Example 3.2.45 *As shown in Example 3.2.7, the subgroups of $(\mathbb{Z}, +)$ are of the form*

$$n\mathbb{Z} = \{n \cdot k \mid k \in \mathbb{Z}\}.$$

A group action of $n\mathbb{Z}$ on $\mathbb{Z}$ (from the right) is given by

$$\begin{aligned} \mathbb{Z} \times n\mathbb{Z} &\to \mathbb{Z} \\ (a, n \cdot k) &\mapsto a + n \cdot k \end{aligned}$$

The orbits are exactly the residue classes modulo n

$$\overline{a} = a + n\mathbb{Z} = \{a + n \cdot k \mid k \in \mathbb{Z}\}.$$

Analogusly, we can also operate by addition from the left, and obtain the same orbits, since $+$ is commutative. Due to the usual notation $a + n\mathbb{Z}$ for residue classes, one prefers the action from the right.

For $n = 4$, we obtain by the action of $4\mathbb{Z}$ on $\mathbb{Z}$ the orbits

$4\mathbb{Z}$	$1 + 4\mathbb{Z}$	$2 + 4\mathbb{Z}$	$3 + 4\mathbb{Z}$
$\vdots$	$\vdots$	$\vdots$	$\vdots$
-4	-3	-2	-1
0	1	2	3
4	5	6	7
$\vdots$	$\vdots$	$\vdots$	$\vdots$

As seen in Example 3.2.8, the set of orbits with the operation

$$\overline{a} + \overline{b} = (a + n\mathbb{Z}) + (b + n\mathbb{Z}) = (a + b) + n\mathbb{Z} = \overline{a + b}$$

is again a group, called $\mathbb{Z}/n$.

Later, we will investigate, when a set of orbits of a subgroup is again a group.

We first introduce the concept of orbits of a subgroup in general:

Definition 3.2.46 (Cosets) *Let $H \subset G$ be a subgroup. Then the operation in G defines an action of H on G*

$$H \times G \longrightarrow G,\ (h, g) \longmapsto h \circ g$$

from the left, and similarly from the right

$$G \times H \longrightarrow G,\ (g, h) \longmapsto g \circ h.$$

For $g \in G$ the orbits of this action

$$Hg := H \circ g := \{h \circ g \mid h \in H\}$$

and

$$gH := g \circ H := \{g \circ h \mid h \in H\}$$

*are called the right and left **cosets** of g, respectively.*

Theorem 3.2.47 *Let $H \subset G$ be a subgroup. Every two cosets of H have the same number of elements.*

Proof. Let $a, b \in G$. Then aH and bH are in bijection by multiplication with ba^{-1} from the left

$$\begin{array}{ccc} g & \longmapsto & b \circ a^{-1} \circ g \\ G & \overset{1:1}{\longrightarrow} & G \\ \cup & & \cup \\ aH & \longrightarrow & bH \\ a \circ h & \longmapsto & b \circ a^{-1} \circ a \circ h = b \circ h \end{array}$$

(what is the inverse?). The right and left cosets aH and Ha are in bijection via **conjugation** with a

$$\begin{array}{ccc} g & \longmapsto & a^{-1} \circ g \circ a \\ G & \overset{1:1}{\longrightarrow} & G \\ \cup & & \cup \\ aH & \longrightarrow & Ha \\ a \circ h & \longmapsto & a^{-1} \circ a \circ h \circ a = h \circ a \end{array}$$

(what is the inverse?). The operation by conjugation will also be discussed in Exercise 3.12. ■

Corollary 3.2.48 (Index formula) *Let $H \subset G$ be a subgroup. Then*

$$|G| = |G/H| \cdot |H|$$

in particular in a finite group G, the order of the subgroup $|H|$ divides $|G|$.

Definition 3.2.49 *If $H \subset G$ is a subgroup, then*

$$[G : H] := |G/H|$$

*is called the **index** of H in G.*

We remark, that

$$\begin{aligned} H &\to aH \\ h &\mapsto a \circ h \end{aligned}$$

is a bijection (see the proof of Theorem 3.2.47), hence

$$|aH| = |H| .$$

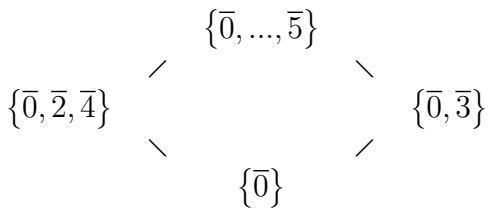
We prove now the index formula:

Proof. By Definition and Theorem 3.2.30 the group G is the disjoint union of all aH with a from a complete set of representatives R, so if $|G| < \infty$ then

$$|G| = \sum_{a \in R} |aH| = |R| \cdot |H|$$

(using Theorem 3.2.47). If $|G| = \infty$, then also $|G/H| = \infty$ or $|H| = \infty$. ■

Example 3.2.50 *The group $G = \mathbb{Z}/6$ has the order 6 and the subgroups*



with the orders $1, 2, 3$ and 6.

Remark 3.2.51 *Note that in a group, there is not necessarily for every divisor a subgroup with the respective order, for example,*

$$A_4 = \{\sigma \in S_4 \mid \operatorname{sign}(\sigma) = 1\}$$

does not have a subgroup of the order 6. *The following* GAP *code computes all possible order of subgroups of* A_4*:*

```
G:=AlternatingGroup(4);;
Order(G);
12
L:=ConjugacyClassesSubgroups(G);;
List(List(L,Representative),Size);
[ 1, 2, 3, 4, 12 ]
```

In the context of the so-called Sylow theorems, one can prove, that there is a subgroup of the respective order for every prime power divisor of $|G|$.

From the index formula (Theorem 3.2.48) we get taking $H = \langle g \rangle$:

Corollary 3.2.52 *In every finite group* G *the order of an element* $g \in G$ *is a divisor of the group order* $|G|$, *that is,* $\operatorname{ord}(g) \mid |G|$.

Example 3.2.53 *In* $G = \mathbb{Z}/6$, *the elements* $\overline{1}$ *and* $\overline{5} = \overline{-1}$ *have order* 6, *the elements* $\overline{2}$ *and* $\overline{4}$ *have order* 3, *and the element* $\overline{3}$ *has order* 2. *The neutral element* $\overline{0}$ *has order* 1.

Corollary 3.2.54 *Every group* G *with* $|G|$ *prime is cyclic.*

Proof. Using the index formula, we get, that G only has the subgroups $\{e\}$ and G. Hence, for every $e \neq g \in G$ we have

$$\{e\} \neq \langle g \rangle = G$$

■

3.3 Normal subgroups

3.3.1 Normal subgroups and the quotient group

Let H be a subgroup of $(G, \circ)$ and

$$G/H = \{gH \mid g \in G\}$$

the set of left cosets

$$gH = \{g \circ h \mid h \in H\}$$

of H, that is, the set of orbits of the translation action $G \times H \to G$, $(g, h) \mapsto g \circ h$ of H on G.

Example 3.3.1 *For $H = n\mathbb{Z} \subset \mathbb{Z} = G$ we have already seen that the set*

$$G/H = \mathbb{Z}/n = \{\overline{0}, \ldots, \overline{n-1}\}$$

of cosets

$$\overline{a} = a + n\mathbb{Z}$$

with the operation induced by the addition in $\mathbb{Z}$

$$\overline{a} + \overline{b} := \overline{a + b}$$

has the structure of a group.

More generally, is it true that G/H with the operation

$$aH \cdot bH := (a \circ b)H$$

induced by that of G becomes a group? As in the case of $\mathbb{Z}/n$ the problem arises from the question whether the operation is well-defined, that is, whether it is independent from the choice of representatives a, b of the cosets aH and bH.

Example 3.3.2 *Let us go back to the respective calculation for $\mathbb{Z}/n$: Let $\overline{a_1} = \overline{a_2}$ and $\overline{b_1} = \overline{b_2}$, that is, $a_1 = a_2 + k \cdot n$ and $b_1 = b_2 + l \cdot n$ for some k and l. Then*

$$a_1 + b_1 = a_2 + k \cdot n + b_2 + l \cdot n = a_2 + b_2 + (k + l) \cdot n,$$

hence $\overline{a_1 + b_1} = \overline{a_2 + b_2}$. In this calculation, we have commuted the summands $k \cdot n$ and b_2. This was possible, since $G = \mathbb{Z}$ is abelian.

Now to the general setting. If G/H with $aH \cdot bH = (a \circ b)H$ is a group, then the quotient map

$$\pi : G \longrightarrow G/H,\ g \longmapsto gH$$

is a group homomorphism, since for all $a, b \in G$ we have

$$\pi(a) \cdot \pi(b) = aH \cdot bH = (a \circ b)H = \pi(a \circ b).$$

Moreover

$$\pi(e) = eH = H \in G/H$$

is the neutral element, hence $H = \mathrm{Ker}(\pi)$. Indeed, for the kernel of a group homomorphism, we observe in general:

Remark 3.3.3 *Let*

$$\varphi : G \longrightarrow F$$

be a group homomorphism and

$$H = \mathrm{Ker}(\varphi) \subset G.$$

Then for $g \in G$ and

$$gHg^{-1} := \left\{ g \circ h \circ g^{-1} \mid h \in H \right\},$$

we have

$$gHg^{-1} = H.$$

Proof. If $h \in \mathrm{Ker}\,\varphi$, then for all $g \in G$

$$\varphi\left(g \circ h \circ g^{-1}\right) = \varphi(g) \circ \varphi(h) \circ \varphi(g)^{-1} = \varphi(g) \circ \varphi(g)^{-1} = e,$$

so $g \circ h \circ g^{-1} \in H$ and hence

$$gHg^{-1} \subset H.$$

If we replace g by g^{-1}, we get the other inclusion. ■

Subgroups with this property of the kernel, are called normal subgroups:

Definition 3.3.4 *A subgroup $H \subset G$ is called a* ***normal subgroup*** *of G (written $H \triangleleft G$), if*

$$gHg^{-1} = H \text{ for all } g \in G$$

(equivalently $gH = Hg$ for all $g \in G$ or $gHg^{-1} \subset H$ for all $g \in G$).

More generally than the above example we have:

Remark 3.3.5 *If $\varphi : G \longrightarrow F$ is a group homomorphism and $M \subset F$ is a normal subgroup, then $\varphi^{-1}(M) \subset G$ is a normal subgroup. If φ is surjective and $N \subset G$ is a normal subgroup, then $\varphi(N) \subset F$ is a normal subgroup.*

We prove this in Exercise 3.17.

Theorem 3.3.6 *Let $H \subset G$ be a subgroup. The set G/H is with the induced operation*

$$aH \cdot bH = (a \circ b)H$$

a group, if and only if H is a normal subgroup. We then call G/H the ***quotient group****.*

Proof. We have already seen that H normal is necessary for G/H becoming a group. The condition is also sufficient: Let $H \subset G$ be a normal subgroup. We prove that

$$aH \cdot bH = (a \circ b)H$$

specifies a well-defined operation, that is, given other representatives

$$a_2 \in a_1 H \qquad b_2 \in b_1 H$$

we have to show that

$$(a_2 \circ b_2)H = (a_1 \circ b_1)H.$$

Write

$$a_2 = a_1 \circ h \qquad b_2 = b_1 \circ h'$$

with $h, h' \in H$. Since H is a normal subgroup, we have

$$Hb_1 = b_1 H,$$

so there exists an $h'' \in H$ with

$$h \circ b_1 = b_1 \circ h''$$

and hence

$$(a_2 \circ b_2)H = (a_1 \circ h \circ b_1 \circ h')H = (a_1 \circ b_1 \circ h'' \circ h')H = (a_1 \circ b_1)H.$$

Note that $hH = H$ for all $h \in H$, since multiplication by h is a bijektive map $H \to H$.

We check that this operation on G/H indeed defines a group structure: Associativity

$$(aH \cdot bH) \cdot cH = aH \cdot (bH \cdot cH)$$

follows from $(a \circ b) \circ c = a \circ (b \circ c)$. Moreover,

$$eH = H$$

is the neutral element, and

$$(aH)^{-1} = a^{-1}H$$

the inverse of aH. ■

Example 3.3.7 *Every subgroup of an abelian group is a normal subgroup. For example, the subgroups $n\mathbb{Z} \subset (\mathbb{Z}, +)$ are normal. We test this using the definition: For all $g \in \mathbb{Z}$ we have*

$$\begin{aligned} g + n\mathbb{Z} &= \{g + nk \mid k \in \mathbb{Z}\} \\ &= \{nk + g \mid k \in \mathbb{Z}\} = n\mathbb{Z} + g. \end{aligned}$$

The quotient group is the residue class group

$$\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/n = \left\{\overline{0}, \ldots, \overline{n-1}\right\}.$$

The neutral element is $\overline{0} = 0 + n\mathbb{Z} = n\mathbb{Z}$ and the inverse is $-\overline{a} = \overline{-a} = \overline{n-a}$.

