Chapter 1

Number Theory and Algebra

1.1 Introduction

Most of the concepts of discrete mathematics belong to the areas of combinatorics, number theory and algebra. In Chapter **??** we studied the first area. Now we turn our attention to algebra and number theory and introduce the concepts in increasing level of complexity, starting with groups, rings and fields, providing the ring of polynomials as a long example and concluding with vector spaces. In the examples and applications of the theory we obtain almost all the necessary number-theoretic background as well.
The material of this chapter is very standard and can be found in any textbook on algebra or number theory. Some recommended references are:

- K. Ireland, M. Rosen "A Classical Introduction to Modern Number Theory", Springer.
- N. Jacobson, "Basic Algebra", W. H. Freeman.
- S. Lang, "Algebra", Springer.
- S. Lang, "Undergraduate Algebra", Springer.

1.2 Introduction to groups

In the previous chapter we introduced sets. Some of the most familiar sets like the integers or the reals come with more structure. We are used to adding or subtracting numbers to obtain their sum or difference respectively, which is again a number; we note that addition is inverse to subtraction. When we multiply or divide two non-zero reals we obtain another real; we note that multiplication is inverse to division. So there is some similarity between the ways of operating in a set. Algebra is about identifying such common structures and classifying them. One big advantage of this approach is that theorems that can be shown to hold, using only the definition of the abstract concept automatically apply to every concrete instantiation – let it be the integers with the operation addition, the reals with the operation multiplication or, as we will see, the rotations and reflections of an equilateral triangle with the operation of composition.

Definition 1 (Group)
A set G is a group *with respect to the operation $\circ$ if*

1. *G is closed under $\circ$: for all $a, b \in G$ one has $a \circ b \in G$.*
2. *Associativity: for all $a, b, c \in G$ one has $(a \circ b) \circ c = a \circ (b \circ c)$.*
3. *Neutral element: there exists an element $e \in G$ so that for all $a \in G$ one has $a \circ e = e \circ a = a$.*
4. *Inverse: for all $a \in G$ there exists an element $\mathrm{inv}(a) \in G$ with $a \circ \mathrm{inv}(a) = e$ and $\mathrm{inv}(a) \circ a = e$.*

We use $(G, \circ)$ as a shorthand to state that G is a group with respect to $\circ$.
A group G is called commutative *or* abelian *if for all $a, b \in G$ one has*

$$a \circ b = b \circ a.$$

Note that associativity allows any rearrangement of parentheses, e.g.

$$(a \circ b) \circ (c \circ d) = a \circ (b \circ (c \circ d)) = a \circ ((b \circ c) \circ d).$$

The neutral element of a group is unique; assume on the contrary that both e and e' satisfy $a \circ e = e \circ a = a$ and $a \circ e' = e' \circ a = a$ for any group element $a \in G$. Letting e' and then e play the role of a we obtain

$$e' = e \circ e' = e, \text{ i.e. } e = e'.$$

The inverse of an element is unique, i.e. if $\mathrm{inv}(a)$ and $\mathrm{inv}'(a)$ are both inverses of a, then $\mathrm{inv}(a) = e \circ \mathrm{inv}(a) = \mathrm{inv}'(a) \circ a) \circ \mathrm{inv}(a) = \mathrm{inv}'(a) \circ (a \circ \mathrm{inv}(a)) = \mathrm{inv}'(a) \circ e = \mathrm{inv}'(a)$.
The inverse of the neutral element is the neutral element itself since by definition of the inverse element $e \circ \mathrm{inv}(e) = e$ while the definition of the neutral element gives $e \circ \mathrm{inv}(e) = \mathrm{inv}(e)$, so $e = \mathrm{inv}(e)$.
Inversion changes the order of the elements $\mathrm{inv}(a \circ b) = \mathrm{inv}(b) \circ \mathrm{inv}(a)$; we show that by direct computation using associativity:

$$(a \circ b) \circ (\mathrm{inv}(b) \circ \mathrm{inv}(a)) = a \circ (b \circ \mathrm{inv}(b)) \circ \mathrm{inv}(a) = a \circ e \circ \mathrm{inv}(a) = a \circ \mathrm{inv}(a) = e.$$

Applying $\mathrm{inv}(\cdot)$ twice leads to the original element:

$$\mathrm{inv}(\mathrm{inv}(a)) = \mathrm{inv}(\mathrm{inv}(a))(\circ \mathrm{inv}(a) \circ a) = (\mathrm{inv}(\mathrm{inv}(a)) \circ \mathrm{inv}(a)) \circ a = e \circ a = a.$$

Example 2 *The integers $\mathbb{Z}$ form a group with respect to $+$:*

1. *If we add two integers $a, b \in \mathbb{Z}$ the result is again an integer, so the integers are closed under addition.*
2. *Associativity: We have $(a + b) + c = a + (b + c)$.*
3. *Neutral element: Adding 0 to an integer does not change its value and $0 \in \mathbb{Z}$, so $0 \in \mathbb{Z}$ is the neutral element.*

4. *Inverse element: The negative of an integer $a \in \mathbb{Z}$ is again an integer (by the very definition of the integers) and we have $a + (-a) = 0$ and thus* $\mathrm{inv}(a) = -a$.

5. *Since the order of summation does not matter, $a + b = b + a$ for all $a, b \in \mathbb{Z}$, we even have that $\mathbb{Z}$ is commutative.*

The natural numbers $\mathbb{N}$ do not form a group with respect to $+$ since there are no inverse elements. Consider $\mathbb{N}$ as subset of $\mathbb{Z}$; if $a \in \mathbb{N}\backslash\{0\}$, i.e. $a > 0$, then $-a < 0$ and thus not in $\mathbb{N}$ which means that that $\mathbb{N}$ does not fulfill the fourth condition. Sets which are closed under an operation which is associative are referred to as *semigroups*. A *monoid* is a semigroup with a neutral element, so the natural numbers form a monoid. Another example of a monoid is that the integers form a monoid with respect to multiplication since no element other than 1 has an inverse, but $\mathbb{Z}$ is closed under $\cdot$ and the operation is associative.

We now state some very common examples to show that groups are quite familiar objects. We use 'abelian group' and 'commutative group' interchangeably; this is common practice in mathematics.

Example 3 1. *The rationals $\mathbb{Q}$ form an abelian group with respect to $+$.*

2. *The reals $\mathbb{R}$ form an abelian group with respect to $+$.*

3. *The complex numbers $\mathbb{C}$ form an abelian group with respect to $+$.*

4. *The set obtained by removing 0 from $\mathbb{Q}$ is usually denoted by $\mathbb{Q}^* = \mathbb{Q}\backslash\{0\}$. Similarly one defines $\mathbb{R}^*$ and $\mathbb{C}^*$.*

   We observe that the product of two rationals is again rational, that $1 \cdot a = a$, that every fraction $a/b \neq 0$ can be inverted to b/a with $(a/b) \cdot (b/a) = 1$, and that $(a/b) \cdot (c/d) = (c/d) \cdot (a/b)$. So $\mathbb{Q}^*$ is a commutative group with respect to multiplication.

5. *$\mathbb{R}^*$ is a commutative group with respect to multiplication.*

6. *$\mathbb{C}^*$ is a commutative group with respect to multiplication.*

We have not yet defined polynomials. Readers not familiar with this concept should skip this example but for the others it might be enlightening. We provide an extensive study of polynomials over a field in Section 1.8.

Example 4 *The set of polynomials $\mathbb{C}[x]$ in one variable x over the complex numbers $\mathbb{C}$ is a commutative group with respect to coefficientwise addition.*

1. *The set is closed under the operation $+$:*

$$\sum_{i=0}^{n} a_i x^i + \sum_{i=0}^{m} b_i x^i = \sum_{i=0}^{\max\{n,m\}} (a_i + b_i)\, x^i,$$

   where the undefined coefficients a_i for $i > n$ and b_i for $i > m$ are put to zero. The result is again a polynomial and the coefficients are in $\mathbb{C}$, since $\mathbb{C}$ forms a group with respect to the same addition $+$.

2. *Associativity is inherited from* $(\mathbb{C}, +)$ *as*

$$\left(\sum_{i=0}^{n} a_i x^i + \sum_{i=0}^{m} b_i x^i\right) + \sum_{i=0}^{l} c_i x^i = \sum_{i=0}^{\max\{m,n,l\}} ((a_i + b_i) + c_i)\, x^i$$
$$= \sum_{i=0}^{\max\{m,n,l\}} (a_i + (b_i + c_i))\, x^i = \sum_{i=0}^{n} a_i x^i + \left(\sum_{i=0}^{m} b_i x^i + \sum_{i=0}^{l} c_i x^i\right),$$

where the missing coefficients are put to zero.

3. *Neutral element:*

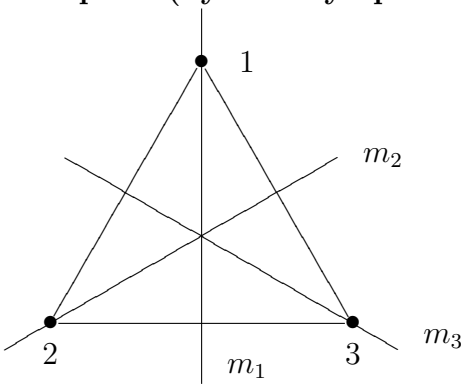
$$e = \sum_{i=0}^{0} 0x^i = 0 \in \mathbb{C}[x].$$

4. *Inverse element: The inverse of* $\sum_{i=0}^{n} a_i x^i \in \mathbb{C}[x]$ *is given by* $\sum_{i=0}^{n} (-a_i) x^i \in \mathbb{C}[x]$.

Example 5 *We consider the set of multiples of* 3*, which is defined by* $3\mathbb{Z} = \{3z \mid z \in \mathbb{Z}\}$. *We now show that this set forms a group under addition.*
Let a *and* b *be in* $3\mathbb{Z}$*, so there exist* $a', b' \in \mathbb{Z}$ *with* $a = 3a'$ *and* $b = 3b'$.

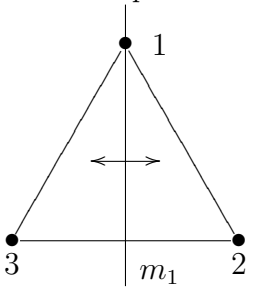
1. $a + b = 3a' + 3b' = 3(a' + b')$ *which is again in* $3\mathbb{Z}$ *as* $3(a' + b')$ *is a multiple of* 3.
2. *Associativity follows from the associativity in* $\mathbb{Z}$.
3. *The neutral element is* 0 *as in the integers. Since* 0 *is divisible by* 3 *we have* $0 \in 3\mathbb{Z}$.
4. *The inverse of* $a = 3a'$ *is* $-a = 3(-a') \in 3\mathbb{Z}$.
5. *Commutativity follows from the commutativity in* $\mathbb{Z}$.

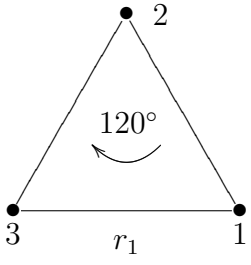
Example 6 (Symmetry operations of equilateral triangle)

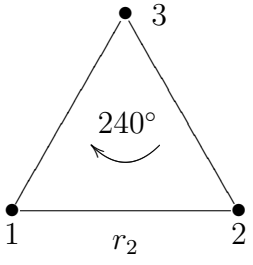


Symmetry operations of the equilateral triangle are maps that do not change the shape of the triangle. There are 6 *different such maps:*
id: identity map,
m_1*: reflection in axis through* 1,
m_2*: reflection in axis through* 2,
m_3*: reflection in axis through* 3,
r_1*: clockwise rotation by* 120° *mapping* 1 *to* 3,
r_2*: clockwise rotation by* 240° *mapping* 1 *to* 2.