Example 3.3.8 *$A_n = \ker(\mathrm{sign}) \subset S_n$ is by Remark 3.3.3 a normal subgroup. We test this using the definition: For all $\tau \in S_n$ and $\sigma \in A_n$ we have*

$$\mathrm{sign}(\tau \circ \sigma \circ \tau^{-1}) = \mathrm{sign}(\tau)\,\mathrm{sign}(\sigma)\,\mathrm{sign}(\tau)^{-1} = \mathrm{sign}(\sigma) = 1.$$

Remark 3.3.9 *Every subgroup $U \subset G$ of index $[G : U] = 2$ is a normal subgroup of G.*

The short proof is Exercise 3.16. See also Exercise 3.13.

3.3.2 Homomorphism theorem

If $\varphi : G \longrightarrow F$ is a monomorphism, then we can consider $G \cong \mathrm{Im}(\varphi) \subset F$ as a subgroup of F. Otherwise, we can make φ injective using the quotient group construction:

Theorem 3.3.10 (Homomorphism theorem) *Let $\varphi : G \longrightarrow F$ be a group homomorphism. Then*

$$G/\operatorname{Ker}\varphi \cong \mathrm{Im}(\varphi).$$

Proof. We define

$$\widetilde{\varphi} : G/\operatorname{Ker}\varphi \longrightarrow \operatorname{Im}\varphi$$
$$\widetilde{\varphi}(a \operatorname{Ker}\varphi) := \varphi(a)$$

This is well-defined, since for

$$a' = a \circ h \in a \operatorname{Ker}\varphi \text{ with } h \in \operatorname{Ker}\varphi$$

we have

$$\varphi(a') = \varphi(a) \cdot \varphi(h) = \varphi(a) \cdot e = \varphi(a).$$

Since φ is a homomorphism, also $\widetilde{\varphi}$ is a homomorphism, it is surjective on the image of φ, and injective, since

$$\widetilde{\varphi}(a \operatorname{Ker}\varphi) = e$$
$$\Rightarrow \varphi(a) = e \Rightarrow a \in \operatorname{Ker}\varphi$$
$$\Rightarrow a \operatorname{Ker}\varphi = \operatorname{Ker}\varphi = e_{G/\operatorname{Ker}\varphi}.$$

■

Hence $\varphi : G \longrightarrow F$ factorizes in

$$\begin{array}{ccccc} & & G & \xrightarrow{\varphi} & F & \\ \text{projection} & & \downarrow & & \uparrow & \text{inclusion} \\ & & G/\operatorname{Ker}\varphi & \cong & \operatorname{Im}\varphi & \end{array}$$

Example 3.3.11 *Let $n \geq 2$. Applied to $\mathrm{sign} : S_n \to (\{-1,1\},\cdot)$ with kernel A_n and $\mathrm{im}(\mathrm{sign}) = \{-1,1\} \cong \mathbb{Z}/2$ we obtain from Theorem 3.3.10, that*

$$S_n/A_n \cong \mathbb{Z}/2.$$

Example 3.3.12 *The* ***Klein four-group***

$$V_4 = \{(), (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}$$

is a normal subgroup of S_4 *and for the quotient group we have*

$$S_4/V_4 \cong S_3.$$

We prove this in Exercise 3.18, where we interpret the isomorphism geometrically by considering S_4 *as the symmetry group of the tetrahedron.*

We can also prove $S_4/V_4 \cong S_3$ *using* GAP*:*

```
S4:=SymmetricGroup(4);;
NormalSubgroups(S4);
[ Group(()),
Group([ (1,4)(2,3), (1,3)(2,4) ]),
Group([ (2,4,3), (1,4)(2,3), (1,3)(2,4) ]),
Sym( [ 1 ..  4 ] ) ]
V4:=Group((1,2)(3,4),(1,3)(2,4));;
Elements(V4);
[ (), (1,2)(3,4), (1,3)(2,4), (1,4)(2,3) ]
Q:=S4/V4;;
Order(Q);
6
IsomorphismGroups(Q,CyclicGroup(6));
fail
IsomorphismGroups(Q,SymmetricGroup(3));
[ f1, f2 ] -> [ (2,3), (1,2,3) ]
```

Example 3.3.13 (Classification of cyclic groups) *A cyclic group* G *is a group which can be generated by a single element* $g \in G$*, that is,* $G = \langle g \rangle$*. Then*

$$\begin{array}{rcl} \varphi : (\mathbb{Z}, +) & \longrightarrow & \langle g \rangle = G \\ k & \longmapsto & g^k \end{array}$$

is an epimorphism. The order $\operatorname{ord}(g) = |G|$ *can be finite or infinite. In case* $\operatorname{ord}(g)$ *is infinite,* φ *is an isomorphism, since only* $g^0 = e$ *, and every element of* G *is of the form* g^k*. If* $\operatorname{ord}(g)$

is finite, then $\operatorname{Ker}\varphi = \langle n \rangle = n\mathbb{Z}$ *(since every subgroup of* $\mathbb{Z}$ *is of the form* $n\mathbb{Z}$*), and the homomorphism theorem gives*

$$\begin{aligned} \mathbb{Z}/n\mathbb{Z} &\cong \langle g \rangle \\ \overline{k} &\mapsto g^k \end{aligned}$$

So we have shown: Every cyclic group G *of finite order is isomorphic to* $\mathbb{Z}/n\mathbb{Z}$ *with* $n = |G|$*, every cyclic group of infinite order is isomorphic to* $\mathbb{Z}$*.*

3.4 Exercises

Exercise 3.1 *Create paper models of the Platonic solids: tetrahedron, cube, octahedron, dodecahedron and icosahedron (see Figure 3.1).*

Exercise 3.2 *Let* G *be a set with an operation*

$$\begin{array}{rccc} \circ: & G \times G & \longrightarrow & G \\ & (a,b) & \mapsto & a \circ b \end{array}$$

which satisfies the following axioms:

(G1) Associativity

$$a \circ (b \circ c) = (a \circ b) \circ c \ \forall a, b, c \in G.$$

(G2') There is a left-neutral element, that is, there is an

$$e \in G$$

with

$$e \circ a = a \ \forall a \in G.$$

(G3') Existence of the left-inverse, that is, $\forall a \in G \ \exists a^{-1} \in G$ *with*

$$a^{-1} \circ a = e.$$

Show:

1) For $a, b \in G$ *we have: If* $a \circ b = e$*, then also* $b \circ a = e$*.*

2) We have $a \circ e = a$ for all $g \in G$.

3) The neutral element of G is unique.

4) The inverses of the elements of G are unique.

5) For $a, b \in G$ we have $(a \circ b)^{-1} = b^{-1} \circ a^{-1}$.

6) For $a \in G$ we have $(a^{-1})^{-1} = a$.

Exercise 3.3 *Check whether the following definitions give a semigroup, a monoid, or a group:*

1) $\mathbb{R} \cup \{-\infty\}$ with the operation

$$a \heartsuit b = \max\{a, b\},$$

2) $3 + 6\mathbb{Z} = \{3 + 6 \cdot k \mid k \in \mathbb{Z}\}$ with addition,

3) $\mathbb{R}^n$ with the operation

$$(a_1, ..., a_n) + (b_1, ..., b_n) = (a_1 + b_1, ..., a_n + b_n).$$

Exercise 3.4 *Let $\varphi : G_1 \longrightarrow G_2$ be a group homomorphism. Show that:*

1) $\mathrm{Ker}(\varphi) \subset G_1$ and $\mathrm{Bild}(\varphi) \subset G_2$ are subgroups.

2) If φ is a group isomorphism, then the inverse map

$$\varphi^{-1} : G_2 \longrightarrow G_1$$

is a group isomorphism.

Exercise 3.5 *Prove that for $n \geq 2$*

$$\begin{array}{rccl} \mathrm{sign}: & S_n & \longrightarrow & (\{1, -1\}, \cdot) \\ & \sigma & \longmapsto & \mathrm{sign}(\sigma) = \prod\limits_{\substack{i,j=1 \\ i<j}}^{n} \frac{\sigma(i) - \sigma(j)}{i - j} \end{array}$$

is a group epimorphism.

Exercise 3.6 *In the following game, we can shift neighboring squares vertically or horizonally to the empty square. Using such moves, is it possible to transform the configuration*

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

into the standard configuration:

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

Exercise 3.7 *Write*

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 1 & 5 & 6 & 4 & 3 & 7 \end{pmatrix}, \quad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 3 & 4 & 2 & 5 & 7 & 6 \end{pmatrix},$$

$\sigma \circ \tau$ and $\tau \circ \sigma$ both as a product of disjoint cycles, as well as, a product of transpositions. Determine the respective orders and signatures.

Exercise 3.8 *1) Show that, if $a, b \in \mathbb{Z}$ with $a, b \geq 1$ and $\gcd(a, b) = 1$, then*

$$\mathbb{Z}/(a \cdot b) \cong \mathbb{Z}/a \times \mathbb{Z}/b.$$

2) Determine the pre-image of $(8 + 10\mathbb{Z}, -11 + 21\mathbb{Z})$ under the group isomorphism

$$\mathbb{Z}/210 \cong \mathbb{Z}/10 \times \mathbb{Z}/21.$$

Exercise 3.9 *1) Let G be a group and let $x, y \in G$ with $x \cdot y = y \cdot x$ and $\langle x \rangle \cap \langle y \rangle = \{e\}$. Show that:*

$$\operatorname{ord}(x \cdot y) = \operatorname{kgV}(\operatorname{ord}(x), \operatorname{ord}(y)).$$

2) Let

$$\sigma = c_1 \cdot \ldots \cdot c_r \in S_n$$

be the product of disjoint cycles c_i with lengths m_i. Determine $\operatorname{ord}(\sigma)$.

Exercise 3.10 *Which orders occur among the elements of S_6?*

Exercise 3.11 *1) Write every element of S_4 as the product of disjoint cycles.*

2) Assign a partition of 4 to every $\sigma \in S_4$ (that is a sum $4 = p_1 + \ldots + p_r$ with $p_i \geq 1$). This partition is called the cycle type of σ.

3) Interpret each cycle type geometrically by interpreting S_4 as the symmetry group of the tetrahedron (Figure 3.8).

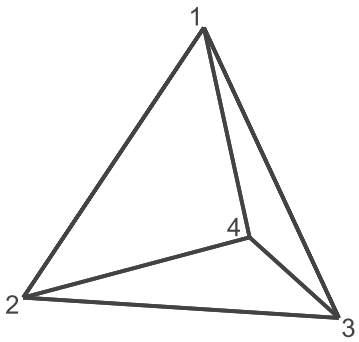


Figure 3.8: Tetraedron

Exercise 3.12 *1) Show that the map*

$$\begin{array}{ccc} G \times G & \longrightarrow & G \\ (a, b) & \longmapsto & a \circ b \circ a^{-1} \end{array}$$

defines a group action, the ***conjugation****, of G on G from the left.*

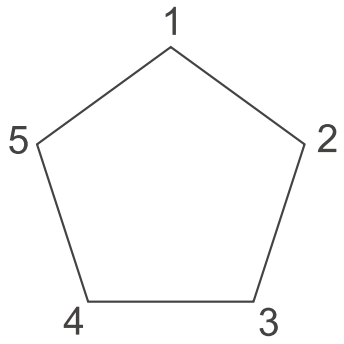


Figure 3.9: Regular 5-gon

2) *The orbit of* $b \in G$

$$b^G := \left\{ a \circ b \circ a^{-1} \mid a \in G \right\}$$

is called the ***conjugacy classes*** *of* b*. Determine all the conjugacy classes of* S_3*.*

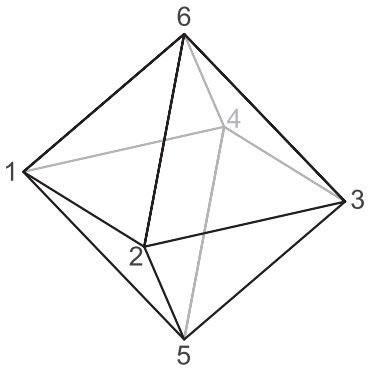
Exercise 3.13 *Let* G *be the symmetry group of the regular pentagon (Figure 3.9). Determine*

1) *the order of* G *(prove your claim),*

2) *all elements of* G *as permutations of the vertices,*

3) *all subgroups of* G *and which thereof are normaldivisors.*

Exercise 3.14 *Let* $G = \mathrm{Sym}(O)$ *be the symmetry group of the octahedron* O*. By numbering the vertices*



of O*, we can consider* G *as a subgroup of* S_6*.*

1) *Find the group order of G with the help of the orbit counting formula.*

2) *Determine generators of G, and prove your claim using* GAP.

3) *Find all conjugacy classes of G using* GAP.