For example:







We now investigate whether the set of symmetry operations on the equilateral triangle forms a group with respect to composition. The set is closed under composition: There are no other symmetry operations, so the result of the composition of two operations must again be one of these operations. For further reference we give a table with all results of composing two transformations. The symbol for composition is $\circ$*. We recall that for maps we write* $r_1 \circ m_1$ *if first* m_1 *and then* r_1 *is executed. The table is to be read as follows: each table entry is the result of performing the operation stated in the same row in the leftmost column first, followed by the one in the same column in the top row. E.g.* $r_1 \circ m_1$ *is found in the row of* m_1 *and the column of* r_1 *and equals* m_2*, which can be checked directly.*

$\circ$	id	m_1	m_2	m_3	r_1	r_2
id	id	m_1	m_2	m_3	r_1	r_2
m_1	m_1	id	r_1	r_2	m_2	m_3
m_2	m_2	r_2	id	r_1	m_3	m_1
m_3	m_3	r_1	r_2	id	m_1	m_2
r_1	r_1	m_3	m_1	m_2	r_2	id
r_2	r_2	m_2	m_3	m_1	id	r_1

Proving associativity with such a group table is cumbersome but possible since we have only finitely many group elements. As an example let us check

$$m_1 \circ (m_2 \circ m_1) = m_1 \circ r_1 = m_3 = r_2 \circ m_1 = (m_1 \circ m_2) \circ m_1$$

which shows associativity in this case. The remaining cases can be checked the same way. The table shows that the identity map id is the neutral element of the group.
For each symmetric transformation there exists an inverse one. This can be seen from the table – and by direct inspection. The reflections $m_i = \mathrm{inv}(m_i)$ *are their own inverses while* $\mathrm{inv}(r_1) = r_2$ *and* $\mathrm{inv}(r_2) = r_1$*.*
So the symmetric transformations on a equilateral triangle form a group with respect to $\circ$*. It is commonly called* S_3*, the symmetry group of a triangle. It is interesting to note that* $(S_3, \circ)$ *is not commutative:*

$$m_1 \circ m_2 = r_2 \neq r_1 = m_2 \circ m_1.$$

We will encounter group tables like in the previous example more often in the course. They offer a convenient way of stating group laws for finite groups. For an entertaining example have a look at "Group Theory in the Bedroom – An insomniac's guide to the curious mathematics of mattress flipping" by Brian Hayes which appeared in American Scientist, September-October 2005, volume 93, page 395.

Example 7 *Let* $(G_1, \circ_1)$ *and* $(G_2, \circ_2)$ *be groups. The* Cartesian product $G_1 \times G_2$ of G_1 and G_2 *is defined to be the set*

$$G_1 \times G_2 = \{(a_1, a_2) | a_1 \in G_1, a_2 \in G_2\}.$$

The operation $\circ$ *defined by*

$$(a_1, a_2) \circ (b_1, b_2) = ((a_1 \circ_1 b_1), (a_2 \circ_2 b_2))$$

turns $G_1 \times G_2$ *into a group, called the* direct product of G_1 and G_2 *. The detailed proof is posed as Exercise 27 e) below.*
The same holds for products of finitely many groups.

A useful tool is the cancellation rule.

Lemma 8 (Cancellation rule)
Let $(G, \circ)$ be a group and let $a, b, c \in G$. If $a \circ b = a \circ c$ then $b = c$.

Proof. The proof is posed as Exercise 27 d). □

Definition 9 (Subgroup)
Let $(G, \circ)$ be a group. A subset G' of G is a subgroup of G *if G' is a group with respect to $\circ$.*

Lemma 10 *Let $(G, \circ)$ be a group. A subset $G' \subseteq G$ is a subgroup of G if and only if the following three conditions are satisfied:*

1. *The neutral element e of G is in G'.*
2. *For all $a, b \in G'$ we have $a \circ b \in G'$.*
3. *For all $a \in G'$ we have $\mathrm{inv}(a) \in G'$.*

If G is commutative then so is G'.

Proof. Let $G' \subseteq G$ be a group. Then it must have a neutral element and by the uniqueness of the neutral element we obtain $e \in G'$. The other two conditions are the same as in the definition of a group.
Conversely, let $G' \subseteq G$ satisfy the above conditions. The only condition of the definition that is missing is associativity. We know that G' is contained in G which is associative, so by the associativity of G we have for all $a', b', c' \in G' \subseteq G$ $a \circ (b \circ c) = (a \circ b) \circ c$ which gives associativity in G'. Similarly, if G is commutative then this property is inherited by the subgroup. □

Remark 11 *The converse of the last statement in the lemma does not hold; there are non-commutative groups which have commutative subgroups. See Example 16.*

There is an equivalent version which is sometimes easier to use.

Lemma 12 *Let $(G, \circ)$ be a group. A subset $G' \subseteq G$ is a subgroup of G if and only if the following two conditions are satisfied:*

1. *The neutral element e of G is in G'.*
2. *For all $a, b \in G'$ we have $a \circ \mathrm{inv}(b) \in G'$.*

Proof. Let $G' \subseteq G$ be a group. Like before we get $e \in G'$. For every $b \in G'$ we must have $\text{inv}(b) \in G'$ and since a group is closed and $a, \text{inv}(b) \in G'$ we must have $a \circ \text{inv}(b) \in G'$. Assume now that $G' \subseteq G$ satisfies the conditions. Like in the previous lemma we obtain associativity for G'. We need to show that G' is closed under $\circ$ and that inverses exist in G'. The latter one is seen since $e \in G'$ and by the second condition thus $e \circ \text{inv}(b) = \text{inv}(b) \in G'$. Consequently, for any $a, b \in G'$ we have $a, \text{inv}(b) \in G'$ and by the second condition we obtain $a \circ \text{inv}(\text{inv}(b)) = a \circ b \in G'$, so G' is closed. □

Example 13 *Let G be a group and let $e \in G$ be the neutral element. We have two (trivial) subgroups of G, namely $G_1 = \{e\} \subset G$ and $G_2 = G$ itself. The latter one is clearly a group. Let us check G_1 now. Since $e \circ e = e$ we have $\text{inv}(e) = e$ and so using the criterion from Lemma 12 we only need to see that $e \circ \text{inv}(e) = e \circ e = e$ is indeed in $G_1 = \{e\}$ which obviously holds.*

If we want to exclude the *trivial* subgroups considered in the previous example we speak of *proper subgroups.*

Example 14 *We have seen that $(\mathbb{C}, +)$ forms a group. With Lemma 10, the observation that $0 \in \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$, and checking that in all these sets addition and inversion is closed we get the earlier obtained result that $(\mathbb{Z}, +), (\mathbb{Q}, +)$, and $(\mathbb{R}, +)$ are groups.*

Example 15 *We have seen that $(\mathbb{Z}, +)$ forms a group and that $5\mathbb{Z} \subset \mathbb{Z}$. The neutral element of $\mathbb{Z}$ is 0 which is also in $5\mathbb{Z}$ as $0 = 5 \cdot 0$. Let $a, b \in 5\mathbb{Z}$, i.e. $a = 5a', b = 5b'$. Then*

$$a \circ \text{inv}(b) = a + (-b) = 5a' - 5b' = 5(a' - b') \in 5\mathbb{Z}$$

and so $(5\mathbb{Z}, +)$ forms a subgroup of $(\mathbb{Z}, +)$ by Lemma 12.

Example 16 (Subgroups of S_3)
In Example 6 we considered S_3, the group of symmetric transformations of the equilateral triangle, as an example of a non-abelian group. We now state all subgroups of S_3.
Clearly $(\{id\}, \circ)$ satisfies the criteria of Lemma 12 and thus is a subgroup.
The reflections are self-inverse and thus $(\{id, m_1\}, \circ)$, $(\{id, m_2\}, \circ)$, and $(\{id, m_3\}, \circ)$ are further subgroups.
If we want a subgroup containing r_1 then it must also contain $r_1 \circ r_1 = r_2$ by the second criterion and any combination of them. Since the rotations are inverse to each other and $r_2 \circ r_2 = r_1$ these three elements are sufficient leading to the subgroup $(\{id, r_1, r_2\}, \circ)$.
As soon as we combine two different reflections or one reflection with a rotation and try to obtain a subgroup containing them, the second criterion dictates that we obtain the whole group. Thus the sixth and last subgroup is the full group $(\{id, m_1, m_2, m_3, r_1, r_2\}, \circ) = (S_3, \circ)$.
It is interesting to note that all proper subgroups are commutative while the full group is not.

In the example we constructed subgroups starting from one element $a \in G$ and considering the elements obtained as $a \circ a$ etc. For a natural number $m \in \mathbb{N}$ we introduce the notation

$[m]a$ to denote the m-fold composition of a with itself:

$$[m]a = \underbrace{a \circ a \circ \cdots \circ a}_{m- \text{ copies of } a} .$$

We extend this to negative scalars m as $[m]a = [-m]\mathrm{inv}(a)$ for $m < 0$.
The set of all such scalar multiples of a is denoted by

$$\langle a \rangle = \{[m]a \mid m \in \mathbb{Z}\} .$$

Definition 17 (Cyclic group)
A group $(G, \circ)$ is called a cyclic group *if there exists an element $g \in G$ so that*

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

A group element g with $G = \langle g \rangle$ is called a generator of G.
Let $a \in G$. The set $\langle a \rangle$ is called the cyclic subgroup generated by a.

The following lemma shows that the notion "subgroup" is justified since $\langle a \rangle$ is indeed a subgroup of G.

Lemma 18
Let $(G, \circ)$ be a group and let $a \in G$. The set $\langle a \rangle$ is a commutative subgroup of G.

Proof. The neutral element $e = [0]a$ is contained in $\langle a \rangle$. Since $\mathrm{inv}(a) = [-1]a$ we have $\mathrm{inv}([m]a) = [-m]a$ and

$$[m]a \circ \mathrm{inv}([n]a) = [m]a \circ [-n]a = [m - n]a \in \langle a \rangle$$

as $m - n \in \mathbb{Z}$ and the result follows by Lemma 12.
Since $\mathbb{Z}$ is abelian and $[m]a \circ [n]a = [m + n]a = [n]a \circ [m]a$ also $\langle a \rangle$ is abelian. □

Example 19
1. *Any integer m can be written as $m = 1 + 1 + \cdots + 1 = [m]1$. So the group $(\mathbb{Z}, +)$ is cyclic and generated by 1. Similarly also -1 is a generator.*
2. *$(3\mathbb{Z}, +)$ is cyclic and generated by 3.*
3. *For any integer n the set $(n\mathbb{Z}, +)$ is a cyclic group and generated by n.*
4. *$(\mathbb{Q}, +)$ is not cyclic; one cannot find a generator for this group. It contains $(\mathbb{Z}, +)$ and $(3\mathbb{Z}, +)$ as cyclic subgroups.*
5. *The subgroup $(\{id, r_1, r_2\}, \circ)$ of S_3 is generated by r_1. Another generator is r_2.*

Definition 20 (Order of element)
Let $(G, \circ)$ be a group and let $a \in G$. If there exists an $m \in \mathbb{N}$ such that $[m]a = e$ then a has finite order. *The smallest such m is called the* order of a, *denoted by* $\mathrm{ord}(a) = m$.
If no such number exists then a has infinite order.

Example 21 *In S_3 every element has finite order. Since $m_1 \circ m_1 = id$ we have* $\mathrm{ord}(m_1) = 2 = \mathrm{ord}(m_2) = \mathrm{ord}(m_3)$. *The rotations have order 3 since $r_1 \circ r_1 = r_2 \neq id$ but $r_1 \circ r_1 \circ r_1 = r_2 \circ r_1 = id$.*

Definition 22 (Order of group)
Let $(G, \circ)$ be a group. The order of G *is the cardinality of G.*

If a group has finite order then there are only finitely many elements in it and thus each element must have finite order. The converse does not hold: There are infinite groups which contain elements of finite order.
For discrete mathematics finite groups are particularly interesting. Therefore, we now investigate some details of finite groups. The groups we encounter later on are mostly abelian, so we give some results only for this case. The interested reader may consult any of the algebra books mentioned in the introduction for the general case.
There is a nice connection between the order of a group and the order of an element given by the following lemma.

Lemma 23 *Let $(G, \circ)$ be a finite abelian group of order $|G| = n$.*
For all $a \in G$ one has $[n]a = e$.

Proof. Let $a \in G$. Since G is finite of order n, it can be written as $G = \{a_1, a_2, \ldots, a_n\}$. The results $a \circ a_1,\ a \circ a_2, a \circ a_3, \ldots, a \circ a_n$ are all distinct as from $a \circ a_i = a \circ a_j$ the cancellation rule gives $a_i = a_j$. There are n results, so we can also write G as $G = \{a \circ a_1, a \circ a_2, a \circ a_3, \ldots, a \circ a_n\}$.
We now take the product over all elements of G – the left side in the representation involving a and the right side without – and use that the group is abelian so that we can re-arrange the order of the elements.

$$\begin{aligned}(a \circ a_1) \circ (a \circ a_2) \circ (a \circ a_3) \circ \cdots \circ (a \circ a_n) &= a_1 \circ a_2 \circ a_3 \circ \cdots \circ a_n, \\ ([n]a) \circ (a_1 \circ a_2 \circ a_3 \circ \cdots \circ a_n) &= a_1 \circ a_2 \circ a_3 \circ \cdots \circ a_n.\end{aligned}$$

Using the cancellation rule we obtain

$$[n]a = e$$

which proves the claim. □

The lemma is actually a special case of Lagrange's Theorem (Theorem 46).