4) *Interpret the elements of G geometrically.*

Hint: Use the GAP *commands* `Group`, `Order` *and* `ConjugacyClasses`.

Exercise 3.15 *Show that there are exactly* 11 *isomorphism classes of (undirected) graphs with* 4 *vertices.*

Exercise 3.16 *Let H be a subgroup of G. Show that if $[G : H] = 2$, then H is a normal subgroup of G.*

Exercise 3.17 *Let $\varphi : G \longrightarrow F$ be a group homomorphism. Prove:*

1) *If $M \subset F$ is a normal subgroup, then $\varphi^{-1}(M) \subset G$ is a normal subgroup.*

2) *If φ is surjective and $N \subset G$ a normal subgroup, then $\varphi(N) \subset F$ is a normal subgroup.*

3) *Give an example of a group homomorphism whose image is not a normal subgroup.*

Exercise 3.18 *Prove that the Kleinian four-group*

$$V_4 = \{(), (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}$$

is a normal subgroup of S_4, and for the quotient group we have

$$S_4/V_4 \cong S_3.$$

Give a geometric interpretation by considering S_4 as the symmetry group of the tetraehedron.

Hint: Every symmetry of the tetrahedron $T \subset \mathbb{R}^3$ with vertices

$$e_1 = (1,-1,-1) \quad e_2 = (-1,1,-1) \quad e_3 = (-1,-1,1) \quad e_4 = (1,1,1)$$

permutes the coordinate axes of $\mathbb{R}^3$, see Figure 3.10. This induces a group homomorphism

$$\varphi : S_4 \to S_3.$$

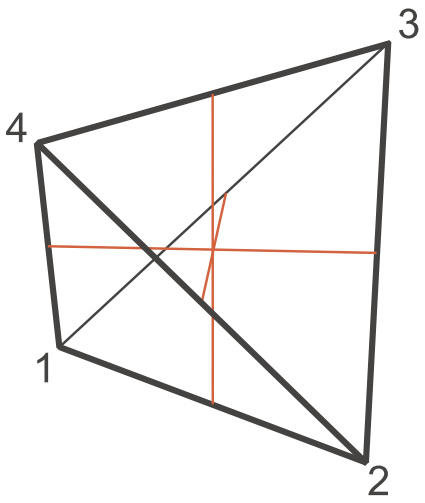


Figure 3.10: Tetrahedron with diagonals connecting mid-points of the edges

Exercise 3.19 *Prove that the Kleinian four-group*

$$V_4 = \{() , (1,2)(3,4) , (1,3)(2,4) , (1,4)(2,3)\}$$

is a normal subgroup of S_4 *and for the quotient group, we have*

$$S_4/V_4 \cong S_3$$

Give a geometric interpretation by considering S_4 *as the symmetry group of the tetraedron.*

Exercise 3.20 *Lrt* G *be the symmetry group of the Ikosaeders.*

1) *Determine the grou order of* G*.*

2) *Find generatofs of the symmetry group* G *of the ikosaederon (Figure 3.11) as a subgroup of* S_{12}*. Prove you claim using* GAP*.*

Exercise 3.21 *Prove:*

1) *I*

$$\sigma = \begin{pmatrix} 1 & \cdots & n-1 & n \\ \sigma(1) & & \sigma(n-1) & k \end{pmatrix} \in S_n,$$

then

$$(n-1,n) \cdot \ldots \cdot (k,k+1) \cdot \sigma \in S_{n-1}.$$

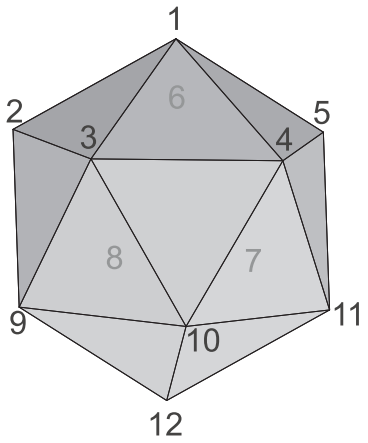


Figure 3.11: Icosahedron with numbering of the vertices

2) The symmetric group S_n is generated by the transpositions $(1,2),(2,3),...,(n-1,n)$, that is

$$S_n = \langle (1,2),(2,3),...,(n-1,n) \rangle .$$

Exercise 3.22 *Let $G \subset S_n$ be a subgroup with $(1,2) \in G$ and $(1,2,...,n) \in G$. Prove that*

$$G = S_n.$$

4

Rings and fields

4.1 Basics

Definition 4.1.1 *A* ***ring*** $(R, +, \cdot)$ *is a set* R *together with two operations*

$$+ : R \times R \longrightarrow R,\ (a, b) \longmapsto a + b$$
$$\cdot : R \times R \longrightarrow R,\ (a, b) \longmapsto a \cdot b$$

for which the following axioms are true

(R1) $(R, +)$ *is an abelian group,*

(R2) multiplication $\cdot$ *is associative,*

(R3) the operations are distributive, that is,

$$a \cdot (b + c) = a \cdot b + a \cdot c$$
$$(a + b) \cdot c = a \cdot c + b \cdot c$$

for all $a, b, c \in R$.

Furthermore if there exists an ***identity****, that is,*

(R4) there is an element $1 \in R$ *with*

$$a \cdot 1 = 1 \cdot a = a$$

for all $a \in R$*, we say that* R *is a* ***ring with 1*** *(as neutral element of the monoid* $(R, \cdot)$ *the* 1 *is unique),*

and if

(R5) the multiplication $\cdot$ is ***commutative****, that is,*

$$a \cdot b = b \cdot a$$

for all $a, b \in R$, then R is called a ***commutative ring****.*

If $\varnothing \neq U \subset R$ with $+$ and $\cdot$ is a ring, then we call U a ***subring*** *of R. If R is a ring with 1, we also require (as a rule) $1 \in U$.*

We write the zero- and identity element as 0_R and 1_R, in case they appear in the context of several rings.

Example 4.1.2 *1) $R = \{0\}$ is a ring with $0 = 1$, the so-called* ***zero-ring****.*

2) $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ are commutative rings with 1.

3) The even numbers $2\mathbb{Z} \subset \mathbb{Z}$ form a commutative ring without 1.

4) If R_1, R_2 are rings, then the cartesian product $R_1 \times R_2$ is a ring with componentwise addition

$$(a_1, a_2) + (b_1, b_2) = (a_1 + b_1, a_2 + b_2)$$

and multiplication

$$(a_1, a_2) \cdot (b_1, b_2) = (a_1 \cdot b_1, a_2 \cdot b_2) .$$

Definition 4.1.3 *Let R and S be rings. a* ***ringhomomorphism***

$$\varphi : R \longrightarrow S$$

is a map, that satisfies

$$\varphi(a + b) = \varphi(a) + \varphi(b)$$

and

$$\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$$

for all $a, b \in R$ (in particular, $\varphi : (R, +) \longrightarrow (S, +)$ is a group homomorphism). If R and S are rings with 1, we require (as a rule) that

$$\varphi(1_R) = 1_S .$$

The concepts mono-, epi-, and isomorphism are defined in a similar way as for groups.

Remark 4.1.4 *The image of* $\varphi(R) \subset S$*, as well as the kernel*

$$\operatorname{Ker}\varphi = \{r \in R \mid \varphi(r) = 0\} \subset R,$$

are subrings.

Remark 4.1.5 *For a ring* R *with* 1*, only in the special case of the zero map,* $\operatorname{Ker}\varphi$ *is also a ring with* 1*, since*

$$1_R \in \operatorname{Ker}\varphi \Leftrightarrow \varphi(r) = \varphi(r \cdot 1_R) = \varphi(r)\cdot\varphi(1_R) = 0 \ \forall r \in R \Leftrightarrow \operatorname{Ker}\varphi = R.$$

This is because $\operatorname{Ker}\varphi$ *is an ideal. In the next section we will come back to ideals.*

Definition 4.1.6 *Let* R *be a commutative ring with* 1*. The* ***polynomial ring*** $R[x]$ *over* R *in the variable* x *is a set of expressions*

$$f = a_0x^0 + a_1x^1 + ... + a_nx^n$$

with $n \in \mathbb{N}_0$*,* $a_i \in R$*,* $a_n \neq 0$*.*

We call call $\deg(f) := n$ *the* ***degree*** *of* f *and put* $\deg(0) = -\infty$*.*

For $i > \deg(f)$ *we put* $a_i = 0$*.*

Addition and multiplication of polynomials are defined as follows.

$$\begin{aligned}&\left(a_0x^0 + a_1x^1 + ... + a_nx^n\right) + \left(b_0x^0 + b_1x^1 + ... + b_mx^m\right)\\ &= \left(a_0 + b_0\right)x^0 + \left(a_1 + b_1\right)x^1 + ... + \left(a_{\max(n,m)} + b_{\max(n,m)}\right)x^{\max(n,m)}\end{aligned}$$

and

$$\begin{aligned}&\left(a_0x^0 + a_1x^1 + ... + a_nx^n\right)\cdot\left(b_0x^0 + b_1x^1 + ... + b_mx^m\right)\\ &= c_0x^0 + c_1x^1 + ... + c_{n+m}x^{n+m}\end{aligned}$$

such that

$$c_k = \sum_{j=0}^{k} a_jb_{k-j}.$$

Polynomial rings in more than one variable are defined inductively

$$R[x_1, ..., x_r] = R[x_1, ..., x_{r-1}][x_r].$$

4.2 The group of units of $\mathbb{Z}/n$

Definition 4.2.1 *Let R be a commutative ring with 1. An element $u \in R$ is called a **unit** of R, if there is a $w \in R$ with*

$$w \cdot u = 1.$$

*The set of units is called $R^\times$. With u also w is a unit and $(R^\times, \cdot)$ is a group, the **group of units** of R.*

If $1 \neq 0$ and

$$R^\times = R \backslash \{0\},$$

*then R is called a **field**.*

Remark: The inverse $w = u^{-1}$ in $R^\times$ is unique.

An element $\overline{a} \in \mathbb{Z}/n$ is invertible if and only if there is a $b \in \mathbb{Z}$ with $\overline{a} \cdot \overline{b} = \overline{1}$, that is, if there are $b, k \in \mathbb{Z}$ with

$$a \cdot b + n \cdot k = 1$$

Such b and k we can obtain using the extended Euclidean algorithm, provided

$$\gcd(a, n) = 1.$$

On the other hand, if we have such a representation of 1, then a and n have to be corpime (since otherwise every common divisor of them also divides 1). We can hence describe the group of units directly:

Theorem 4.2.2 *For $n \in \mathbb{N}$ we have*

$$(\mathbb{Z}/n)^\times = \{\overline{a} \in \mathbb{Z}/n \mid \gcd(a, n) = 1\}$$

*The elements are called **prime residue classes**. The group $(\mathbb{Z}/n)^\times$ we also call the **prime residue class group** modulo n.*

As a direct corollary, we obtain:

Corollary 4.2.3 *The ring $\mathbb{Z}/n$ is a field if and only if n is a prime number.*

Example 4.2.4 *The residue class* $\overline{8} \in \mathbb{Z}/15$ *has an inverse, that is,* $\overline{8} \in (\mathbb{Z}/15)^\times$*, since*

$$\gcd(8, 3 \cdot 5) = 1$$

With the extended Euclidean algorithm, we obtain a representation of the greatest common divisor

$$1 = (2) \cdot 8 + (-1) \cdot 15$$

hence

$$\overline{8}^{-1} = \overline{2}$$

Definition 4.2.5 *The* ***Euler φ-function*** $\varphi : \mathbb{N} \to \mathbb{Z}$ *defined by*

$$\varphi(n) := \left|(\mathbb{Z}/n)^\times\right| = |\{r \in \mathbb{Z} \mid 1 \leq r \leq n,\ \gcd(r, n) = 1\}|$$

gives for n *the order of the group of units* $(\mathbb{Z}/n)^\times$*.*

Theorem 4.2.6 (Theorem of Fermat-Euler) *For all* $a, n \in \mathbb{Z}$*,* $n \geq 1$ *with* $\gcd(a, n) = 1$ *we have*

$$a^{\varphi(n)} \equiv 1 \bmod n.$$

Proof. By Corollary 3.2.52, the order of every element g of a group G divides the group order, hence

$$g^{|G|} = e.$$

Applied to $\overline{a} \in (\mathbb{Z}/n)^\times$ we obtain

$$\overline{a}^{\varphi(n)} = \overline{1}.$$

■

For prime numbers p, we have

$$\varphi(p) = p - 1,$$

hence

$$a^{p-1} \equiv 1 \bmod p \quad \text{if } p \nmid a$$

and thus (since for $p \mid a$ we have $a^p \equiv 0 \equiv a \bmod p$):

Corollary 4.2.7 (Fermat's little theorem) *If p is a prime number and $a \in \mathbb{Z}$, then*

$$a^p \equiv a \bmod p.$$

To compute the Euler φ-function, one uses that it is multiplicative over coprime products. For this, we first note that the Chinese remainder theorem group isomorphism is indeed a ring isomorphism (see Exercise 3.8):

Theorem 4.2.8 *Let $m_1, m_2 \in \mathbb{N}$ be copime. Then*

$$\mathbb{Z}/m_1m_2 \cong \mathbb{Z}/m_1 \times \mathbb{Z}/m_2.$$

Proof. As shown in Exercise 3.8, by

$$\begin{array}{rccc} \pi: & \mathbb{Z}/m_1m_2 & \longrightarrow & \mathbb{Z}/m_1 \times \mathbb{Z}/m_2 \\ & a + m_1m_2\mathbb{Z} & \longmapsto & (a + m_1\mathbb{Z},\ a + m_2\mathbb{Z}) \end{array}$$

we get a well-defined isomorphism of abelian groups with respect to $+$. Moreover

$$\begin{aligned} \pi(ab + m_1m_2\mathbb{Z}) &= (ab + m_1\mathbb{Z},\ ab + m_2\mathbb{Z}) \\ &= ((a + m_1\mathbb{Z}) \cdot (b + m_1\mathbb{Z}),\ (a + m_2\mathbb{Z}) \cdot (b + m_2\mathbb{Z})) \\ &= (a + m_1\mathbb{Z},\ a + m_2\mathbb{Z}) \cdot (b + m_1\mathbb{Z},\ b + m_2\mathbb{Z}) \\ &= \pi(a + m_1m_2\mathbb{Z}) \cdot \pi(b + m_1m_2\mathbb{Z}), \end{aligned}$$

hence π is a ring isomorphism. ■

Example 4.2.9 *Using Theorem 2.4.1 we obtain by determining the solution set of the simultaneous congruences*

$$x \equiv 7 \bmod 15 \iff \begin{cases} x \equiv 1 \bmod 3 \\ x \equiv 2 \bmod 5 \end{cases}$$

According to Theorem 4.2.8 we can rephrase this equivalence as

$$\begin{array}{ccccccc} \mathbb{Z}/15 & \cong & \mathbb{Z}/3 & \times & \mathbb{Z}/5 & \text{and} \\ \overline{7} & \mapsto & (\overline{1} & , & \overline{2}) \end{array}$$

Computing the preimage of $(\overline{1},\overline{2})$ *under this isomorphism is solving the simultaneous congruence*

$$\begin{aligned} x &\equiv 1 \bmod 3 \\ x &\equiv 2 \bmod 5 \end{aligned}$$

Vice versa, computing the image of $\overline{7}$ *is just reduction modulo* 3 *and* 5.

With regard to the multiplication, we have, for example,

$$\begin{aligned} \pi(\overline{7}) \cdot \pi(\overline{4}) = \left(\overline{1},\overline{2}\right) \cdot \left(\overline{1},\overline{4}\right) = \left(\overline{1},\overline{8}\right) = \left(\overline{1},\overline{3}\right) \\ = \pi(\overline{13}) = \pi(\overline{7} \cdot \overline{4}). \end{aligned}$$

By Theorem 4.2.8 the φ-function is multiplicative:

Corollary 4.2.10 *If* $m_1, m_2 \in \mathbb{N}$ *are corpime, then*

$$\varphi\left(m_1 m_2\right) = \varphi\left(m_1\right) \varphi\left(m_2\right).$$

Proof. We have $a + m_1 m_2 \mathbb{Z} \in \left(\mathbb{Z}/m_1 m_2\right)^\times$ if and only if

$$\left(a + m_1\mathbb{Z}, a + m_2\mathbb{Z}\right) \in \left(\mathbb{Z}/m_1 \times \mathbb{Z}/m_2\right)^\times,$$

equivalently, if $a + m_i\mathbb{Z} \in \left(\mathbb{Z}/m_i\right)^\times$ for alle i, since multiplication is defined component-wise. Hence

$$\left(\mathbb{Z}/m_1 m_2\right)^\times = \left(\mathbb{Z}/m_1\right)^\times \times \left(\mathbb{Z}/m_2\right)^\times$$

■

In particular, we obtain:

Remark 4.2.11 *If* $n = p \cdot q$ *is the product of two primes, then*

$$\varphi\left(n\right) = (p-1)(q-1).$$

4.3 Ideals and quotient rings

In this section, we aim at generalizing the construction of the ring $\mathbb{Z}/n$. To do so, we investigate, in which sense we can give the quotient group the structure of a ring. Let R be a commutative ring with 1. Every subgroup $I \subset (R,+)$ is a normal subgroup,

we hence can construct the quotient group R/I, the surjective group homomorphism

$$\begin{array}{rccc} \pi: & (R,+) & \longrightarrow & (R/I,+) \\ & r & \longmapsto & \overline{r} = r + I \end{array}$$

has $\operatorname{Ker}\pi = I$, and the neutral element of R/I with respect to $+$ is $0 + I = I$.

If we want also a multiplication on R/I, such that π is a ring homomorphism, then the multiplication has to be induced by the multiplication in R, since

$$\overline{r_1} \cdot \overline{r_2} = \pi(r_1) \cdot \pi(r_2) = \pi(r_1 r_2) = \overline{r_1 r_2}.$$

However, multiplication by multiplication of the representative may not be well-defined. If $r_2' = r_2 + b$ with $b \in I$ is a different representative of $r_2 + I$, then

$$r_1 \cdot r_2' = r_1 \cdot r_2 + r_1 \cdot b,$$

so we need $r_1 \cdot b \in I$ for all $r_1 \in R$ and $b \in I$. Subgroups of $(R,+)$ with this property are called ideals:

Definition 4.3.1 *Let R be a commutative ring with 1. An **ideal** is a non-empty subset $I \subset R$ with*

$$\begin{aligned} a + b &\in I \\ ra &\in I \end{aligned}$$

for all $a, b \in I$ and $r \in R$.

We remark, that with $a \in I$ also the additive inverse $-a$ is in I.

All together, we have proven (as an easy exercise the distributive law in R/I follows directly from that in R):

Theorem 4.3.2 *Let $I \subset R$ be an ideal. Then the quotient group R/I carries the structure of a commutative ring with 1 by multiplication of representatives*

$$(r_1 + I) \cdot (r_2 + I) := r_1 r_2 + I.$$

*The neutral element of R/I with respect to $\cdot$ is $1 + I$. We call R/I the **quotient ring** of R by I.*

Ideals play an important role in the theory of rings.

Example 4.3.3 *1) If $I_1, I_2 \subset R$ are ideals, then also their intersection $I_1 \cap I_2$.*

2) Let $a_1, ..., a_n \in R$. Then

$$(a_1, ..., a_n) := \{\textstyle\sum_{i=1}^{n} r_i a_i \mid r_i \in R\}$$

*is an ideal, the ideal generated by the **generating system** $a_1, ..., a_n$.*

3) The ideals of $\mathbb{Z}$ are exactly the subgroups

$$n\mathbb{Z} = \{na \mid a \in \mathbb{Z}\} = (n)$$

with $n \in \mathbb{Z}$.

For the ideal $I = n\mathbb{Z} \subset \mathbb{Z}$, we obtain by Theorem 4.3.2, that $\mathbb{Z}/n\mathbb{Z}$ is a commutative ring with 1. The elements are exactly the residue classes $\bar{0}, \bar{1}, ..., \overline{n-1}$, that is,

$$\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/n.$$

4) Let $\varphi : R \longrightarrow S$ be a ring homomorphism. The kernel

$$\operatorname{Ker}\varphi = \{r \in R \mid \varphi(r) = 0\} \subset R$$

is an ideal: If $r' \in R$ and $\varphi(r) = 0$, then also

$$\varphi(r' \cdot r) = \varphi(r') \cdot \varphi(r) = 0$$

As in the case of groups we have:

Theorem 4.3.4 (Homomorphism theorem) *Let $\varphi : R \longrightarrow S$ be a ring homomorphism. Then*

$$R/\operatorname{Ker}\varphi \cong \operatorname{Im}\varphi$$

Proof. From Theorem 3.3.10, we obtain an isomorphism

$$\widetilde{\varphi} : R/\operatorname{Ker}\varphi \longrightarrow \operatorname{Im}\varphi$$
$$\overline{r} = r + \operatorname{Ker}\varphi \longmapsto \varphi(r)$$

of the additive abelian groups. Moreover, $\widetilde{\varphi}$ is a ring homomorphism, since

$$\widetilde{\varphi}(\overline{r_1} \cdot \overline{r_2}) = \widetilde{\varphi}(\overline{r_1 \cdot r_2}) = \varphi(r_1 \cdot r_2)$$
$$= \varphi(r_1) \cdot \varphi(r_2) = \widetilde{\varphi}(\overline{r_1}) \cdot \widetilde{\varphi}(\overline{r_2}).$$

■

4.4 Integral domains and fields

Definition 4.4.1 *Let R be a commutative ring with 1.*

*1) An element $a \in R$ is called a **zero divisor** of R, if there exists an $x \in R \backslash \{0\}$ with*

$$x \cdot a = 0.$$

*2) If R does not have any zero divisors except 0, then R is called an **integral domain**.*

We already have seen, that an element of R cannot be both a unit and a zero divisor.

Example 4.4.2 *1) $\mathbb{Z}$ is an integral domain. The units are $+1$ and -1, hence*

$$\mathbb{Z}^\times = \{+1, -1\}.$$

2) Every field K is an integral domain, for example, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$. The units are $K^\times = K \backslash \{0\}$.

3) $\mathbb{Z}/6 = \{\overline{0}, \overline{1}, ...\overline{5}\}$ is not an integral domain, $\overline{2}, \overline{3}, \overline{4}$ (and $\overline{0}$) are zero divisors, $\overline{1}$ and $\overline{5}$ are units.

See also Exercise 4.2.

4) If R is an integral domain, then also $R[x]$ and

$$R[x]^\times = R^\times$$

are, since if $f \cdot g = 1$, then

$$0 = \deg(1) = \deg(f \cdot g) = \deg(f) + \deg(g)$$

hence $\deg(f) = \deg(g) = 0$.

5) The ring of Gaussian integers

$$\mathbb{Z}[i] = \{a + i \cdot b \mid a, b \in \mathbb{Z}\} \subset \mathbb{C}$$

is an integral domain and

$$\mathbb{Z}[i]^\times = \{1, -1, i, -i\}\,.$$

Clearly these are units:

$$\begin{aligned} 1 \cdot 1 &= 1 \\ (-1) \cdot (-1) &= 1 \\ i \cdot (-i) &= 1 \end{aligned}$$

Prove as an exercise that there are no further units.

Remark 4.4.3 *For integral domains R we can use, similarly to the construction of $\mathbb{Q}$ from $\mathbb{Z}$, the calculation with fractions*

$$Q(R) = \left\{ \frac{a}{b} \mid a, b \in R,\ b \neq 0 \right\}$$

to form a field, the ***quotient field****, see Exercise 4.6.*

For example for a field K we obtain in this way the field of ***rational functions****.*

$$K(x) = Q(K[x]).$$

For finite integral domains, there is no need for the quotient field construction:

Theorem 4.4.4 *Every finite integral domain is a field.*

We prove this in Exercise 4.5. This observation gives another proof of Corollary 4.2.3:

Corollary 4.4.5 *If p is a prime number, then*

$$\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$$

is a field.

Proof. Follows directly from Theorem 4.4.4: If $\overline{a} \cdot \overline{b} = \overline{0}$ for $\overline{a}, \overline{b} \in \mathbb{F}_p$ then $p \mid ab$, hence $p \mid a$ or $p \mid b$, that is, $\overline{a} = \overline{0}$ or $\overline{b} = \overline{0}$. ∎

Remark 4.4.6 *Let K be a field and*

$$\begin{array}{rccc} \chi: & \mathbb{Z} & \longrightarrow & K \\ & n & \longmapsto & n \cdot 1_K \end{array}$$

the characteristic map. The kernel is an ideal

$$\operatorname{Ker} \chi = p\mathbb{Z}$$

with $p \geq 0$. We call

$$\operatorname{char}(K) = p \geq 0$$

*the **characteristic** of K. There are two possible cases:*

1) *$p = 0$, that is, χ is injective. In this case, $\mathbb{Z}$ and hence also $\mathbb{Q}$ is a subring of K.*

2) *$p > 0$. Then*

$$\mathbb{Z}/p\mathbb{Z} \to K$$

is by the homomorphism theorem 4.3.4 injective, hence $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ is a subring of K and thus an integral domain. Hence p must be a prime number, because if $p = a \cdot b$ with $a, b > 1$, then $\bar{a} \cdot \bar{b} = \bar{0}$, hence $\bar{a}, \bar{b} \neq \bar{0}$ are zero divisors.