Lemma 24 *Let $(G, \circ)$ be a group and let $a \in G$. If $[m]a = e$ then* $\mathrm{ord}(a) \mid m$.
In particular if G is finite with $|G| = n$ then for all $a \in G$ one has $\mathrm{ord}(a) | n$.

Proof. Assume on the contrary that $m = k\,\mathrm{ord}(a) + r$ for $0 < r < \mathrm{ord}(a)$. Then

$$e = [m]a = [k\,\mathrm{ord}(a) + r]a = [k\,\mathrm{ord}(a)]a \circ [r]a = e \circ [r]a = [r]a,$$

so $e = [r]a$ which contradicts the minimality of $\mathrm{ord}(a)$.
By Lemma 23 for all group elements a we have $[n]a = e$. By the first part of the lemma we obtain $\mathrm{ord}(a)|n$. □

The converse of this lemma is not true in general. For $m|\mathrm{ord}(G)$ there need not exist an element $a \in G$ of order m. Only for prime numbers Cauchy's Theorem (Theorem 55) guarantees the existence of an element with that order.
Lagrange's and Cauchy's theorems will both be presented in Section 1.4.

Definition 25 (Exponent)
Let $(G, \circ)$ be a finite group. The smallest $m \in \mathbb{N}$ such that $[m]a = e$ for all $a \in G$ is called the exponent of G.

Example 26 *The symmetry group $(S_3, \circ)$ is finite. The elements have order 2 and 3, therefore $[6]a = id$ for any $a \in S_3$. No smaller integer with this property exists since it must be divisible by 2 and 3, thus S_3 has exponent 6.*

In more generality let $g_1, g_2, \ldots, g_k$ be elements of a group G with orders $m_1, m_2, \ldots, m_k$ respectively. The exponent of G must be divisible by the least common multiple $\mathrm{lcm}(m_1, m_2, \ldots, m_k)$ of the orders.

Exercise 27 *a) Consider the subset $\mathbb{Z}[i]$ of the complex numbers given by*

$$\mathbb{Z}[i] = \{a + bi \in \mathbb{C} \,|\, a, b \in \mathbb{Z}\}.$$

Show that $\mathbb{Z}[i]$ is a subgroup of $(\mathbb{C}, +)$.

b) Find all symmetric transformations of the square and show that they form a group with respect to composition. Give the group table. State all subgroups. Compute the order of this group and the exponent.

c) Find all symmetry operations of a rectangle which is not a square and show that they form a group with respect to composition. Give the group table. State all subgroups. Compute the order of this group and the exponent. You do not need to prove associativity.

d) Prove the cancellation rule, Lemma 8.

e) Let $(G_1, \circ_1)$ and $(G_2, \circ_2)$ be groups. Give all details of the proof that the Cartesian product $G_1 \times G_2$ is a group.

1.3 Modular arithmetic

We briefly pause our algebraic considerations and introduce modular arithmetic in $\mathbb{Z}$ and consider quotient groups in general.
We have seen that the relation $a \sim b \Leftrightarrow 3|(a-b)$ is an equivalence relation. We now study such relations systematically for arbitrary numbers n in place of 3 and introduce names for the different concepts.

Definition 28 (Modulus)
Let n, a, b be integers. If n divides $(a-b)$ we write

$$a \equiv b \bmod n,$$

read "a is equivalent to b modulo n". In such a relation, the integer n is called the modulus.
The equivalence classes under $\equiv$ are called residue classes modulo n.

Example 29 *We have $12 \equiv 27 \bmod 5$ since $12 - 27 = -15$ is divisible by 5.*

Since any number which is divisible by n is also divisible by $-n$ we restrict to positive integers n in most of the following considerations.
We have $a \equiv b \bmod n$ exactly if a and b have the same remainder under division by n, i.e. if we write $a = a'n + r_a$ and $b = b'n + r_b$ with minimal remainders $0 \leq r_a, r_b < n$ then $r_a = r_b$.
We often represent the residue classes by the smallest non-negative integer in the class, i.e. for $0 \leq r < n$ we let

$$\bar{r} = \{a \in \mathbb{Z} | a = a'n + r\},$$

where the notation assumes that the modulus n is fixed.
One can combine the operations $+$ and $\cdot$ with modular reduction. The following lemma shows that this is compatible.

Lemma 30 *Let $a, b, n \in \mathbb{Z}$ with $a = a'n + r_a, b = b'n + r_b$, where the remainders are not necessarily minimal. We have the following equivalences*

1. $(a + b) \equiv (r_a + r_b) \bmod n$,
2. $(a \cdot b) \equiv (r_a \cdot r_b) \bmod n$.

Proof. The proof is left the the reader as Exercise 38 a). □

So we can also define operations $+$ and $\cdot$ on the residue classes and the lemma shows that one can work with any representative of the class.

Example 31 *1. Let $n = 6$. A complete set of residue classes is given by*

$$\{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}.$$

To determine the value of $\bar{3} + \bar{4}$, we find one element in the resulting class, e.g. $3 + 4 = 7$ and then reduce it modulo 6 to find the smallest remainder, here $7 \equiv 1 \bmod 6$. So, as classes: $\bar{3} + \bar{4} = \bar{1}$.

Multiplication works the same: To find the resulting class of $\bar{3} \cdot \bar{4}$ *we multiply the representatives of the classes* $3 \cdot 4 = 12$ *and reduce the result modulo* 6*, so* $\bar{3} \cdot \bar{4} = \bar{0}$.

The complete tables of addition and multiplication of classes look as follows:

$+$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{5}$	$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$

$\cdot$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{0}$	$\bar{2}$	$\bar{4}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{0}$	$\bar{3}$
$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{2}$	$\bar{0}$	$\bar{4}$	$\bar{2}$
$\bar{5}$	$\bar{0}$	$\bar{5}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

The set $\{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}$ *forms an abelian group under addition – the table shows that the set is closed under this operation,* $\bar{0}$ *is the neutral element and each element has an inverse. Associativity and commutativity are inherited from* $\mathbb{Z}$.

The set does not does not form a group under multiplication. The neutral element is $\bar{1}$ *but there are elements that do not have an inverse, namely there are no inverses of* $\bar{0}, \bar{2}, \bar{3}$*, and* $\bar{4}$.

The subset $\{\bar{1}, \bar{5}\}$ *forms a group under multiplication with* $\bar{1}$ *as neutral element and* $\bar{5} \cdot \bar{5} = \bar{1}$.

2. *We now do the same considerations modulo* 3 *and demonstrate, that one can also use other representatives for the classes, e.g.* $\{-\bar{1}, \bar{0}, \bar{1}\}$ *can be used just as well as the more standard choice* $\{\bar{0}, \bar{1}, \bar{2}\}$.

$+$	$-\bar{1}$	$\bar{0}$	$\bar{1}$
$-\bar{1}$	$\bar{1}$	$-\bar{1}$	$\bar{0}$
$\bar{0}$	$-\bar{1}$	$\bar{0}$	$\bar{1}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$-\bar{1}$

$\cdot$	$-\bar{1}$	$\bar{0}$	$\bar{1}$
$-\bar{1}$	$\bar{1}$	$\bar{0}$	$\bar{1}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$-\bar{1}$	$\bar{0}$	$\bar{1}$

We see that $(\{-\bar{1}, \bar{0}, \bar{1}\}, +)$ *and* $(\{-\bar{1}, \bar{1}\}, \cdot)$ *are both abelian groups.*

These examples can be generalized.

Lemma 32 *Let* $n \in \mathbb{Z}$ *be positive. The residue classes modulo* n *form a commutative group with respect to addition, where the addition is defined as*

$$\bar{r}_1 + \bar{r}_2 = \bar{r}_3 \Leftrightarrow r_1 + r_2 \equiv r_3 \bmod n$$

and r_3 *is the unique representative of the class containing* $r_1 + r_2$.

Proof. We first have to show that the operation is well-defined, i.e. that for any element in the class of $\bar{r}_1$ and for any element in the class of $\bar{r}_2$ the result is in the same class $\bar{r}_3$. So let $a \in \bar{r}_1, b \in \bar{r}_2$, then there exist integers a' and b' so that $a = a'n + r_1$ and $b = b'n + r_2$. Their sum is in the class of $a + b = (a'n + r_1) + (b'n + r_2) = (a' + b')n + r_1 + r_2 \equiv r_1 + r_2 \equiv r_3 \bmod n$ by definition of r_3.
The neutral element is $\bar{0}$ and the inverse of $\bar{r}$ is the residue class containing $-r$. If one uses representatives $0 \leq r < n$ then for $r \neq 0$ the inverse is $\overline{n - r}$.

Associativity and commutativity follow from $\mathbb{Z}$. $\square$

The example with $n = 6$ demonstrated that one cannot hope for the same generality for multiplication. Analyzing which elements besides $\bar{0}$ do not have an inverse one sees that those are exactly the elements which have a factor in common with 6.

Lemma 33 *Let $a, n \in \mathbb{Z}$ be integers. The class containing a is invertible modulo n with respect to multiplication $\cdot$ if and only if*

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

Proof. Let $a = a'n + r_a$ with $0 \leq r_a < n$. We first observe that $\gcd(a, n) = \gcd(r_a, n)$ because any divisor of a and n also divides linear combinations of them like $a - a'n = r_a$. Similarly any divisor of r_a and n also divides $a'n + r_a = a$.
Let $b = b'n + r_b$ with $0 \leq r_b < n$ be a candidate multiplicative inverse. Their product is

$$a \cdot b = (a'n + r_a) \cdot (b'n + r_b) = (a'b'n + a'r_b + b'r_a)n + r_a r_b.$$

Let $r_a r_b$ be in the residue class of $0 \leq r_c < n$. By the same considerations, $\gcd(a, n)$ also divides $r_a r_b$ and r_c. So if $\gcd(a, n) = k \neq 1$ is non-trivial then k divides r_c which therefore cannot be 1 no matter which b is chosen.
Now let $\gcd(a, n) = 1$. Let $\{r_0, r_1, \ldots, r_{n-1}\}$ be a complete set of remainders modulo n. The products $a \cdot r_i$ are all different modulo n; because if $a \cdot r_i \equiv a \cdot r_j \bmod n$ then $n|a(r_i - r_j)$ and since $\gcd(a, n) = 1$ it must be that $n|(r_i - r_j)$ which by the size restrictions implies $r_i = r_j$. This means that there is one r_l such that $ar_l \equiv 1 \bmod n$ and so a is invertible. $\square$

Definition 34 (Euler φ-function)
Let $n \in \mathbb{Z}$ be positive. We define the Euler φ-function $\varphi(n)$ *of n as the number of integers a with $0 \leq a < n$ and $\gcd(a, n) = 1$.*

Sometimes the Euler φ-function is also called *Euler's totient function.*

Example 35

1. *We have $\varphi(7) = 7 - 1 = 6$ since all positive integers < 7 are coprime to 7.*

2. *Let p be a prime. Like in the previous example we have $\varphi(p) = p - 1$.*

3. *Let $n = p^2$ be the square of a prime. The integers $0 \leq a < n$ which have $\gcd(a, n) \neq 1$ are exactly the multiples of p, i.e. $p, 2p, 3p, \ldots, (p-1)p$. There are $p^2 - 1 - (p-1) = p(p-1)$ numbers $0 \leq a < n$ with $\gcd(a, n) = 1$.*

4. *Let $n = pq$ be the product of two different primes p and q. The integers a with $1 \leq a \leq pq - 1$ and $\gcd(a, n) \neq 1$ are multiples of p or q, precisely the numbers $p, 2p, 3p, \ldots, (q-1)p, q, 2q, 3q, \ldots (p-1)q$. I.e. there are $pq - 1 - (q-1) - (p-1) = pq - p - q + 1 = (p-1)(q-1)$ positive integers coprime to pq and smaller than pq.*

The Euler φ-function is a typical function of elementary number theory. The examples in Example 35 can be generalized to the following lemma which we will not prove here but in Section 1.5 after stating the Chinese Remainder Theorem 79.