So every field contains either $\mathbb{Q}$ or $\mathbb{F}_p$.

Remark 4.4.7 *One can show, that up to isomorphism, there is for any prime power p^r exactly one field K with $|K| = p^r$ elements. This field is called $\mathbb{F}_{p^r}$ and has $\operatorname{char}(\mathbb{F}_{p^r}) = p$. See also Exercise 4.4, where we construct a field with 4 elements.*

Caveat:

$$\mathbb{F}_4 \neq \mathbb{Z}/4$$

since $\bar{2} \cdot \bar{2} = \bar{0} \in \mathbb{Z}/4$, that is $\mathbb{Z}/4$ is not an integral domain. In general, $\mathbb{F}_{p^r}$ is constructed as an algebaic extension of $\mathbb{F}_p$.

4.5 Exercises

Exercise 4.1 *Let R ein ring. Show, that for all $x, y \in R$*

$$\begin{aligned} 0x = x0 &= 0 \\ (-x)\,y = x\,(-y) &= -xy \\ (-x)\,(-y) &= xy \end{aligned}$$

Exercise 4.2 *Find the multiplication and addition tables of the ring* $\mathbb{Z}/10\mathbb{Z}$. *Which elements of* $\mathbb{Z}/10\mathbb{Z}$ *are units, which are zero divisors? Find also the multiplication table of the group of units* $(\mathbb{Z}/10\mathbb{Z})^\times$

Exercise 4.3 *Let* K *be a field.*

1) *Show that the set of polynomials* $K[x]$ *with coefficients in* K *and the addition and multiplication from Definition 4.1.6 is an integral domain.*

2) *Implement the addition and multiplication in* $K[x]$.

Exercise 4.4 *Show that there is a field with exactly* 4 *elements by specifying the addition and multiplication tables.*
Hint: Denote the elements of K *by* $0, 1, a, a+1$.

Exercise 4.5 *Show:*

1) *Every integral domain with finitely many elements is a field.*

2) *In a finite ring, every element is either a unit or a zero divisor.*

Exercise 4.6 *Let* R *be an integral domain and* $S = R\backslash\{0\}$. *We construct the ring von fractions*

$$Q(R) = \left\{ \frac{r}{s} \mid r \in R,\ s \in S \right\}$$

as $Q(R) = (R \times S) / \sim$ *with the equivalence relation*

$$(r, s) \sim (r', s') \Leftrightarrow rs' - sr' = 0$$

and write $\frac{r}{s} := [(r, s)]$. *Addition and multiplication are given*

$$\frac{r_1}{s_1} + \frac{r_2}{s_2} = \frac{r_1 s_2 + r_2 s_1}{s_1 s_2}$$
$$\frac{r_1}{s_1} \cdot \frac{r_2}{s_2} = \frac{r_1 r_2}{s_1 s_2}$$

1) *Show: Addition and multiplication are well-defined and* $Q(R)$ *is a field.*

2) *Implement the arithmetic in $\mathbb{Q} = Q(\mathbb{Z})$, that is, addition, multiplication, inverse, a function to decide equality, and a function, which finds for every element a representative which is reduced to lowest terms.*

3) *Can you modify your implementation such that it also works for the field of rational functions $\mathbb{Q}(X) = Q(\mathbb{Q}[X])$?*

Exercise 4.7 *Let R be an integral domain. Show:*

1) *For $a, b, c \in R$, $c \neq 0$ it follows from $ac = bc$, that $a = b$.*

2) *For all $a \in R$ we have $a \mid 0$ and $a \mid a$ and $1 \mid a$.*

3) *Let $a, b, c \in R$. If $c \mid b$ and $b \mid a$, then $c \mid a$.*

4) *If $a \in R$ and $u \in R^\times$ and $a \mid u$, then $a \in R^\times$.*

5) *Let $a, b, d \in R$ with $d \mid a$ and $d \mid b$. Then $d \mid (xa + yb)$ for all $x, y \in R$.*

6) *Let $a, b \in R$. Then $(a) \subset (b) \iff b \mid a$.*

7) *If $a, b \in R$, then*

$$a \mid b \text{ and } b \mid a \iff \exists u \in R^\times \text{ with } a = ub \iff (a) = (b)$$

We then say that, a and b are associated.

This is an equivalence relation.

Exercise 4.8 *Let $\mathbb{F}_2$ be the field with the two elements 0 and 1. Find all elements of*

$$K = \mathbb{F}_2[x]/(x^2 + x + 1)$$

and the addition and multiplication table of K. Show that K is a field.

5

Vector spaces

5.1 Overview

Linear Algebra is concerned with the description of vector spaces, the most frequently occuring structure of mathematics. The reason for this lies in the fact that they arise in the description of the solution spaces of linear systems of equations. We illustrate this at an example: If we want to find the set V of all polynomials

$$f = x_1t^3 + x_2t^2 + x_3t + x_4 \in \mathbb{R}[t]$$

of degree ≤ 3 with zeros in $t = -1$ and $t = 2$ and an inflection point in $t = 0$, we have to find all f with

$$\begin{aligned} f(-1) &= 0 \\ f''(0) &= 0 \\ f(2) &= 0. \end{aligned}$$

The coefficients of f hence must satisfy the system of equations

$$\begin{array}{rcrcrcrcl} -x_1 & + & x_2 & - & x_3 & + & x_4 & = & 0 \\ & & 2x_2 & & & & & = & 0 \\ 8x_1 & + & 4x_2 & + & 2x_3 & + & x_4 & = & 0 \end{array}$$

All these equations are linear (that is of degree 1) in the variables x_i. Such a system, we call a **linear system of equations**. Since none of the equations has a constant term, it is a **homogeneous** linear system of equations.

Definition 5.1.1 *A polynomial $f \in K[x_1, \ldots, x_n]$ is called **homogeneous**, if all terms of f have the same degree.*

Example 5.1.2 *The polynomials $x_1 + x_2$ and $x_1^2 x_2 + x_1 x_2^2$ are homogeneous, $x_1 + 1$ and $x_1^2 x_2 + x_1 x_2$ are not.*

In contrast to general systems of polynomial equations, linear systems can be solved easily.

5.2 Gauß algorithm

Let K be a field. We can manipulate a linear system as follows:

Remark 5.2.1 *If $l_1, l_2 \in K[x_1, \ldots, x_n]$ are polynomials and $0 \neq c \in K$, then for all $x \in K^n$ we have*

$$\left.\begin{array}{l} l_1(x) = 0 \\ l_2(x) = 0 \end{array}\right\} \Longleftrightarrow \left\{\begin{array}{r} l_1(x) = 0 \\ l_2(x) + c \cdot l_1(x) = 0 \end{array}\right.$$

and

$$l_1(x) = 0 \Longleftrightarrow c \cdot l_1(x) = 0$$

and

$$\left.\begin{array}{l} l_1(x) = 0 \\ l_2(x) = 0 \end{array}\right\} \Longleftrightarrow \left\{\begin{array}{l} l_2(x) = 0 \\ l_1(x) = 0 \end{array}\right.$$

Fixing a total ordering on the set of variables, for example, $x_1 > x_2 > \ldots > x_n$, we can use this observation to solve linear systems.

Definition 5.2.2 *If $f = c_s x_s + \ldots + c_n x_n$ with $c_s \neq 0$, then*

$$\mathrm{L}(f) = x_s$$

*is called the **lead variable** (or the lead monomial of f),*

$$\mathrm{LC}(f) = c_s$$

*the **lead coefficient** of f,*

$$\mathrm{LT}(f) = c_s x_s$$

*the **lead term** of f, and*

$$\mathrm{tail}(f) = f - \mathrm{LT}(f) = c_{s+1} x_{s+1} + \ldots + c_n x_n$$

*the **tail** of f.*

Example 5.2.3 *For*

$$f = \mathbf{2x_2} + 5x_3 + x_4$$

we have

$$\begin{aligned} \mathrm{L}(f) &= x_2 \\ \mathrm{LC}(f) &= 2 \\ \mathrm{LT}(f) &= 2x_2 \\ \mathrm{tail}(f) &= 5x_3 + x_4. \end{aligned}$$

Theorem 5.2.4 *For a homogeneous linear system of equations given by $l_1, \ldots, l_r \in K[x_1, \ldots, x_n]$, all $l_i \neq 0$, Algorithm 5.1 finds an equivalent system, such that all equations have pairwise different lead monomials.*

Algorithm 5.1 Gauß algorithm

1: **for all** i **do** $l_i = \frac{1}{\mathrm{LC}(l_i)} \cdot l_i$
2: **while** exist $i \neq j$ with $\mathrm{L}(l_i) = \mathrm{L}(l_j)$ **do**
3: $\quad l_j = l_j - l_i$
4: $\quad$ **if** $l_j = 0$ **then**
5: $\quad\quad$ **delete** l_j
6: $\quad$ **else**
7: $\quad\quad l_j = \frac{1}{\mathrm{LC}(l_j)} \cdot l_j$

Example 5.2.5 *In the above example*

$$\begin{array}{lrcrcrcrcl} l_1 = & \mathbf{-x_1} & + & x_2 & - & x_3 & + & x_4 & = & 0 \\ l_2 = & & & \mathbf{2x_2} & & & & & = & 0 \\ l_3 = & \mathbf{8x_1} & + & 4x_2 & + & 2x_3 & + & x_4 & = & 0 \end{array}$$

the algorithm proceeds as follows:

- $l_1 := -l_1$, $l_2 := \frac{1}{2} l_2$ *and* $l_3 := \frac{1}{8} l_3$

$$\begin{array}{rcrcrcrcl} \mathbf{x_1} & - & x_2 & + & x_3 & - & x_4 & = & 0 \\ & & \mathbf{x_2} & & & & & = & 0 \\ \mathbf{x_1} & + & \frac{1}{2}x_2 & + & \frac{1}{4}x_3 & + & \frac{1}{8}x_4 & = & 0 \end{array}$$

- $l_3 := l_3 - l_1$

$$\begin{array}{rcrcrcrcl} \boldsymbol{x_1} & - & x_2 & + & x_3 & - & x_4 & = & 0 \\ & & \boldsymbol{x_2} & & & & & = & 0 \\ & & \frac{3}{2}\boldsymbol{x_2} & - & \frac{3}{4}x_3 & + & \frac{9}{8}x_4 & = & 0 \end{array}$$

- $l_3 := \frac{2}{3}l_3$

$$\begin{array}{rcrcrcrcl} \boldsymbol{x_1} & - & x_2 & + & x_3 & - & x_4 & = & 0 \\ & & \boldsymbol{x_2} & & & & & = & 0 \\ & & \boldsymbol{x_2} & - & \frac{1}{2}x_3 & + & \frac{3}{4}x_4 & = & 0 \end{array}$$

- $l_3 := l_3 - l_2$

$$\begin{array}{rcrcrcrcl} \boldsymbol{x_1} & - & x_2 & + & x_3 & - & x_4 & = & 0 \\ & & \boldsymbol{x_2} & & & & & = & 0 \\ & & & & -\frac{1}{2}\boldsymbol{x_3} & + & \frac{3}{4}x_4 & = & 0 \end{array}$$

- $l_3 := -2l_3$

$$\begin{array}{rcrcrcrcl} \boldsymbol{x_1} & - & x_2 & + & x_3 & - & x_4 & = & 0 \\ & & \boldsymbol{x_2} & & & & & = & 0 \\ & & & & \boldsymbol{x_3} & - & \frac{3}{2}x_4 & = & 0 \end{array}$$

Remark 5.2.6 *If we sort the l_i according to increasing lead monomal $\mathrm{L}(l_i)$ we obtain the **row echelon form** of the system.*

Example 5.2.7 *In Example 5.2.5 the system is already in row echelon form, while for example*

$$\begin{array}{rcrcrcl} l_1 = & \boldsymbol{x_1} & & & & = & 0 \\ l_2 = & & & & \boldsymbol{x_3} & = & 0 \\ l_3 = & & \boldsymbol{x_2} & & & = & 0 \end{array}$$

ist not.

Remark 5.2.8 *By applying Algorithm 5.2 we can always achieve, that the variable $\mathrm{L}(l_i)$ occurs exactly once in l_i. We then say that the system is in a **reduced row echelon form**.*

Algorithm 5.2 Reduction

1: **while** exist $i \neq j$ with $\mathrm{L}(l_j)$ in $\mathrm{tail}(l_i)$ with coeff c **do**
2: $\quad l_i = l_i - c \cdot l_j$

Example 5.2.9 *In Example 5.2.5 we obtain by* $l_1 := l_1 + l_2$

$$\begin{array}{ccccccc} \boldsymbol{x_1} & & + & x_3 & - & x_4 & = & 0 \\ & \boldsymbol{x_2} & & & & & = & 0 \\ & & & \boldsymbol{x_3} & - & \frac{3}{2}x_4 & = & 0 \end{array}$$

and $l_1 := l_1 - l_3$ *the reduced row echelon form*

$$\begin{array}{ccccccc} \boldsymbol{x_1} & & & & + & \frac{1}{2}x_4 & = & 0 \\ & \boldsymbol{x_2} & & & & & = & 0 \\ & & & \boldsymbol{x_3} & - & \frac{3}{2}x_4 & = & 0 \end{array}$$

Remark 5.2.10 (Solution set) *From the reduced row echelon form, we can read off the solution set of the linear system directly: We solve for the lead variables, while the remaining variables can assume arbitrary values: We first write*

$$V = \{x \in K^n \mid \mathrm{L}(l_i) = -\mathrm{tail}(l_i) \text{ for all } i\}.$$

From this implicit (that is given by equations) representation of the solutoin set, we obtain the ***parametric*** *representation of the solution set, by replacing in the vector* x *the variable* $\mathrm{L}(l_i)$ *by* $-\mathrm{tail}(l_i)$.

Example 5.2.11 *The solution set of Example 5.2.5 is*

$$V = \left\{x \in \mathbb{R}^4 \mid \boldsymbol{x_1} = -\frac{1}{2}x_4,\ \boldsymbol{x_2} = 0,\ \boldsymbol{x_3} = \frac{3}{2}x_4\right\}.$$

The variable x_4 *can assume arbitrary values, while* x_1, x_2, x_3 *are then determined. The parametric form is then*

$$V = \left\{\begin{pmatrix} -\frac{1}{2}x_4 \\ 0 \\ \frac{3}{2}x_4 \\ x_4 \end{pmatrix} \mid x_4 \in \mathbb{R}\right\}$$

Example 5.2.12 *Hence, the set of polynomials*

$$f = x_1t^3 + x_2t^2 + x_3t + x_4 \in \mathbb{R}[t]$$

in Section 5.1 of degree ≤ 3 *with zeros in* $t = -1$ *and* $t = 2$ *and inflection point in* $t = 0$ *is*

$$V = \left\{ -\frac{1}{2}x_4 \cdot t^3 + \frac{3}{2}x_4 \cdot t + x_4 \mid x_4 \in \mathbb{R} \right\}.$$

Figure 5.1 shows the function graphs of some $f \in V$ *(considered as maps* $\mathbb{R} \to \mathbb{R}$, $x \mapsto f(x)$*). In particular, we observe that each such function indeed automatically has in* $t = -1$ *a double zero.*

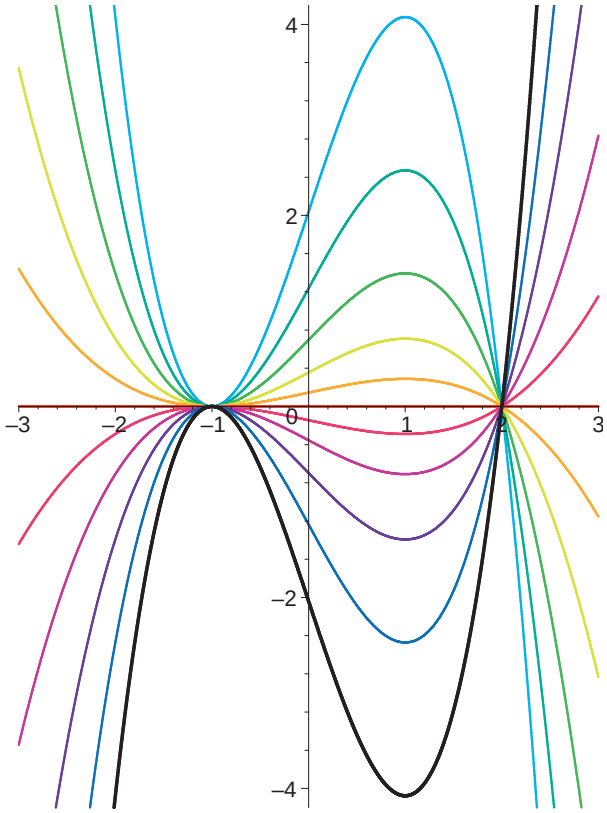


Figure 5.1: Cubic polynomials with zeroes −1 and 2 and inflection point at 0.

We observe that in Example 5.2.11, the elements of V depend only linearly on x_4, hence, we can write

$$V = \{x_4 \cdot f \mid x_4 \in \mathbb{R}\}$$

with

$$f = -\frac{1}{2}t^3 + \frac{3}{2}t + 1.$$

To put it differently, with f also all its $\mathbb{R}$-multiples are in V. This is a more general property of solution sets of linear systems of equations, and motivates the definition of a vector space.

5.3 Vector spaces and bases

Definition 5.3.1 *Let K be a field. A K-**vector space** is a set V together with two operations*

$$\begin{array}{ccccc} V \times V & \longrightarrow & V & & \textit{(addition)} \\ (v, w) & \longmapsto & v + w & & \end{array}$$

$$\begin{array}{ccccc} K \times V & \longrightarrow & V & & \textit{(scalar multiplication)} \\ (\lambda, v) & \longmapsto & \lambda \cdot v & & \end{array}$$

which obey the following axioms:

(V1) $(V, +)$ *is an abelian group,*

(V2) Associativity

$$\lambda \cdot (\mu \cdot v) = (\lambda \cdot \mu) \cdot v$$

for all $\lambda, \mu \in K$ and $v \in V$,

(V3) $1 \cdot v = v$ *for all $v \in V$,*

(V4) Distributive laws

$$(\lambda + \mu) \cdot v = \lambda \cdot v + \mu \cdot v$$
$$\lambda \cdot (v + w) = \lambda \cdot v + \lambda \cdot w$$

for all $\lambda, \mu \in K$ and $v, w \in V$.

*The elements of a vector space we call **vectors**.*

Note that here, we use + both for the addition in K and in V, and $\cdot$ both for the multiplication in K and the scalar multiplication. Which of the two is meant is clear from the type of elements connected by the operation.

Example 5.3.2 *Let K be a field. Examples of K-vector spaces are:*

1) $K^n = \{(a_1, ..., a_n) \mid a_i \in K\}$ *mit*

$$(a_1, ..., a_n) + (b_1, ..., b_n) := (a_1 + b_1, ..., a_n + b_n)$$
$$\lambda\,(a_1, ..., a_n) := (\lambda a_1, ..., \lambda a_n)$$

where we also write elements of K^n as column vectors, that is, as

$$\begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} \in K^n,$$

The neutral element of K^n is the zero vector

$$0 = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$$

2) the polynomial ring $K[x]$,

3) the set of all polynomials up to degree d, denoted $K[x]_{\leq d}$.

Sums and multiples of homogeneous linear systems of equations are again solutions. We hence define:

Definition 5.3.3 *Let V be a K-vector space. A non-empty subset $U \subset V$ is called* ***sub (vector) space****, if*

$$u_1, u_2 \in U \Longrightarrow u_1 + u_2 \in U$$
$$\lambda \in K,\ u \in U \Longrightarrow \lambda \cdot u \in U.$$

Remark 5.3.4 *1) Together with the addition and scalar multiplication, U is again a K-vector space .*

2) Every sub vector space U contains $0 \in V$ (since there is an element $u \in U$ and $0 = 0 \cdot u \in U$).

Theorem 5.3.5 *The solution space of a linear system of equations for $x_1, ..., x_n$ over the field K is a sub vector space of K^n.*

Proof. Consider the system

$$\begin{aligned} a_{1,1}x_1 + ... + a_{1,n}x_n &= 0 \\ &\vdots \\ a_{r,1}x_1 + ... + a_{r,n}x_n &= 0 \end{aligned}$$

over the field K. If $x, y \in K^n$ are solutions, then also $x + y$ and $\lambda \cdot x$ for all $\lambda \in K$:

If $\sum_{j=1}^n a_{i,j}x_j = 0$ and $\sum_{j=1}^n a_{i,j}y_j = 0$ for all $i = 1, ..., r$, then

$$\sum_{j=1}^n a_{i,j}(x_j + y_j) = \sum_{j=1}^n a_{i,j}x_j + \sum_{j=1}^n a_{i,j}y_j = 0$$

and

$$\sum_{j=1}^n a_{i,j}(\lambda \cdot x_j) = \lambda \cdot \sum_{j=1}^n a_{i,j}x_j = 0.$$

■

Example 5.3.6 *1) Sub vector spaces of $\mathbb{R}^3$ are $\{0\}$, the lines through 0, the planes through 0 (exercise) and $\mathbb{R}^3$. We will see later that these are the only sub vector spaces of $\mathbb{R}^3$.*

2) $K[x]_{\leq d} = \{f \in K[x] \mid \deg f \leq d\} \subset K[x]$ is a sub vector space.

3) The sets

$$U_1 = \{(x, y) \in \mathbb{R}^2 \mid y \geq a\}$$

with $a \in \mathbb{R}$ (see Figure 5.2 for $a = 0$) and

$$U_2 = \{(x, y) \in \mathbb{R}^2 \mid y = x^2\}$$

(see Figure 5.3) are no sub vector spaces of $\mathbb{R}^2$. Why?

Definition and Theorem 5.3.7 *Let V be a K-vector sub space and $v_1, ..., v_n \in V$. A vector $v \in V$ is a **linear combination** of $v_1, ..., v_n$, when there are $\lambda_i \in K$ with*

$$v = \lambda_1 v_1 + ... + \lambda_n v_n.$$

The set of all linear combinations

$$\langle v_1, ..., v_n \rangle := \{\lambda_1 v_1 + ... + \lambda_n v_n \mid \lambda_i \in K\} \subset V$$

*is a sub vector space, called the **span of $v_1, ..., v_n$** or the **sub vector space spanned by $v_1, ..., v_n$** .*

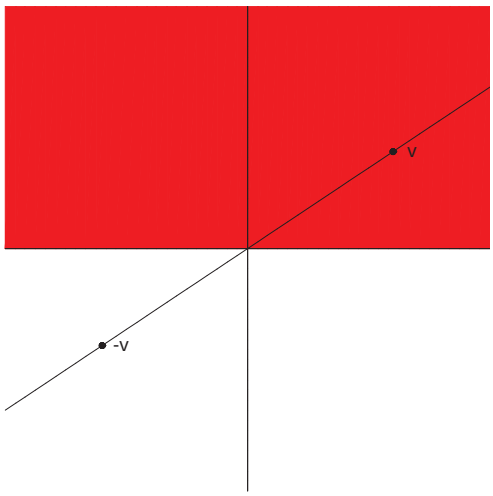


Figure 5.2: Half plane

Proof. If $v, w \in \langle v_1, ..., v_n \rangle$, that is, $v = \sum_{i=1}^{n} \lambda_i v_i$ and $w = \sum_{i=1}^{n} \mu_i v_i$ with $\lambda_i, \mu_i \in K$, then

$$v + w = \sum_{i=1}^{n} (\lambda_i + \mu_i) v_i \in \langle v_1, ..., v_n \rangle$$

and

$$\lambda v = \sum_{i=1}^{n} (\lambda \cdot \lambda_i) v_i \in \langle v_1, ..., v_n \rangle .$$

■

Example 5.3.8 *1) The vectors*

$$v_1 = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \quad v_2 = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} \in \mathbb{R}^3$$

span the plane $E = \{z = 0\}$*, since ever vector in the plane can be written as*

$$E \ni \begin{pmatrix} \lambda_1 \\ \lambda_2 \\ 0 \end{pmatrix} = \lambda_1 v_1 + \lambda_2 v_2.$$

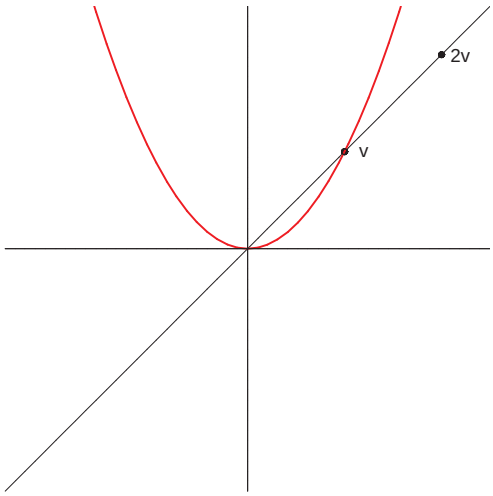


Figure 5.3: Parabola

The vectors

$$w_1 = \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}, \quad w_2 = \begin{pmatrix} 1 \\ -1 \\ 0 \end{pmatrix} \in \mathbb{R}^3$$

also span the plane, so

$$E = \langle v_1, v_2 \rangle = \langle w_1, w_2 \rangle$$

2) The monomials $1, x, ..., x^d \in K[x]$ *span* $K[x]_{\leq d}$.