Lemma 36 *Let $n = p_1^{e_1} p_2^{e_2} p_3^{e_3} \cdots p_r^{e_r}$ with $p_1, p_2, \ldots, p_r$ distinct primes and positive exponents $e_1, e_2, \ldots, e_r \in \mathbb{Z}$. We have*

$$\varphi(n) = \prod_{i=1}^{r} (p_i^{e_i} - p_i^{e_i - 1}) = n \cdot \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right).$$

The following lemma gives a nice illustration of the use of modular reduction in proofs.

Lemma 37 *For any nonzero $a, b \in \mathbb{Z}$ there exist $m, n \in \mathbb{Z}$ with $|m| < |b|$ and $|n| < |a|$ so that*

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

Proof. Let $d = \gcd(a, b)$. For simplicity assume that a and b are positive. Put $p = a/d$ and $q = b/d$, then p and q are coprime. The $q - 1$ multiples $p, 2p, 3p, \ldots, (q-1)p$ of p are all not divisible by q and all in distinct residue classes modulo q. Since there are $q - 1$ non-zero residue classes modulo q one of the multiples, say pm, is in the class of 1 modulo q, i.e. $pm \equiv 1 \bmod q$. This implies $1 = pm + qn$ for some $1 \leq n < p$. Multiplying both sides of this equation by d we obtain the desired equation $d = am + bn$, where $1 \leq m < q \leq b$ and $1 \leq n < p \leq a$. For negative values of a or b similar considerations hold. □

This representation is often called *Bézout's identity* and is obtained using the *Extended Euclidean Algorithm* **??** which we will state later in this chapter and consider in detail in Chapter **??**. It is possible to extend Bézout's identity to give a linear combination of any number of elements.

Exercise 38 *a) Prove Lemma 30.*

b) Write addition and multiplication tables for arithmetic modulo 4 and modulo 8. How many elements are invertible modulo 4 and modulo 8 respectively.

c) Compute $\varphi(1001)$. You may use Lemma 36.

1.4 Advanced concepts of groups

Modular arithmetic as considered in the previous section is one example of considering one group modulo a subgroup, in this case the group $\mathbb{Z}$ modulo $n\mathbb{Z}$ for some integer n. In this section we generalize the approach and show some properties of the resulting constructs. The whole section is rather technical and the proofs can be skipped on first reading but the results will be needed in later sections and chapters.
Let $(G, \circ)$ be a group and let G' be a subgroup. We define a relation $\sim$ on G by

$$a \sim b \Leftrightarrow a \circ \mathrm{inv}(b) \in G'. \tag{1.1}$$

We observe that $\sim$ is an equivalence relation as it is

reflexive: $a \sim a$ as $a \circ \text{inv}(a) = e \in G'$ since G' is a subgroup.

symmetric: If $a \sim b$ then also $b \sim a$, because with $a \circ \text{inv}(b) = c \in G'$ also $\text{inv}(c) = \text{inv}(a \circ \text{inv}(b)) = b \circ \text{inv}(a)$ must be in G' by the second criterion in Lemma 12.

transitive: If $a \sim b$ and $b \sim c$ then also $a \sim c$ because $a \circ \text{inv}(c) = a \circ (\text{inv}(b) \circ b) \circ \text{inv}(c) = (a \circ \text{inv}(b)) \circ (b \circ \text{inv}(c))$ must be in G' as combination of the two group elements $a \circ \text{inv}(b)$ and $b \circ \text{inv}(c)$.

The set of equivalence classes is denoted by G/G' and we have

$$G/G' = \{a \circ G' | a \in G\}.$$

Example 39 *In Example 31 we considered* $\mathbb{Z}/6\mathbb{Z}$ *and* $\mathbb{Z}/3\mathbb{Z}$.

Lemma 40 *Let* $(G, \circ)$ *be an abelian group and let* G' *be a subgroup. The set of equivalence classes* G/G' *forms an abelian group under the operation*

$$\circ' : (a \circ G') \circ' (b \circ G') = (a \circ b) \circ G'$$

inherited from G.

Proof. We first need to show that the operation is well defined on the classes. Let $a' \in a \circ G'$ and $b' \in b \circ G'$, so there exist $c, d \in G'$ so that $a' = a \circ c$ and $b' = b \circ d$. The result of $a' \circ b'$ is

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

where in the last step we used associativity and commutativity of G and that $c \circ d \in G'$. So the resulting class is independent of the chosen representative.
The set G/G' is closed under $\circ'$, associativity and commutativity are inherited from G. The neutral element is $G' = e \circ G'$ since $(a \circ G') \circ' (e \circ G') = (a \circ e) \circ G' = a \circ G'$. The inverse element to $a \circ G'$ is $\text{inv}(a) \circ G'$. □

Because $\circ'$ is so closely related to $\circ$ we drop the extra notation and use the same symbol $\circ$ for the group operation in G/G'.

Definition 41
Let $(G, \circ)$ *be an abelian group and let* G' *be a subgroup. The group* $G/G' = \{a \circ G' | a \in G\}$ *is called the* quotient group *of* G *modulo* G'.

With this theoretical background, the earlier proven fact that $(\mathbb{Z}/n\mathbb{Z}, +)$ is a group follows as an easy corollary from Lemma 40.

Example 42 *In Example 13 we saw that every group* G *has trivial subgroups, namely* $G_1 = \{e\}$ *and* $G_2 = G$. *The first one leads to equivalence classes which contain only one element each, since* $a \sim b$ *requires* $a \circ \text{inv}(b) \in G_1$, *i.e.* $a \circ \text{inv}(b) = e$ *and thus* $a = b$. *This means that* $G/\{e\}$ *behaves like* G *itself.*
The same considerations for G_2 *show that there is only one equivalence class which contains all of* G, *so the quotient group* G/G *has only one element.*

The integers are not a group with respect to multiplication, so we cannot use this lemma to deduce anything about $\mathbb{Z}/n\mathbb{Z}$ under multiplication. Example 31 showed that there are subsets of $\mathbb{Z}/n\mathbb{Z}$ of elements that are invertible modulo n and that these subsets formed groups.

Definition 43 (Multiplicative group modulo n)
Let $n \in \mathbb{N}$. We denote by $(\mathbb{Z}/n\mathbb{Z})^\times$ the set of multiplicatively invertible elements modulo n. By Lemma 33 we have with unique representatives for the equivalence classes

$$(\mathbb{Z}/n\mathbb{Z})^\times = \{a + n\mathbb{Z} \mid 0 \leq a < n, \gcd(a, n) = 1\}.$$

Lemma 44 *Let $n \in \mathbb{Z}$. The set $(\mathbb{Z}/n\mathbb{Z})^\times$ forms a commutative group under multiplication. It is called the* multiplicative group modulo n. *We have $|(\mathbb{Z}/n\mathbb{Z})^\times| = \varphi(n)$.*

Proof. We use the definition and Lemma 33. Let $a + n\mathbb{Z}, b + n\mathbb{Z} \in (\mathbb{Z}/n\mathbb{Z})^\times$, i.e. $\gcd(a, n) = \gcd(b, n) = 1$. Since ab is coprime to n, so is the remainder of ab modulo n and thus the set is closed under multiplication. Associativity and commutativity follow from the same properties in $\mathbb{Z}$. The neutral element is $1 + n\mathbb{Z}$ which is clearly in the set. By definition, the a's are exactly those integers which are invertible modulo n and so there exists a b with $ab \equiv 1 \bmod n$ and $(a + n\mathbb{Z})^{-1} = b + n\mathbb{Z}$. The second claim follows from the definition of the Euler φ-function. □

Since $\varphi(n)$ is the cardinality of the multiplicative group modulo n we get Fermat's little theorem as a corollary of Lemma 23

Corollary 45 (Fermat's Little Theorem)
Let $n \in \mathbb{Z}$. For all $a \in (\mathbb{Z}/n\mathbb{Z})^\times$ one has $a^{\varphi(n)} \equiv 1 \bmod n$.

The proof of the following theorem is rather technical and can be skipped on first reading. However, the result is important.

Theorem 46 (Lagrange's Theorem)
Let $(G, \circ)$ be a finite group of order $|G| = n$.
Let G' be a subgroup of G. The order of G' divides n.

Proof. We use again the equivalence relation (1.1) $a \sim b$ if and only if $a \circ \mathrm{inv}(b) \in G'$ and decompose G into disjoint equivalence classes

$$G = H_1 \cup H_2 \cup \cdots \cup H_k,$$

for some number k. Since G' is closed under $\circ$, the equivalence class of any $b \in G'$ equals G' and so we can assume $H_1 = G'$.
For each equivalence class we can define a bijection between it and G'. Let $c \in H_i$ for some $1 \leq i \leq k$, i.e.

$$H_i = \{a \in G | c \circ \mathrm{inv}(a) \in G'\}$$

and this gives us a map

$$\psi_c : H_i \to G',\ a \mapsto c \circ \mathrm{inv}(a).$$

By the definition of H_i we have $c \circ \mathrm{inv}(a) \in G'$ and so the map indeed maps to G'. It is easy to give the inverse map $\psi_c^{-1}$of ψ_c as

$$\psi_c^{-1} : G' \to H_i,\ b \mapsto \mathrm{inv}(b) \circ c.$$

Indeed

$$\psi_c^{-1}(\psi_c(a)) = \psi_c^{-1}(c \circ \mathrm{inv}(a)) = \mathrm{inv}(c \circ \mathrm{inv}(a)) \circ c = a \circ \mathrm{inv}(c) \circ c = a$$

and

$$\psi_c(\psi_c^{-1}(b)) = \psi_c(\mathrm{inv}(b) \circ c) = c \circ \mathrm{inv}(\mathrm{inv}(b) \circ c) = c \circ \mathrm{inv}(c) \circ b = b.$$

So $|H_i| = |G'|$ for any $1 \leq i \leq k$ and from the above partition we have

$$|G| = |H_1| + |H_2| + \cdots + |H_k| = k \cdot |G'|$$

which proves the claim. □
So we have that the order of any subgroup divides the group order.
The ψ_c's in the previous proof were maps between sets. We now consider maps that respect the group operation.

Definition 47 (Group homomorphism)
Let $(G_1, \circ_1)$ and $(G_2, \circ_2)$ be two groups and let $\psi : G_1 \to G_2$ be a map between them. It is a group homomorphism *(or* homomorphism*) if for all $a_1, b_1 \in G_1$ one has*

$$\psi(a_1 \circ_1 b_1) = \psi(a_1) \circ_2 \psi(b_1).$$

A group homomorphism is an isomorphism *if it is bijective.*
Two groups G_1, G_2 are isomorphic*, written $G_1 \cong G_2$, if there exists an isomorphism between them.*

Example 48
1. *The map $[3] : \mathbb{Z} \to 3\mathbb{Z},\ a \mapsto 3a$ is a group homomorphism between $(\mathbb{Z}, +)$ and $(3\mathbb{Z}, +)$. First we observe that the map is well-defined since each element of $\mathbb{Z}$ is indeed mapped into $3\mathbb{Z}$. Since for all integers a and b we have $3(a + b) = (3a) + (3b)$ the map is a homomorphism. It is easy to give the inverse map $[1/3] : 3\mathbb{Z} \to \mathbb{Z}, a \mapsto a/3$. This map is actually well-defined since any $a \in 3\mathbb{Z}$ is divisible by 3. So in fact $\mathbb{Z}$ and $3\mathbb{Z}$ are isomorphic $\mathbb{Z} \cong 3\mathbb{Z}$.*

2. *Let $(G, \circ)$ be a group. For any integer n the map*

$$[n] : G \to G,\ a \mapsto [n]a$$

is a group homomorphism. Clearly, $[n]a \in G$ for any $a \in G$ and by the definition of $[n]$ it is a homomorphism.

A group homomorphism might map some elements to the neutral element in the target group. These elements will play a special role later on.