Definition 5.3.9 *Let* V *be a* K*-vector space.*

1) Vectors $v_1, ..., v_n \in V$ *are called a* ***generating system*** *of* V*, if*

$$V = \langle v_1, ..., v_n \rangle .$$

2) Vectors $v_1, ..., v_n \in V$ *are called* ***linearly independent****, if*

$$\lambda_1 v_1 + ... + \lambda_n v_n = 0$$

implies that

$$\lambda_1 = ... = \lambda_n = 0,$$

otherwise ***linearly dependent****.*

3) A generating system $v_1, ..., v_n$ of V consisting of linearly independent vectors is called a ***basis*** *of V.*

Algorithm 5.3.10 *Vectors $v_1, ..., v_n \in K^m$ are linearly independent if and only if the homogeneous linear system of equations*

$$x_1 v_1 + ... + x_n v_n = 0$$

has only the solution

$$\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$$

This can be decided via the Gauß algorithm.

Algorithm 5.3.11 *A basis of the solution space of a homogeneous linear system of equations is obtained from the parametric representation given in Remark 5.2.10 by substituting a unit basis for the free variables.*

Example 5.3.12 *The system*

$$\begin{array}{lllllllllll} l_1 & = & \boldsymbol{x_1} & + & 2x_2 & & & & - & 2x_5 & = & 0 \\ l_2 & = & & & & \boldsymbol{x_3} & & & + & x_5 & = & 0 \\ l_3 & = & & & & & \boldsymbol{x_4} & + & 2x_5 & = & 0 \end{array}$$

in $\mathbb{Q}[x]$ has already reduced row echelon form, so the solution set in its parametric representation is

$$V = \left\{ \begin{pmatrix} -2x_2 + 2x_5 \\ x_2 \\ -x_5 \\ -2x_5 \\ x_5 \end{pmatrix} \mid x_2, x_5 \in \mathbb{Q} \right\}$$

and we hence obtain a basis by considering $(x_2, x_5) = (1, 0)$ and $(x_2, x_5) = (0, 1)$:

$$V = \left\langle \begin{pmatrix} -2 \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} -2 \\ 0 \\ -1 \\ -2 \\ 1 \end{pmatrix} \right\rangle$$

5.4 Dimension

In this section we will see that any two (finite) bases of a vector space have the same dimension. This number is called the dimension of the vector space, which is the key classifying invariant: Every n-dimensional K-vector space is isomorphic to K^n.

Theorem 5.4.1 *Let V be a K-vector space and $\Omega = (v_1, ..., v_n)$ a list of vectors in V. Then it is equivalent:*

1) Ω is a basis of V.

2) Ω is generating system of V, which cannot be shortened.

3) Ω is system of linearly independent vectors in V, which cannot be extended.

4) Every vector in V can be written in a unique way as a linear combination of the elements of Ω.

Remark 5.4.2 *Let Ω be a finite basis of V. The* ***linear combination map***

$$\begin{array}{rccl} \mathrm{lc}_\Omega : & K^n & \longrightarrow & V \\ & \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} & \longmapsto & a_1 v_1 + ... + a_n v_n \end{array}$$

is bijective. Its inverse

$$\mathrm{co}_\Omega = \mathrm{lc}_\Omega^{-1} : V \longrightarrow K^n$$

is called the ***coordinate representation*** *with resepect to Ω.*

Example 5.4.3 *If we choose for the vector space $V = K[x]_{\leq 2}$ the basis $\Omega = (1, x, x^2)$, we get the bijection*

$$\begin{array}{rccl} \mathrm{lc}_\Omega : & K^3 & \longrightarrow & K[x]_{\leq 2} \\ & \begin{pmatrix} a_0 \\ a_1 \\ a_2 \end{pmatrix} & \longmapsto & a_0 + a_1 x + a_2 x^2 \end{array}$$

The coordinate representation of $3x^2 + x$ *is*

$$\mathrm{co}_\Omega(3x^2 + x) = \begin{pmatrix} 0 \\ 1 \\ 3 \end{pmatrix}$$

Definition 5.4.4 *A vector space is called* ***finite dimenional****, if it has a finite generating system.*

Corollary 5.4.5 *By Theorem 5.4.1, from any finite generating system of a vector space, we can choose a basis. Hence any finite dimenisional vector space has a basis.*

We mention without proof:

Definition and Theorem 5.4.6 (Fundamental theorem) *Let* V *a finite dimensional* K*-vector space. Then any two basis of* V *have the same number of elements.*

This number we call the ***dimension*** $\dim_K V$ *of* V *over* K*.*

If V *is not finite-dimensional, then we set* $\dim_K V = \infty$*.*

Example 5.4.7 *Using Theorem 5.4.6 and the specified basis, we have*

1) *The unit vectors* $e_1, \ldots, e_n$ *are a basis of* K^n*, hence* $\dim K^n = n$*,*

2) *The monomials* $1, \ldots, x^d$ *are a basis of* $K[x]_{\leq d}$*, hence* $\dim K[x]_{\leq d} = d + 1$*,*

3) $\dim K[x] = \infty$*, since any finite set of polynomials only involves polynomials of finite degree.*

4) $\mathbb{R}$ *is a* $\mathbb{Q}$*-vector space of infinite dimension (if* $\mathbb{R}$ *would have finite dimension* n *over* $\mathbb{Q}$*, then there would be a bijective map* $\mathbb{Q}^n \to \mathbb{R}$*. So with* $\mathbb{Q}$ *also* $\mathbb{R}$ *would be countable , a contradiction). Hence* $\dim_{\mathbb{Q}} \mathbb{R} = \infty$ *(but* $\dim_{\mathbb{R}} \mathbb{R} = 1$ *with the basis* $e_1 = 1$*).*

5.5 Vector space homomorphisms

The maps lc_Ω and co_Ω respect the vector space structures on K^n and V, that is, it does not play a role whether we first do a calculation with elements of K^n and then apply lc_Ω or we first apply lc_Ω and then do the respective calculation. Indeed we have

$$\mathrm{lc}_\Omega\left(\begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} + \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix}\right) = \mathrm{lc}_\Omega\begin{pmatrix} a_1+b_1 \\ \vdots \\ a_n+b_n \end{pmatrix} = \sum_{i=1}^{n}(a_i+b_i)\,v_i$$
$$= \sum_{i=1}^{n} a_i v_i + \sum_{i=1}^{n} b_i v_i = \mathrm{lc}_\Omega\begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} + \mathrm{lc}_\Omega\begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix}$$

and

$$\mathrm{lc}_\Omega\left(\lambda \cdot \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}\right) = \mathrm{lc}_\Omega\begin{pmatrix} \lambda a_1 \\ \vdots \\ \lambda a_n \end{pmatrix} = \sum_{i=1}^{n}(\lambda a_i)\,v_i$$
$$= \lambda \sum_{i=1}^{n} a_i v_i = \lambda \cdot \mathrm{lc}_\Omega\begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}.$$

This means that lc_Ω is a Homomorphism of vector spaces:

Definition 5.5.1 *A K-**vector space homomorphism** is a K-linear map $F : V \to W$ of K-vector spaces, that is*

$$F(v_1 + v_2) = F(v_1) + F(v_2)$$

for all $v_i \in V$ and

$$F(\lambda v) = \lambda F(v)$$

for all $v \in V$ and $\lambda \in K$.

The terms Mono-, Epi- and Isomorphism are used analogsly to the cases of groups and rings.

Example 5.5.2

$$\begin{array}{rccl} \mathrm{lc}_{(1,x,\ldots,x^d)}: & K^{d+1} & \longrightarrow & K[x]_{\le d} \\ & \begin{pmatrix} a_0 \\ \vdots \\ a_d \end{pmatrix} & \longmapsto & a_0 + a_1 x + \ldots + a_d x^d \end{array}$$

is a K-vector space isomorphism.

For the classification of finite dimensional vector spaces already the dimension is sufficient:

Theorem 5.5.3 (Classification theorem for vector spaces) *Let V be a K-vector space of dimension $n < \infty$. Then V is isomorphic to K^n. We write*

$$V \cong K^n.$$

Proof. By Remark 5.4.5 and Definition and Theorem 5.4.6 we observe that V has a basis $\Omega = (v_1, ..., v_n)$ with n elements, and by what we have said above

$$\mathrm{lc}_\Omega : K^n \to V$$

is an isomorphism. ■

Definition and Theorem 5.5.4 *A $n \times m$-**matrix** A over K is a table*

$$A = \begin{pmatrix} a_{1,1} & \cdots & a_{1,m} \\ \vdots & & \vdots \\ a_{n,1} & \cdots & a_{n,m} \end{pmatrix} = (a_{i,j})_{\substack{i=1,...,n \\ j=1,...,m}}$$

The set of $n \times m$-matrices with entry-wise addition and scalar multiplication is a K-vector space, which we denote by $K^{n\times m}$.

*By **matrix multiplication***

$$\begin{pmatrix} a_{11} & \cdots & a_{1,m} \\ \vdots & & \vdots \\ a_{n,1} & \cdots & a_{n,m} \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_m \end{pmatrix} := \begin{pmatrix} \left(\sum_{j=1}^m a_{1,j} x_j\right) \\ \vdots \\ \left(\sum_{j=1}^m a_{n,j} x_j\right) \end{pmatrix}$$

a vector space homomorphism

$$K^m \to K^n,\ x \mapsto A \cdot x$$

is given, which we denote again by A. The image of x is just the x_j-linear combination of the columns $A_i \in K^n$ of $A = (A_1 \mid ... \mid A_m)$, that is,

$$(A_1 \mid ... \mid A_m) \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_m \end{pmatrix} = \sum_{j=1}^m x_j \cdot A_j.$$

Proof. The map $A = \mathrm{lc}_{(A_1,\ldots,A_m)}$, which is a homomorphism, as remarked above. ■

Example 5.5.5 *We have*

$$\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix} = \begin{pmatrix} 1\cdot 1 + 2\cdot 2 + 3\cdot 3 \\ 4\cdot 1 + 5\cdot 2 + 6\cdot 3 \end{pmatrix} = \begin{pmatrix} 14 \\ 32 \end{pmatrix}$$

using the formula for matrix multiplication. On the other hand, using the interpretation of the map as a linear combination map we get:

$$\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix} = 1 \cdot \begin{pmatrix} 1 \\ 4 \end{pmatrix} + 2 \cdot \begin{pmatrix} 2 \\ 5 \end{pmatrix} + 3 \cdot \begin{pmatrix} 3 \\ 6 \end{pmatrix} = \begin{pmatrix} 14 \\ 32 \end{pmatrix}$$

Example 5.5.6 *The derivative*

$$\tfrac{d}{dx} : \quad \mathbb{R}[x] \quad \longrightarrow \quad \mathbb{R}[x]$$

is a $\mathbb{R}$-vector space homomorphism, since

$$\frac{d}{dx}\left(\textstyle\sum_{i=0}^{d} a_i x^i\right) = \textstyle\sum_{i=1}^{d} i a_i x^{i-1}$$

and hence the image depends linearly on the coefficients a_i of the input polynomial (check!). It is not a monomorphism since

$$\frac{d}{dx} 0 = \frac{d}{dx} 1,$$

however it is an epimorhpism, since

$$\frac{d}{dx}\left(\textstyle\sum_{i=0}^{d} \frac{a_i}{i+1} x^{i+1}\right) = \textstyle\sum_{i=0}^{d} a_i x^i,$$

that is, every polynomial has a antiderivative.

Definition 5.5.7 *Let $F : V \longrightarrow W$ be a K-vector space homomorphism. For bases $\Omega = (v_1, \ldots, v_m)$ of V and $\Delta = (w_1, \ldots, w_n)$ of W we define a K-vector space homomorphism*

$$M_\Delta^\Omega(F) : K^m \longrightarrow K^n$$

by

$$M_\Delta^\Omega(F) := \mathrm{co}_\Delta \circ F \circ \mathrm{lc}_\Omega \,.$$

So we have a diagram

$$\begin{array}{ccccc} & V & \xrightarrow{F} & W & \\ \mathrm{lc}_\Omega & \uparrow & & \uparrow & \mathrm{lc}_\Delta \\ & K^m & \xrightarrow[M_\Delta^\Omega(F)]{} & K^n & \end{array}$$

that is

$$F = \mathrm{lc}_\Delta \circ M_\Delta^\Omega(F) \circ \mathrm{co}_\Omega$$

We already know how to use the isomorphisms lc_Ω and co_Ω. The key observation is that $M_\Delta^\Omega(F)$ can be realized by matrix multiplication (which, for example, can be easily implemented in a computer):

Theorem 5.5.8 *Let $F : K^m \to K^n$ be a homomorphism and $A = (a_{i,j}) \in K^{n\times m}$ with*

$$F(e_j) = \sum_{i=1}^{n} a_{i,j} e_i$$

that is in the columns of

$$A = (F(e_1) \mid \ldots \mid F(e_m))$$

are the images of the unit basis vectors. Then

$$F(c) = A \cdot c.$$

Proof. For

$$c = \begin{pmatrix} c_1 \\ \vdots \\ c_m \end{pmatrix} \in K^m$$

we have

$$\begin{aligned} F(c) &= F\left(\sum_{j=1}^{m} c_j e_j\right) = \sum_{j=1}^{m} c_j F(e_j) \\ &= A \cdot c. \end{aligned}$$

■

Every homomorphism $F : K^m \to K^n$ is hence given by multiplication by an $n \times m$-matrix A.