Definition 49 (Image and kernel of homomorphism)
Let $(G_1, \circ_1)$ *and* $(G_2, \circ_2)$ *be two groups and let* $\psi : G_1 \to G_2$ *be a group homomorphism. The* image of ψ, *denoted* $\mathrm{Im}(\psi)$, *is the subset of* G_2 *defined by*

$$\mathrm{Im}(\psi) = \{\psi(a_1) \in G_2 | a_1 \in G_1\}.$$

The kernel of ψ, *denoted* $\mathrm{Ker}(\psi)$, *is the subset of* G_1 *that is mapped to the neutral element* e_2 *of* G_2

$$\mathrm{Ker}(\psi) = \{a_1 \in G_1 | \psi(a_1) = e_2\}.$$

Theorem 50 (First isomorphism theorem) *Let* $(G_1, \circ_1)$ *and* $(G_2, \circ_2)$ *be abelian groups and let* $\psi : G_1 \to G_2$ *be a group homomorphism. The kernel of* ψ *is a subgroup of* G_1 *and* $\mathrm{Im}(\psi) \cong G_1/\mathrm{Ker}(\psi)$.

Proof. We use Lemma 12. Since $e_1 \circ_1 a_1 = a_1$ for any $a_1 \in G_1$ and by the definition of homomorphisms we have

$$\psi(a_1) = \psi(e_1 \circ_1 a_1) = \psi(e_1) \circ_2 \psi(a_1).$$

By the cancellation rule we get $\psi(e_1) = e_2$, the neutral element in G_2. So $e_1 \in \mathrm{Ker}(\psi)$.
We remark that for $a_1 \in G_1$ we have $\psi(\mathrm{inv}_1(a_1)) = \mathrm{inv}_2(\psi(a_1))$, where the first inverse is with respect to $\circ_1$ and the second one with respect to $\circ_2$, as $e_2 = \psi(e_1) = \psi(a_1 \circ_1 \mathrm{inv}_1(a_1)) = \psi(a_1) \circ_2 \psi(\mathrm{inv}_1(a_1))$.
Let $a_1, b_1 \in \mathrm{Ker}(\psi)$, i.e. $\psi(a_1) = \psi(b_1) = e_2$. We see that

$$\psi(a_1 \circ_1 \mathrm{inv}_1(b_1)) = \psi(a_1) \circ_2 \psi(\mathrm{inv}_1(b_1)) = e_2 \circ_2 \mathrm{inv}_2(\psi(b_1)) = \mathrm{inv}_2(e_2) = e_2$$

and so $a_1 \circ_1 \mathrm{inv}_1(b_1) \in \mathrm{Ker}(\psi)$.
To prove the isomorphism we construct a homomorphism between the sets and show that an inverse map exists. Let

$$\psi' : G/\mathrm{Ker}(\psi) \to \mathrm{Im}(\psi),\ \psi'(a_1 \circ \mathrm{Ker}(\psi)) = \psi(a_1).$$

By definition of $\mathrm{Im}(\psi)$ indeed ψ' maps to $\mathrm{Im}(\psi)$ and the map is well-defined since for $k \in \mathrm{Ker}(\psi)$ we have $\psi'((a_1 \circ k) \circ \mathrm{Ker}(\psi)) = \psi(a_1 \circ k) = \psi(a_1) \circ \psi(k) = \psi(a_1)$ and so the image is independent of the representative. Since ψ is a homomorphism so is ψ'. If $a_2 \in \mathrm{Im}(\psi)$ there must exist an $a_1 \in G$ with $a_2 = \psi(a_1)$; a_1 is unique up to elements from $\mathrm{Ker}(\psi)$: If $\psi(a_1) = \psi(b_1) = a_2$ then $\psi(b_1 \circ \mathrm{inv}_1(a_1)) = \psi(b_1) \circ \mathrm{inv}_2(\psi(a_1)) = e_2$ and so $b_1 \circ \mathrm{inv}_1(a_1) \in \mathrm{Ker}(\psi)$ and a_1 and b_1 are in the same residue class modulo $\mathrm{Ker}(\psi)$. This allows to define the inverse map $(\psi')^{-1} : \mathrm{Im}(\psi) \to G/\mathrm{Ker}(\psi)$ as $(\psi')^{-1}(a_2) = a_1 \circ \mathrm{Ker}(\psi)$ if $\psi(a_1) = a_2$. □

Example 51 *Let* $\psi : G \to H$ *be an isomorphism, i.e.* ψ *is injective and so* $\mathrm{Ker}(\psi) = \{e\}$ *and surjective, i.e.* $\mathrm{Im}(\psi) = H$. *Theorem 50 says that*

$$H = \mathrm{Im}(\psi) \cong G/\{e\} \cong G,\ \textit{i.e. } H \cong G$$

which we knew already from ψ *being an isomorphism. So the lemma fits with our expectation.*

Example 52 *Let $(G, \circ)$ be a group. The elements of order n for some integer n form a group as they are the kernel of the homomorphism*

$$[n] : G \to G,\ a \mapsto [n]a.$$

Definition 53 (Product of groups)
Let $(G, \circ)$ be a group and let G' and G'' be subgroups of G. The set

$$G'G'' = \{a' \circ a'' | a' \in G', a'' \in G''\}$$

is called the product of G' and G''.

Lemma 54 *Let $(G, \circ)$ be an abelian group and let G' and G'' be subgroups of G. The product $G'G''$ is a subgroup of G and*

$$|G'G''| = |G'| \cdot |G''|/|G' \cap G''|.$$

Proof. We use Lemma 12. Since G' and G'' are subgroups of G they both contain e and thus $e = e \circ e \in G'G''$.
Let $a', b' \in G'$ and $a'', b'' \in G''$. We show that with $a' \circ a'' \in G'G''$ and $b' \circ b'' \in G'G''$ also $(a' \circ a'') \circ \text{inv}(b' \circ b'')$ is in $G'G''$. Since G is abelian we can rearrange the last expression to

$$(a' \circ a'') \circ \text{inv}(b' \circ b'') = (a' \circ \text{inv}(b')) \circ (a'' \circ \text{inv}(b'))$$

and use that $(a' \circ \text{inv}(b')) \in G'$ and $(a' \circ \text{inv}(b')) \in G''$ so that the result is indeed in $G'G''$.
To prove the statement about the cardinality of $G'G''$ we consider the following map between the Cartesian product $G' \times G''$ and $G'G''$:

$$\psi : G' \times G'' \to G'G'',\ (a', a'') \mapsto a' \circ \text{inv}(a'').$$

Since all groups involved are abelian and subgroups of G, this is a group homomorphism and in particular $G'G'' = \text{Im}(\psi)$. The kernel consists of

$$\text{Ker}(\psi) = \{(a', a'') \in G' \times G'' | a' \circ \text{inv}(a'') = e\},$$

in other words of the tuples (a, a) such that $a \in G' \cap G''$ and so the proof follows by Theorem 50 and taking cardinalities. □

The next theorem provides a partial inverse to Lagrange's Theorem. The proof needs all the concepts introduced so far.

Theorem 55 *Cauchy's Theorem*
Let $(G, \circ)$ be a finite abelian group of order n and let p be a prime dividing n.
There exists an element $a \in G$ with $\text{ord}(a) = p$. *The subgroup generated by this a is cyclic of order p.*

Proof. Let $G = \{g_1, g_2, \ldots, g_n\}$ and consider the finite product of groups $P_m = \langle g_1\rangle\langle g_2\rangle\langle g_3\rangle\cdots\langle g_m\rangle$ for some $m \leq n$, which by $m-1$-fold application of Lemma 54 is a subgroup of G. By the same lemma the cardinality is

$$|P_m| = |\langle g_1\rangle||\langle g_2\rangle||\langle g_3\rangle|\cdots|\langle g_m\rangle|/k_m,$$

where k_m is an integer taking care of the cardinalities of the intersections.
By construction P_n contains all g_i and since P_n is a subgroup of G we actually have $G = P_n$, so we get

$$|G| = |P_n| = |\langle g_1\rangle||\langle g_2\rangle||\langle g_3\rangle|\cdots|\langle g_n\rangle|/k_n.$$

Since p is a prime and divides $|G|$ it must also divide the product on the right hand side, and by the primality it must divide one of the factors $|\langle g_i\rangle|$ for one $1 \leq i \leq n$. Let $c = |\langle g_i\rangle|/p$ and put $a = [c]g_i$. By construction $[p]a = [p]([c]g_i) = [\mathrm{ord}g_i]g_i = e$ and $a \neq e$. □

Corollary 56 *Every finite abelian group of prime order is cyclic.*

Proof. Let $|G| = p$ be a prime. There exists an element $g \in G$ of order $\mathrm{ord}(g) = p$ and thus $G = \langle g\rangle$. □

Example 57 *Let $(G, \circ)$ be a cyclic group of order m. How many generators does G have?*
Since G is cyclic there exists a generator g, so let $G = \langle g\rangle = \{[n]g \mid n \in \mathbb{Z}\}$. For any $a = [n]g \in G$ we have $[m]a = [n]([m]g) = e$ but if n has a non-trivial common divisor with m then a $\mathrm{ord}(a) < n$. So there are exactly $|\{0 \leq n < m \mid \gcd(n, m) = 1\}| = \varphi(m)$ generators.

Example 58 *In Exercise 38 we considered the multiplicative group modulo 8 and found that $(\mathbb{Z}/8\mathbb{Z})^\times = \{\bar{1}, \bar{3}, \bar{5}, \bar{7}\}$ has order 4. The multiplication table shows that there is no element of order 4 but that the orders are $\mathrm{ord}(\bar{1}) = 1, \mathrm{ord}(\bar{3}) = 2, \mathrm{ord}(\bar{5}) = 2, \mathrm{ord}(\bar{7}) = 2$. This structure – a non-cyclic group of order 4 – is a famous example in the theory of finite groups. It is called the* Klein four-group.

Exercise 59 *a) Let $(G, \circ)$ be a group and let G_1, G_2 be two subgroups of it. Show that their intersection is also a subgroup of G.*
In fact one can even show that the intersection of arbitrarily many subgroups is a subgroup.

b) Consider the group $(\mathbb{Z}/12\mathbb{Z}, +)$. Find all subgroups. Note that Lagrange's Theorem helps to determine possible group orders.

c) The multiplicative group $(\mathbb{Z}/299\mathbb{Z})^\times$ is of order $(13-1)(23-1) = 264$ which is divisible by 11. Find an element of order 11.

d) Let G be a group of order $13 \cdot p$, where p is a prime. State a randomized algorithm to find an element of order p in G.

1.5 Rings

We have seen that the integers form an abelian group with respect to addition and only a semigroup with respect to multiplication and we have seen other sets on which we can define more than one operation. Such structures are called rings if they satisfy some extra conditions. The integers are a particularly familiar example of a ring. In the following section we study fields, which are rings in which both are sets which are closed under two different operations.

Definition 60 (Ring)
A set R is a ring *with respect to two operations $\circ, \diamond$ denoted by $(R, \circ, \diamond)$ if*

1. *$(R, \circ)$ is an abelian group.*
2. *$(R, \diamond)$ is a semi-group (closed under $\diamond$ and the associative rule holds).*
3. *The distributive laws hold in R:*

   Let $a, b, c \in R$. Then we must have

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

If there exists a neutral element $e_\diamond$ with respect to $\diamond$ then R is called a ring with unity.
If $\diamond$ is commutative in R then R is called a commutative ring.

Example 61 *The integers $(\mathbb{Z}, +, \cdot)$ form a ring. We have already seen that $(\mathbb{Z}, +)$ is an abelian group and that $(\mathbb{Z}, \cdot)$ is a semi-group. It remains to be shown that the distributive laws hold. We first observe that multiplication is commutative as can be seen in rearranging $a \cdot b = b + b + \cdots + b$ (a times) and $b = 1 + 1 + \cdots + 1$ (b times) to $a \cdot b = b \cdot a$. This implies that only one of the two laws need to be checked explicitly.*
By definition and commutativity of $(\mathbb{Z}, +)$ we have $a \cdot (b + c) = (b + c) + \cdots + (b + c) = (b + \cdots + b) + (c + \cdots + c) = ab + ac$.
The number 1 is the neutral element with respect to multiplication since $1 \cdot a = a \cdot 1 = a$.
To sum up, the integers form a commutative ring with unity.