Definition 5.5.9 *Using the above notation, we call* $M_\Delta^\Omega(F) \in K^{n\times m}$ *the* ***represenating matrix*** *of* F *with regard to the bases* Ω *of* V *and* Δ *of* W*.*

The representing matrix can now easily be computed:

Remark 5.5.10 *The* i*-th column of* $M_\Delta^\Omega(F)$ *contains the coefficients of the representation of* $F(v_i)$ *with respect to the basis* Δ*.*

Proof. The i-the column of $M_\Delta^\Omega(F)$ is

$$M_\Delta^\Omega(F)(e_i) = (\mathrm{co}_\Delta \circ F \circ \mathrm{lc}_\Omega)(e_i) = (\mathrm{co}_\Delta \circ F)(v_i) = \mathrm{co}_\Delta(F(v_i)),$$

so

$$M_\Delta^\Omega(F) = (\mathrm{co}_\Delta(F(v_1)) \mid \ldots \mid \mathrm{co}_\Delta(F(v_m))) \in K^{n\times m}$$

■

Example 5.5.11 *We consider the derivative*

$$\tfrac{d}{dx}: \quad \mathbb{R}[x]_{\leq 3} \quad \longrightarrow \quad \mathbb{R}[x]_{\leq 2}$$

and and the bases $\Omega = (1, x, x^2, x^3)$ *and* $\Delta = (1, x, x^2)$*. Then*

$$\frac{d}{dx}(x^s) = s \cdot x^{s-1}$$

hence

$$M_\Delta^\Omega(\frac{d}{dx}) = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 3 \end{pmatrix}.$$

Using this, we can now compute, for example,

$$\begin{aligned} \frac{d}{dx}\left(x^3 - 5x^2 + 7x - 11\right) &= \mathrm{lc}_\Delta\left(M_\Delta^\Omega(\frac{d}{dx}) \cdot \mathrm{co}_\Omega\left(x^3 - 5x^2 + 7x - 11\right)\right) \\ &= \mathrm{lc}_\Delta\left(\begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 3 \end{pmatrix} \cdot \begin{pmatrix} -11 \\ 7 \\ -5 \\ 1 \end{pmatrix}\right) \\ &= \mathrm{lc}_\Delta\begin{pmatrix} 7 \\ -10 \\ 3 \end{pmatrix} = 3x^2 - 10x + 7 \end{aligned}$$

The practical implementation of a K-vector space homomorphism $F : V \to W$ in a computer can we hence do as follows: After using co_Δ the convert the input vector in V to a vector in K^m, the actual computation is realized as matrix multiplication with the representing matrix $M_\Delta^\Omega(F)$, and the output is then interpreted as a vector in W using lc_Ω. Here $M_\Delta^\Omega(F)$ can be precomputed and can then be reused for any input vector.

5.6 Exercises

Exercise 5.1 *Let V be a K -vector space and $U \subset V$ a vector sub space. Show:*

1) $(-1) \cdot v = -v$ for all $v \in V$.

2) U is with the addition and skalar multiplication induced by those of V a K-vector space.

Exercise 5.2 *Determine the solutions space $V \subset \mathbb{Q}^5$ and a basis thereof for each of the following linear systems of equations:*

1)

$$\begin{array}{rcrcrcrcrcl} x_1 & + & 2x_2 & + & 2x_3 & - & 2x_4 & - & x_5 & = & 0 \\ -2x_1 & - & 3x_2 & - & x_3 & + & 8x_4 & + & x_5 & = & 0 \\ x_1 & + & 4x_2 & + & 8x_3 & + & 8x_4 & - & 4x_5 & = & 0 \\ 2x_1 & + & 5x_2 & + & 7x_3 & + & 2x_4 & - & 4x_5 & = & 0 \end{array}$$

2)

$$\begin{array}{rcrcrcrcrcl} x_1 & + & x_2 & + & x_3 & + & x_4 & - & x_5 & = & 0 \\ x_1 & + & 2x_2 & + & 3x_3 & + & 4x_4 & - & 5x_5 & = & 0 \\ x_1 & + & 4x_2 & + & 9x_3 & + & 16x_4 & - & 25x_5 & = & 0 \\ x_1 & + & 8x_2 & + & 27x_3 & + & 64x_4 & - & 125x_5 & = & 0 \end{array}$$

Exercise 5.3 *Determine for all $t \in \mathbb{Q}$ a basis of the solution space $V_t \subset \mathbb{Q}^3$ of the homogeneous linear system of equations*

$$\begin{array}{rcrcrcl} -x_1 & + & x_2 & - & 2x_3 & = & 0 \\ x_1 & + & (t-1) \cdot x_2 & + & 2x_3 & = & 0 \\ 2x_1 & + & (t-2) \cdot x_2 & + & (t^2 - t + 4) \cdot x_3 & = & 0 \end{array}$$

Exercise 5.4 *Let*

$$\begin{aligned} l_1 &= a_{1,1}x_1 + \ldots + a_{1,n}x_n = 0 \\ &\vdots \\ l_r &= a_{r,1}x_1 + \ldots + a_{r,n}x_n = 0 \end{aligned}$$

with $a_{i,j} \in \mathbb{Q}$ *a homogeneous linear system of equations. Write a function which*

1) *transforms the system in row echelon form.*
2) *transforms the system in reduced row echelon form.*
3) *finds a basis of the solution space.*

Exercise 5.5 *Let* $d \geq 2$ *and*

$$\mathbb{R}[x]_{\leq d} = \{f \in \mathbb{R}[x] \mid \deg f \leq d\}$$

the vector space of polynomial of degree $\leq d$.

1) *Determine, whether the following sets are sub vector spaces of* $\mathbb{R}[x]_{\leq d}$*:*

$$\begin{aligned} U_1 &= \left\{f \in \mathbb{R}[x]_{\leq d} \mid f(0) = 0\right\} \\ U_2 &= \left\{f \in \mathbb{R}[x]_{\leq d} \mid f(0) = 1\right\} \\ U_3 &= \left\{f \in \mathbb{R}[x]_{\leq d} \mid f(1) = 0\right\} \\ U_4 &= \left\{f \in \mathbb{R}[x]_{\leq d} \mid f'(0) + f''(0) = 0\right\} \\ U_5 &= \left\{f \in \mathbb{R}[x]_{\leq d} \mid f'(0) \cdot f''(0) = 0\right\} \end{aligned}$$

2) *For each* U_i *which is a sub vector space, find a basis.*

Exercise 5.6 *Do the following vectors*

$$\begin{pmatrix} 1 \\ 0 \\ -2 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \\ -3 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \\ -1 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \\ 1 \end{pmatrix} \in \mathbb{R}^4$$

form a basis of $\mathbb{R}^4$*? Proof you claim.*

Exercise 5.7 *Show: For every $b \in \mathbb{R}$ the following $d+1$ polynomials*

$$1, (x-b), (x-b)^2, ..., (x-b)^d \in \mathbb{R}[x]_{\leq d}$$

form a basis of $\mathbb{R}[x]_{\leq d}$.

Exercise 5.8 *Let p be a prime number and $\mathbb{F}_p = \mathbb{Z}/p$ the finite field with p element.*

1) *Show: Ever d-dimensional $\mathbb{F}_p$-vector space V has exactly p^d elements.*

2) *Let $V = (\mathbb{F}_2)^3$ and*

$$v_1 = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} \quad v_2 = \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}$$

Find all elements of the sub vector space $\langle v_1, v_2 \rangle \subset V$ and all vectors $v_3 \in V$, such that v_1, v_2, v_3 form a basis of V.

3) *How many different bases of $(\mathbb{F}_p)^d$ are there? Give a formula.*

Exercise 5.9 *Determine which subsets of*

$$\left\{x^3 + x,\ \ x^2,\ \ x^3,\ \ x^2 + 1,\ \ x,\ \ 1\right\}$$

form a basis of $\mathbb{R}[x]_{\leq 3}$.

Exercise 5.10 *Let K be a field, and let $U, V \subset K^n$ be sub vector spaces given by bases $u_1, ..., u_s$ of U and $v_1, ..., v_t$ of V.*

1) *Show that $U \cap V \subset K^n$ is a sub vector space.*

2) *Describe an algorithm to find a basis of $U \cap V$.*

3) *Apply your method to the sub vector spaces*

$$U = \left\langle \begin{pmatrix} 4 \\ 0 \\ 2 \\ 4 \end{pmatrix}, \begin{pmatrix} 2 \\ 1 \\ 1 \\ 1 \end{pmatrix} \right\rangle \qquad V = \left\langle \begin{pmatrix} 2 \\ 0 \\ 3 \\ 1 \end{pmatrix}, \begin{pmatrix} 4 \\ 3 \\ 2 \\ 3 \end{pmatrix}, \begin{pmatrix} 2 \\ 2 \\ 3 \\ 1 \end{pmatrix} \right\rangle$$

of $\mathbb{Q}^4$.

Index

Bibliography

[1] The Axiom Group: *Axiom*, http://www.axiom-developer.org/ (2012).

[2] M. Artin: Algebra, Birkhäuser (2003).

[3] J. Böhm: Grundlagen der Algebra und Zahlentheorie, Springer (2016).

[4] J. Böhm: Mathematik für Informatiker: Algebraische Strukturen, Lecture Notes (2018).

[5] J. Böhm: Mathematik für Informatiker: Kombinatorik und Analysis, Lecture Notes (2018).

[6] J. Böhm: Mathematik für Informatiker: Analysis, Lecture Notes (2019).

[7] J. Böhm: Mathematik für Informatiker: Kombinatorik, Stochastik und Statistik, Lecture Notes (2019).

[8] S. Bosch: Algebra, Springer (1993).

[9] P. Bundschuh: Einführung in die Zahlentheorie, Springer (1998).

[10] Decker, W.; Greuel, G.-M.; Pfister, G.; Schönemann, H.: SINGULAR *4-1-1 — A computer algebra system for polynomial computations*. http://www.singular.uni-kl.de (2018).

[11] G. Fischer: Lineare Algebra, Vieweg (2010).

[12] G. Fischer, R. Sacher: Einführung in die Algebra, Teubner (1983).

[13] The GAP Group, *GAP – Groups, Algorithms, and Programming, Version 4.8.10*; http://www.gap-system.org, (2018).

[14] Grayson, D. R.; Stillman, M. E.: *Macaulay2, a software system for research in algebraic geometry*, available at http://www.math.uiuc.edu/Macaulay2/ (2019).

[15] G.H. Hardy, E.M. Wright: An introduction to the theory of numbers, Oxford (1956).

[16] J. C. Jantzen, J. Schwermer: Algebra, Springer (2006).

[17] C. Karpfinger, K. Meyberg: Algebra, Spektrum Akademischer Verlag (2008).

[18] E. Kunz: Algebra, Vieweg (1994).

[19] B. Kreußler, G. Pfister: Mathematik für Informatiker: Algebra, Analysis, Diskrete Strukturen, Springer (2009).

[20] Bosma, W.; Cannon J.; Playoust C.: *The Magma algebra system. I. The user language*, J. Symbolic Comput., 24 (1997), 235–265.

[21] Maple (Waterloo Maple Inc.): Maple 2018, http://www.maplesoft.com/ (2018).

[22] Maxima: *Maxima, a Computer Algebra System.* Version 5.25.1, available at http://maxima.sourceforge.net/ (2011).

[23] Wolfram Research, Inc.: *Mathematica Edition: Version 11* (2018).

[24] MATLAB. Natick, Massachusetts: The MathWorks Inc., http://www.mathworks.de/products/matlab/ (2018).

[25] Hearn, A. C.: *REDUCE 3.8*, available at http://reduce-algebra.com/ (2009).

[26] R. Remmert, P. Ullrich: Elementare Zahlentheorie, Birkhäuser (1987).

[27] P. Ribenboim: Die Welt der Primzahlen, Springer (2006).

[28] R. Schulze-Pillot: Einführung in die Algebra und Zahlentheorie, Springer (2008).

[29] V. Shoup: A Computational Introduction to Number Theory and Algebra, Cambridge University Press (2005).

[30] W. Willems: Codierungstheorie und Kryptographie, Birkhäuser (2008).

[31] J. Wolfart: Einführung in die Algebra und Zahlentheorie, Vieweg (1996).

[32] G. Wüstholz: Algebra, Vieweg (2004).