Example 62

1. *The rational numbers $(\mathbb{Q}, +, \cdot)$, the reals $(\mathbb{R}, +, \cdot)$ and the complex numbers $(\mathbb{C}, +, \cdot)$ form commutative rings with 1.*
2. *Let $n \in \mathbb{N}$. The set $n\mathbb{Z}$ of multiples of n forms a ring with addition and multiplication as in $\mathbb{Z}$: associativity, commutativity, and the distributive laws follow from $\mathbb{Z}$. We have shown that $(n\mathbb{Z}, +)$ is a group. The only thing we need to check is that the set is closed under multiplication which holds since $an \cdot bn = (abn)n$ is a multiple of n.*
3. *In Example 4 we considered the additive group of polynomials $\mathbb{C}[x]$ over $\mathbb{C}$. We can define multiplication of polynomials by*

$$\left(\sum_{i=0}^{n} a_i x^i\right) \cdot \left(\sum_{i=0}^{m} b_i x^i\right) = \sum_{i=0}^{n+m} \left(\sum_{j=0}^{i} a_j b_{i-j}\right) x^i,$$

where $a_i = 0$ for $i > n$ and $b_i = 0$ for $i > m$. The set $\mathbb{C}[x]$ is closed under multiplication since all coefficients are again in $\mathbb{C}$. Associativity can be checked by direct computation and follows from associativity in $\mathbb{C}$. The polynomial $1 \in \mathbb{C}[x]$ is the neutral element with respect to multiplication and the operation is commutative. So, $\mathbb{C}[x]$ is a commutative ring with unity. We study polynomial rings in more detail in Section 1.8.

4. *Let $n \in \mathbb{N}$ and consider the set $\mathbb{Z}/n\mathbb{Z}$. We have seen in Lemma 32 that $(\mathbb{Z}/n\mathbb{Z}, +)$ is an abelian group. Multiplication of residue classes is well-defined and closed by Lemma 30. Associativity follows from associativity of $(\mathbb{Z}, \cdot)$. The residue class $1 + n\mathbb{Z}$ is the neutral element of multiplication. Commutativity and distributive laws are inherited from $(\mathbb{Z}, \cdot)$. So $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ is a commutative ring with unity for any n.*

5. *Let $(R, \circ_R, \diamond_R)$ and $(S, \circ_S, \diamond_S)$ be rings. The Cartesian product $R \times S$ is defined by*

$$R \times S = \{(r, s) | r \in R, s \in S\}.$$

With the operations $\circ$ and $\diamond$ defined by

$$\begin{aligned} (r_1, s_1) \circ (r_2, s_2) &= ((r_1 \circ_R r_2), (s_1 \circ_S s_2)) \\ (r_1, s_1) \diamond (r_2, s_2) &= ((r_1 \diamond_R r_2), (s_1 \diamond_S s_2)) \end{aligned}$$

the Cartesian product $R \times S$ is a ring. If both R and S are commutative rings then so is $R \times S$; if both are rings with unity then so is $R \times S$.

This example can be generalized to arbitrarily many rings.

In a ring we have the following useful computation laws which we know very well for the integers.

Lemma 63 *Let $(R, \circ, \diamond)$ be a ring and let $e_\circ$ be the neutral element with respect to $\circ$. If R is a ring with unity, let $e_\diamond$ be the neutral element of $\diamond$. We have for arbitrary $a, b \in R$:*

1. $e_\circ \diamond a = a \diamond e_\circ = e_\circ$.
2. $\mathrm{inv}_\circ(e_\diamond) \diamond a = a \diamond \mathrm{inv}_\circ(e_\diamond) = \mathrm{inv}_\circ(a)$.
3. $\mathrm{inv}_\circ(a) \diamond b = a \diamond \mathrm{inv}_\circ(b) = \mathrm{inv}_\circ(a \diamond b)$.

Proof. By the distributive laws we have

$$(e_\circ \diamond a) \circ (e_\circ \diamond a) = (e_\circ \circ e_\circ) \diamond a = e_\circ \diamond a = (e_\circ \diamond a) \circ e_\circ.$$

By the cancellation rule, Lemma 8, it follows that

$$e_\circ \diamond a = e_\circ.$$

Similarly one proves $a \diamond e_\circ = e_\circ$.

For the second result we use the definitions of $e_\circ$ and $e_\diamond$, the first result and the distributive laws on

$$e_\circ = e_\circ \diamond a = (e_\diamond \circ \mathrm{inv}_\circ(e_\diamond)) \diamond a = (e_\diamond \diamond a) \circ (\mathrm{inv}_\circ(e_\diamond) \diamond a) = a \circ (\mathrm{inv}_\circ(e_\diamond) \diamond a)$$

and add $\mathrm{inv}_\circ(a)$ on both sides from the left giving $\mathrm{inv}_\circ(a) = \mathrm{inv}_\circ(e_\diamond) \diamond a$ as claimed. The proof for $a \diamond \mathrm{inv}_\circ(e_\diamond) = \mathrm{inv}_\circ(a)$ follows along the same lines.
The last result follows from the second and associativity

$$\mathrm{inv}_\circ(a) \diamond b = (a \diamond \mathrm{inv}_\circ(e_\diamond)) \diamond b = a \diamond (\mathrm{inv}_\circ(e_\diamond) \diamond b) = a \diamond \mathrm{inv}_\circ(b)$$

and

$$\mathrm{inv}_\circ(a) \diamond b = (\mathrm{inv}_\circ(e_\diamond) \diamond a) \diamond b = \mathrm{inv}_\circ(e_\diamond) \diamond (a \diamond b) = \mathrm{inv}_\circ(a \diamond b).$$

□

Definition 64 (Divisibility)
Let $(R, \circ, \diamond)$ be a ring and let $a, b \in R$. We say that a divides *b, written $a|b$, if there exists $c \in R$ with*

$$a \diamond c = b.$$

Definition 65 (Domain, zero-product property)
Let $(R, \circ, \diamond)$ be a ring with unity. It is called a domain *if $e_\circ \neq e_\diamond$ and there are no zero divisors, i.e. if*

$$a \diamond b = e_\circ \text{ implies } a = e_\circ \text{ or } b = e_\circ.$$

This last property is called the zero-product property*.*

Definition 66 (Greatest common divisor)
Let R be a commutative ring and let $a, b \in R$. A greatest common divisor $\gcd(a, b)$ of a and b *is a common divisor of a and b so that for all common divisors c of a and b one has that $c|d$.*

In the integers we have that if $a|b$ then also $-a|b$ and the factorization of an integer is unique only up to factors of -1 – even though one usually restricts to positive primes. In general rings, greatest common divisors and factorizations can be unique only up to invertible elements from R.

Definition 67 (Units)
Let $(R, \circ, \diamond)$ be a commutative ring with unity $e_\diamond$. An element $a \in R$ is called a unit *if there exists an element $b = \mathrm{inv}_\diamond(a) \in R$ so that $a \diamond b = e_\diamond$.*
The set of units in R is denoted by $R^\times$ and we have

$$R^\times = \{a \in R | \text{ there exists an element } b \in R \text{ so that } a \diamond b = e_\diamond\}.$$

Example 68 *The invertible elements in $(\mathbb{Z}/n\mathbb{Z}, \cdot)$ are exactly the elements in the multiplicative group modulo n, so the notation $(\mathbb{Z}/n\mathbb{Z})^\times$ is consistent with these elements being the units in $(\mathbb{Z}/n\mathbb{Z}, \cdot)$.*

Lemma 69 *Let $(R, \circ, \diamond)$ be a commutative ring with unity $e_\diamond$. The set of units $R^\times$ of R forms a group under $\diamond$.*

Proof. Left to the reader as Exercise 4. □

Lemma 70 *Let $(R, \circ, \diamond)$ be a domain and let $e_\circ \neq a, b \in R$. If $a|b$ and $b|a$ then there exists a unit $u \in R^\times$ so that $a = b \diamond u$.*

Proof. By the definition of divisibility, $a|b$ and $b|a$ imply that there exist $c, d \in R$ with $b = a \diamond c$ and $a = b \diamond d$. The combination leads to

$$a \diamond e_\diamond = a = b \diamond d = (a \diamond c) \diamond d = a \diamond (c \diamond d).$$

Using distributive laws this gives $a \diamond (e_\diamond \circ \mathrm{inv}_\circ(c \diamond d)) = e_\circ$. Since R is a domain and $a \neq e_\circ$, the zero-product property gives $e_\diamond \circ \mathrm{inv}_\circ(c \diamond d)) = e_\circ$, i.e. $e_\diamond = c \diamond d$, and so $c, d \in R^\times$ are units. □

Modular arithmetic (cf. Section 1.3) is about computing with remainders of division by an integer n. For the integers it is very easy to find unique representatives for the residue classes, namely one uses the non-negative integers $< n$ to represent their respective classes and all classes are distinct. In general one cannot hope to find a canonical representative for each class and so rings in which we can define a division with remainder in a unique way deserve a special name.

Definition 71 (Euclidean domain)
Let $(R, \circ, \diamond)$ be a commutative domain and let $v : R \backslash \{e_\circ\} \to \mathbb{Z}_+$ be a function. The ring R is called a Euclidean domain *with respect to v if for each $a, b \in R$ with $b \neq e_\circ$ one can find $q, r \in R$ with*

$$a = q \diamond b \circ r \text{ and } r = e_\circ \text{ or } v(r) < v(b).$$

In Euclidean domains any two elements have a greatest common divisor and one can give an algorithm to determine it. The method to find greatest common divisors makes extensive use of the following lemma.

Lemma 72 *Let $(R, \circ, \diamond)$ be a Euclidean domain. Let $a, b, q, r \in R$ with $a = q \diamond b \circ r$. The set of common divisors of a and b equals the set of common divisors of b and r.*

Proof. Let $d|a$ and $d|b$ which implies that $d|(a \circ \mathrm{inv}_\circ(q \diamond b))$, i.e. $d|r$ and so every divisor of a and b also divides r. Reversing the same argument gives that every common divisor f of b and r also divides the linear combination $q \diamond b \circ r = a$. □

As a shorthand we speak of computing modulo b when using the remainder r of division by b instead of a itself, so we write $a \equiv r \bmod b$ and speak of r as the remainder. Since R is Euclidean we can find a remainder r such that $v(r) < v(b)$ or $r = e_\circ$. We use $(a \bmod b)$ to denote this (smallest) remainder.
Repeated application of this lemma leads to remainders r_i with strictly decreasing values under v and since v maps to the non-negative integers this process must eventually lead to a remainder $r_j = 0$. This recursive algorithm is known as *Euclidean algorithm* and will be studied in much more algorithmic detail in Chapter **??**.

Lemma 73 *Let $(R, \circ, \diamond)$ be a Euclidean domain. For any two elements $a, b \in R$ there exists a greatest common divisor $d = \gcd(a, b)$ and d is unique up to units from $R^\times$.*

Proof. The sequence of values $v(r_i)$ of the remainders r_i in the following algorithm is strictly decreasing and consists of non-negative integers so it must terminate which means that $r_j = e_\circ$ for some j. By Lemma 72 we have that each two consecutive remainders r_{i-1} and r_i have the same common divisors as a and b. Since $r_j = e_\circ$ the common divisors of a and b are the same as those of r_{j-1} and $e_\circ$. These are precisely all divisors of r_{j-1} and a greatest common divisor is thus given by r_{j-1} itself.
Let d be another greatest common divisor of a and b. Then we have $r_{j-1}|d$ since d is greatest common divisor and $d|r_{j-1}$ since r_{j-1} is greatest common divisor. By Lemma 70 this means that there exists a unit $u \in R^\times$ with $d = u \diamond r_{j-1}$. □

Algorithm 74 (Euclid's Algorithm)
IN: $e_\circ \neq a, b \in R$
OUT: $\gcd(a, b)$

1. $i \leftarrow 0$
2. $r_{-1} \leftarrow a$
3. $r_0 \leftarrow b$
4. `while` $r_i \neq e_\circ$
   (a) $i \leftarrow i + 1$
   (b) $r_i \leftarrow (r_{i-2} \bmod r_{i-1})$ *where* $r_{i-2} = q_i \diamond r_{i-1} \circ r_i$ *with* $r_i = e_\circ$ *or* $v(r_i) < v(r_{i-1})$
5. `return` r_{i-1}

This algorithm must terminate since the size of the remainder is strictly decreasing until $r_i = e_\circ$ is reached. This implies that $r_{i-1}|r_{i-2}$ and by Lemma 72 this r_{i-1} is the greatest common divisor of the input values a and b.
In Section 1.3 we gave a special version of the following result as Lemma 37. With the help of the Euclidean algorithm we can not only generalize the result to arbitrary Euclidean rings but also give a constructive proof of Bézout's identity.

Lemma 75 *Let R be a Euclidean domain with respect to v. For any non-zero $a, b \in R$ there exist $m, n \in R$ so that*

$$\gcd(a, b) = m \diamond a \circ n \diamond b.$$

Proof. Algorithm 74 produces a sequence of remainders r_i and (implicitly) of quotients q_i with the property that $r_{i-2} = q_i \diamond r_{i-1} \circ r_i$. When the algorithm terminates we have $r_i = e_\circ$ and before that $r_{i-3} = q_{i-1} \diamond r_{i-2} \circ r_{i-1}$, i.e. $\gcd(a, b) = r_{i-3} \circ \mathrm{inv}_\circ(q_{i-1} \diamond r_{i-2})$. Recursively replacing r_{i-2}, r_{i-3} etc. by these linear combinations leads to an equation of the requested form since the first equation was $a = r_{-1} = q_1 \diamond r_0 \circ r_1 = q_1 \diamond b \circ r_1$. □

Example 76 *Bézout's identity leads to an efficient way of computing modular inverses. Let $a, n \in \mathbb{N}$ and let $\gcd(a, n) = 1$. By Lemma 33 a is invertible modulo n and indeed the previous lemma shows that there exists b, m such that*

$$1 = \gcd(a, n) = ab + nm, \text{ i.e. } 1 \equiv ab \bmod n,$$

so the b computed in Bézout's identity is the inverse of a modulo n.

Lemma 77 *Let R be a Euclidean domain and let $a, b \in R$ so that a and b have no non-trivial common divisor and let $c \in R$. If $a|c$ and $b|c$ then also $(a \diamond b)|c$.*

Proof. There exist k, l with $c = a \diamond k$ and $c = b \diamond l$. If a and b are co-prime we have $\gcd(a, b) = e_\diamond$ and by Lemma 75 there exist $m, n \in R$ so that $e_\diamond = m \diamond a \circ n \diamond b$.
This leads to $c = a \diamond k = (a \diamond k) \diamond e_\diamond = (a \diamond k) \diamond (m \diamond a \circ n \diamond b) = (b \diamond l) \diamond (m \diamond a) \circ (a \diamond k) \diamond (n \diamond b) = (a \diamond b) \diamond ((m \diamond l) \circ (n \diamond k))$, so $a \diamond b$ divides c. □

Example 78 *In recreational mathematics one often encounters stories like the following example:*
A Chinese general has a fast way of "counting" the number of soldiers in his army. He first lets them line up in rows of 11 and counts the number of soldiers in the last, incomplete row. He then repeats the process with rows of 13 and rows of 17.
One morning, he finds that there are 3 soldiers left when the rest are in rows of 11, 4 soldiers left when the rest are in rows of 13, and 9 soldiers left when the rest are in rows of 17. He knows that there are 1000 soldiers in his army. How many of the soldiers are present this morning?
We fist look what the numbers would look like if all 1000 were present. We have

$$1000 \equiv 10 \bmod 11; 1000 \equiv 12 \bmod 13; 1000 \equiv 14 \bmod 17,$$

so clearly not all soldiers are present. So we are asked to find a number X such that the following systems of equivalences is satisfied

$$\begin{aligned} X &\equiv 3 \bmod 11; \\ X &\equiv 4 \bmod 13; \\ X &\equiv 9 \bmod 17. \end{aligned}$$

From the last equivalence we get $X = 17Y + 9$ for some Y. From the second we get $X = 17Y + 9 \equiv 4Y + 9 \stackrel{!}{\equiv} 4 \bmod 13$, i.e., $4Y \equiv 8 \bmod 13$. In this case we can divide both sides by 4 and get $Y \equiv 2 \bmod 13$; in general we could use Bézout's identity to compute the inverse of 4 modulo 13, namely $4 \cdot 10 \equiv 1 \bmod 13$, to obtain $Y \equiv 2 \bmod 13$. This means that with some Z we have

$$X = 17 \cdot 13Z + 17 \cdot 2 + 9 = 17 \cdot 13Z + 43$$

as combination of the last two equations. Continuing to the first we get $X = 17 \cdot 13Z + 43 \equiv Z + 10 \stackrel{!}{\equiv} 3 \bmod 11$ which immediately gives $Z \equiv 4 \bmod 11$ and thus for some A

$$X = 17 \cdot 13 \cdot 11A + 17 \cdot 13 \cdot 4 + 43 = 2431A + 927.$$

From the story we know that the number of soldiers is positive and at most 1000 *and so* $A = 0$ *is the only possibility leading to* $X = 927$.
So apparently the general got a very bad day to count his soldiers since 73 *were absent (which is a sufficiently high number to avoid students guessing the correct solution).*

In the following section we show a generalization of this example to arbitrary rings; to conclude this section we state the *Chinese Remainder Theorem* only for the integers.

Theorem 79 (Chinese Remainder Theorem)
Let $r_1, \ldots, r_k \in \mathbb{Z}$ *and let* $0 \neq n_1, \cdots, n_k \in \mathbb{N}$ *such that the* n_i *are pairwise coprime. The system of equivalences*

$$\begin{aligned} X &\equiv r_1 \bmod n_1, \\ X &\equiv r_2 \bmod n_2, \\ &\vdots \\ X &\equiv r_k \bmod n_k, \end{aligned}$$

has a solution X *which is unique up to multiples of* $N = n_1 \cdot n_2 \cdots n_k$. *The set of all solutions is given by* $\{X + aN | a \in \mathbb{Z}\} = X + N\mathbb{Z}$.

Proof. To prove the theorem we state a homomorphism between $\mathbb{Z}/N\mathbb{Z}$ and the Cartesian product $\mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z}$ and show it to be an isomorphism. That implies that every set of equations (right hand side of the map) has a unique preimage $X \in \mathbb{Z}/N\mathbb{Z}$.
Define $\psi : \mathbb{Z}/N\mathbb{Z} \to \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z};\ X + N\mathbb{Z} \mapsto ((X \bmod n_1) + n_1\mathbb{Z}, (X \bmod n_2) + n_2\mathbb{Z}, \ldots, (X \bmod n_k) + n_k\mathbb{Z})$. The map ψ is homomorphic with respect to $+$ and to $\cdot$ since by Lemma 30 we have $X + Y \equiv (X \bmod n_i) + (Y \bmod n_i)$ and $X \cdot Y \equiv (X \bmod n_i) \cdot (Y \bmod n_i)$ and each n_i divides N.
The image and the domain have the same cardinality N and so the map is an isomorphism if it is injective. The kernel of ψ consists of those elements which map to $(n_1\mathbb{Z}, n_2\mathbb{Z}, \ldots, n_k\mathbb{Z})$, which are exactly those $X + N\mathbb{Z}$ where X is divisible by $n_1, n_2, \ldots, n_k$. Since the n_i are coprime, X must be divisible by their product, i.e. by N, which implies $X \equiv 0 \bmod N$ and so ψ is an isomorphism. □

If the n_i are not all coprime the system might not have a solution at all. E.g. the system $X \equiv 1 \bmod 8$ and $X \equiv 2 \bmod 6$ does not have a solution since the first congruence implies that X is odd while the second one implies that X is even. If the system has a solution then it is unique only modulo $\operatorname{lcm}(n_1, n_2, \ldots, n_k)$. E.g. the system $X \equiv 4 \bmod 8$ and $X \equiv 2 \bmod 6$ has solutions and the solutions are unique modulo 24. Replace $X \equiv 2 \bmod 6$ by $X \equiv 2 \bmod 3$; the system still carries the same information and we obtain $X = 8a + 4 \equiv 2a + 1 \overset{!}{\equiv} 2 \bmod 3$, thus $a \equiv 2 \bmod 3$ and $X = 8(3b + 2) + 4 = 24b + 20$. The smallest positive solution is thus 20.

We can now prove Lemma 36 which states that for $n = p_1^{e_1} p_2^{e_2} p_3^{e_3} \cdots p_r^{e_r}$ with $p_1, p_2, \ldots, p_r$ distinct primes and positive exponents $e_1, e_2, \ldots, e_r \in \mathbb{Z}$ we have

$$\varphi(n) = \prod_{i=1}^{r} (p_i^{e_i} - p_i^{e_i - 1}) = n \cdot \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right).$$

Proof. We first observe that the two expressions are equal as $p_i^{e_i} - p_i^{e_i-1} = p_i^{e_i}(1-1/p_i)$ and $n = p_1^{e_1}p_2^{e_2}p_3^{e_3}\cdots p_r^{e_r}$.
We prove the main result by induction on the number of prime factors r. For $r = 1$, i.e. $n = p_1^{e_1}$ a prime power, there are $p_1^{e_1} - p_1^{e_1-1}$ positive numbers coprime to n and $< n$ because there are $p_1^{e_1-1}$ multiples of p_1 in $\{0, 1, 2, \ldots, n-1\}$.
By assumption we have $\varphi\left(p_1^{e_1}p_2^{e_2}p_3^{e_3}\cdots p_{r-1}^{e_{r-1}}\right) = \prod_{i=1}^{r-1}(p_i^{e_i} - p_i^{e_i-1})$ and $\varphi\left(p_r^{e_r}\right) = p_r^{e_r} - p_r^{e_r-1}$.
Let $0 \leq a < p_1^{e_1}p_2^{e_2}p_3^{e_3}\cdots p_{r-1}^{e_{r-1}}$ and $0 \leq b < p_r^{e_r}$. The system of equations

$$\begin{aligned} X &\equiv a \bmod p_1^{e_1}p_2^{e_2}p_3^{e_3}\cdots p_{r-1}^{e_{r-1}}, \\ X &\equiv b \bmod p_r^{e_r}, \end{aligned}$$

has a unique solution $0 \leq X < n$. So for each of the $\varphi\left(p_1^{e_1}p_2^{e_2}p_3^{e_3}\cdots p_{r-1}^{e_{r-1}}\right)$ values of a coprime to $p_1^{e_1}p_2^{e_2}p_3^{e_3}\cdots p_{r-1}^{e_{r-1}}$ and each of the $\varphi\left(p_r^{e_r}\right)$ values of b coprime to $p_r^{e_r}$ there is exactly one solution $0 \leq X < n$ which shows that

$$\varphi(n) = \left(p_r^{e_r} - p_r^{e_r-1}\right)\prod_{i=1}^{r-1}(p_i^{e_i} - p_i^{e_i-1}) = \prod_{i=1}^{r}(p_i^{e_i} - p_i^{e_i-1}).$$

□

Exercise 80 *1. The Gaussian integers $\mathbb{Z}[i]$ are a subset of the complex numbers, defined as*

$$\mathbb{Z}[i] = \{a + bi | a, b \in \mathbb{Z}\}.$$

We define addition and multiplication as in $\mathbb{C}$ by

$$\begin{aligned} (a+bi) + (c+di) &= (a+c) + (b+d)i, \\ (a+bi)\cdot(c+di) &= (ac-bd) + (ad+bc)i. \end{aligned}$$

Show that $(\mathbb{Z}[i], +, \cdot)$ is a commutative ring with unity.

2. Let $(R, \circ, \diamond)$ be ring and let $a, b \in R$, $n \in \mathbb{N}$. Show that

$$(a \circ b)^n = \sum_{i=0}^{n}\left[\binom{n}{i}\right] a^i b^{n-i},$$

*where $[n]g = g \circ g \circ \cdots \circ g$ (n-times), the binomial coefficients are as in Chapter **??**, and the exponentiation a^i denotes the i fold product of a with itself: $a \diamond a \diamond \cdots \diamond a$. Hint: Use induction on n.*

3. Show that the set

$$\mathbb{C}[x, y] = \left\{ \sum_{i=0}^{n}\sum_{j=0}^{m} a_{ij}x^i y^j \,\middle|\, a_{ij} \in \mathbb{C}, n, m \in \mathbb{N} \right\}$$

is a ring with respect to the usual addition and multiplication.

4. Prove Lemma 69. Note that the proof is completely analogous to the considerations for the special case $(\mathbb{Z}/n\mathbb{Z})^\times$.

1.6 Further reading on rings

This section introduces ideals and subrings. These concepts are important in algebra and the proofs in the previous section could be stated more elegantly and in full generality using these notations but we decided to go for a more direct approach of proving results for special cases only. We include this section for the interested reader. The exercises are optional.
In Example 62 we considered the ring $n\mathbb{Z}$ which is a subset of $\mathbb{Z}$ and forms a ring with respect to the same operations. So we can define subrings analogously to subgroups. However, even more is true: we can multiply an element $an \in n\mathbb{Z}$ by *any* integer $b \in Z$ and obtain $an \cdot b = (ab)n$, a multiple of n. Subrings with this property are called *ideals*. For simplicity and since all examples we encounter are commutative, we from now on work with commutative rings R.

Definition 81 (Subring, ideal)
Let $(R, \circ, \diamond)$ be a ring and let $R' \subseteq R$ be a subset of R. If $(R', \circ, \diamond)$ is a ring then R' is a subring of R.
Let $I \subseteq R$ be a subset of the commutative ring R. If I is a subring of R and closed under $\diamond$ with arbitrary elements from R, i.e. $I \diamond R \subseteq I$ then I is called an ideal of R.

Example 82 *1. Let $n \in \mathbb{N}$. The set $n\mathbb{Z}$ of multiples of n is a ring and thus a subring of $\mathbb{Z}$. Since $an \cdot b = (ab)n$ a multiple of n for arbitrary integers b, the set $n\mathbb{Z}$ is an ideal in $\mathbb{Z}$.*

2. Consider the ring of polynomials $\mathbb{C}[x]$ in x over $\mathbb{C}$ and the subset

$$x\mathbb{C}[x] = \left\{ x \sum_{i=0}^{n} a_i x^i | a_i \in \mathbb{C}, n \in \mathbb{N} \right\}.$$

Sums and differences of such polynomials are of the same form

$$x \sum_{i=0}^{n} a_i x^i - x \sum_{i=0}^{m} b_i x^i = x \sum_{i=0}^{\max\{n,m\}} (a_i + b_i) x^i$$

and if we multiply a polynomial in $x\mathbb{C}[x]$ by an arbitrary one, the resulting polynomial is a multiple of x since

$$x \left(\sum_{i=0}^{n} a_{i+1} x^i \right) \cdot \left(\sum_{i=0}^{m} b_i x^i \right) = x \sum_{i=0}^{n+m} \left(\sum_{j=0}^{i} a_j b_{i-j} \right) x^i.$$

So $x\mathbb{C}[x]$ not only forms a subring of $\mathbb{C}[x]$ but even an ideal.

Ideals are an important concept particularly since they allow to generalize the concept of quotient groups to rings.

Definition 83 (Quotient ring)
Let $(R, \circ, \diamond)$ be a commutative ring and let I be an ideal of R. The quotient ring R/I of R modulo I *is defined as*

$$R/I = \{a \circ I | a \in R\}.$$

We have the analogue of Lemma 40 in the setting of rings:

Lemma 84 *Let $(R, \circ, \diamond)$ be a commutative ring and let I be an ideal in R. The quotient ring R/I is a commutative ring with respect to the following operations inherited from R:*

$$\begin{aligned}(a \circ I) \circ (b \circ I) &= (a \circ b) \circ I \\ (a \circ I) \diamond (b \circ I) &= (a \diamond b) \circ I.\end{aligned}$$

Proof. Since an ideal is in particular a subgroup with respect to the first operation $\circ$ we get from Lemma 40 that $(R/I, \circ)$ is a group. If R is abelian with respect to $\circ$ then so is R/I.
For the second operation we first need to show that the operation is well-defined. Let $a' \circ I = a \circ I$ and $b' \circ I = b \circ I$, i.e. there exist $i_a, i_b \in I$ so that $a' = a \circ i_a$ and $b' = b \circ i_b$. We have

$$(a' \circ I) \diamond (b' \circ I) = ((a \circ i_a) \circ I) \diamond ((b \circ i_b) \circ I) = ((a \circ i_a) \diamond (b \circ i_b)) \circ I = (a \diamond b) \circ (a \diamond i_b) \circ (i_a \diamond b) \circ (i_a \diamond i_b) \circ I = (a \diamond b) \circ I$$

since $a \diamond i_b, i_a \diamond b, i_a \diamond i_b \in I$ by the definition of an ideal. So the resulting residue class is independent of the representatives chosen.
Since R is closed under $\diamond$ so is R/I and associativity, commutativity, and the distributive laws are inherited, too. □

Remark 85 *Note that this lemma does not hold if the conditions on I are released and only a subring is required.*
Let R' be a subring, then the operation $\diamond$ need not necessarily be well-defined on R/R' since we have no reason to assume that $a \diamond i_b$ and $i_a \diamond b$ (expressions from the proof of Lemma 84) are in R'. This is where the property that ideals are closed under $\diamond$ with arbitrary elements is crucial.

Example 86 *Since for any $n \in \mathbb{N}$ we have that $n\mathbb{Z}$ is an ideal in $\mathbb{Z}$, Lemma 84 directly gives that $\mathbb{Z}/n\mathbb{Z}$ is a ring for any n.*

Definition 87 (Ring homomorphism)
Let $(R, \circ, \diamond)$ and $(R', \circ', \diamond')$ be rings and let ψ be a map $\psi : R \to R'$. If for any $a, b \in R$ the map ψ satisfies

$$\begin{aligned}\psi(a \circ b) &= \psi(a) \circ' \psi(b) \\ \psi(a \diamond b) &= \psi(a) \diamond' \psi(b)\end{aligned}$$

then ψ is a ring homomorphism.
A homomorphism ψ is an isomorphism *if it is bijective.*

Similar to the group case one can study the kernel and image of this map.

Theorem 88 *Let $(R, \circ, \diamond)$ and $(R', \circ', \diamond')$ be rings with unity and let ψ be a homomorphism. The kernel* $\mathrm{Ker}(\psi)$ *of ψ is an ideal in R and* $\mathrm{Im}(\psi) \cong R/\mathrm{Ker}(\psi)$.

Proof. Theorem 50 shows that $(\mathrm{Ker}(\psi), \circ)$ is a subgroup of $(R, \circ)$. Let $a \in \mathrm{Ker}(\psi)$, i.e. $\psi(a) = e_{\circ'}$. We have to show that for any $r \in R$ we have $r \diamond a \in \mathrm{Ker}(\psi)$:

$$\psi(r \diamond a) = \psi(r) \diamond' \psi(a) = \psi(r) \diamond' e_{\circ'} = e_{\circ'},$$

where the last result followed by Lemma 63. So $\mathrm{Ker}(\psi)$ is indeed an ideal.
To show the isomorphism the same construction as in Theorem 50 works. □

Remark 89 *A different way to motivate ideals is to start from the properties a ring homomorphisms should have and obtain, that the kernel of that map is not only a subring but has additional multiplicative structure.*

Definition 90 (Generator, principal ideal)
Let $(R, \circ, \diamond)$ be a commutative ring and let I be an ideal.
If there exist elements $g_1, \ldots, g_l$ such that

$$I = \{(g_1 \diamond r_1) \circ \cdots \circ (g_l \diamond r_l) | r_1, \ldots r_l \in R\}$$

then I is generated by $g_1, \ldots, g_l$ *written*

$$I = (g_1, \ldots, g_l).$$

If there exists a single element $g \in I$ such that

$$I = (g) = \{g \diamond r | r \in R\}$$

then I is called a principal ideal. *In this case, I is the ideal* generated by g *and g is called the* generator of I.
The ring R is called a principal ideal domain (PID) *if every ideal is a principal ideal.*

Lemma 91 *Let $(R, \circ, \diamond)$ be a commutative ring and let $g \in R$. The set $(g) = \{g \diamond r | r \in R\}$ forms an ideal in R.*
In more generality, let $g_1, \ldots, g_l \in R$. The set $(g_1, \ldots, g_l)$ is an ideal.

Proof. The proof is left to the reader as Exercise 1. □

Example 92 *1. Consider the ring of integers Z. We have seen that the subrings $n\mathbb{Z}$ for $n \in \mathbb{N}$ are ideals in $\mathbb{Z}$. This gives*

$$n\mathbb{Z} = \{nz | z \in \mathbb{Z}\} = (n),$$

and so $n\mathbb{Z}$ is a principal ideal generated by n.

We now show that every *ideal in $\mathbb{Z}$ is a principal ideal and thus $\mathbb{Z}$ is a principal ideal domain. We have to distinguish two cases, $I = \{0\} = (0)$ which is generated by 0 and $I \neq \{0\}$.*

Let $g \in I$ be the smallest positive integer in I. We now show that $I = (g)$. Since I is an ideal all multiples of g are in I and thus $I \supseteq (g)$. Assume that there is an element $b \in I \backslash (g)$. Then we can divide b by g with remainder $0 < r < g$ and obtain $b = qg + r$. Since b and qg are in I so is $r = b - qg$ by the definition of ideals. This contradicts the minimality of g.

So $\mathbb{Z}$ is a principal ideal domain.

2. *The Gaussian integers $\mathbb{Z}[i] \subset \mathbb{C}$ are a principal ideal domain. As for the integers we can define greatest common divisors and the proof follows along the same lines.*

3. *The set*

$$\mathbb{C}[x,y] = \left\{ \sum_{i=0}^{n} \sum_{j=0}^{m} a_{ij} x^i y^j \mid a_{ij} \in \mathbb{C}, n, m \in \mathbb{N} \right\}$$

is a ring, the polynomial ring in two variables (cf. Exercise 3). The ideal (x,y) generated by x and y is not a principal ideal. Assume on the contrary that there exists some $f(x,y) \in \mathbb{C}[x,y]$ such that $(f) = (x,y)$, so in particular there must exist f_x and f_y such that $x = f_x \cdot f$ and $y = f_y \cdot f$. The first condition limits f to constants $f \in \mathbb{C}$ or constant multiples of x, i.e. $f \in x\mathbb{C}$, while the second condition eliminates the latter possibility. So $f \in \mathbb{C}$ but since (x,y) does not contain any constant except for 0 we must have $f = 0$ which contradicts that f can generate a non-trivial ideal.

In the previous section we showed the Chinese remainder theorem for the integers. Now that we have the vocabulary of quotient rings and homomorphisms we can state the general version.

Theorem 93 (Chinese Remainder Theorem)
Let R be a Euclidean domain and let $n_1, \ldots, n_k \in R$ be pairwise coprime. Let $n = n_1 \diamond n_2 \diamond \cdots \diamond n_k$. The quotient ring R/nR and the product ring $R/n_1R \times R/n_2R \times \cdots \times R/n_kR$ are isomorphic via the map

$$\psi : R/nR \to (R/n_1R \times \cdots \times R/n_kR);\ \psi(x \circ nR) = (x \circ n_1R, \ldots, x \circ n_kR).$$

Proof. The proof is similar to the integer case. We first note that ψ is a homomorphism since $\circ$ and $\diamond$ are compatible with computing modulo principal ideals.
For the integers we could argue with the cardinalities of the domain and image. In the general case it is easier to give the inverse map to show that ψ is an isomorphism. Let l_i be defined by $l_i \diamond n_i = n$. Since l_i and n_i are coprime, Bézout's identity (Lemma 75) says that there exist elements $a_i, b_i \in R$ such that $a_i \diamond l_i \circ b_i \diamond n_i = e_\diamond$. Put $c_i = a_i \diamond l_i$. The inverse map is given by

$$\psi^{-1} : (R/n_1R \times \cdots \times R/n_kR) \to R/nR;\ (x_1 \circ n_1R, \ldots, x_k \circ n_kR) \mapsto \left(\sum_{i=1}^{k} x_i \diamond c_i \right) \circ nR,$$

where the summation sign stands for repeated application of $\circ$. To see that ψ^{-1} is well defined note that $((x_i \circ (n_i \diamond r_i)) \diamond c_i) \circ nR = ((x_i \diamond c_i) \circ ((n_i \diamond r_i) \diamond c_i)) \circ nR = ((x_i \diamond c_i) \circ ((n_i \diamond r_i) \diamond (a_i \diamond l_i))) \circ nR = (x_i \diamond c_i) \circ nR$ since $(n_i \diamond r_i) \diamond (a_i \diamond l_i) = (n_i \diamond l_i) \diamond (a_i \diamond r_i)$ is a multiple of n.
We have

$$\psi(\psi^{-1}(x \circ n_1R, \ldots, x \circ n_kR)) = \psi\left(\left(\sum_{i=1}^{k} x_i \diamond c_i \right) \circ nR \right) = (x \circ n_1R, \ldots, x \circ n_kR),$$

since for every $1 \leq j \leq k$ we have $\left(\sum_{i=1}^k x_i \diamond c_i\right) \circ n_j R = \left(\sum_{i=1}^k x_i \diamond (a_i \diamond l_i)\right) \circ n_j R = x_j \diamond (a_j \diamond l_j) \circ n_j R = x_j \diamond e_\diamond \circ n_j R = x_j \circ n_j R$. Here we used that $l_i \in n_j R$ for $i \neq j$.
Likewise we have

$$\begin{aligned}\psi^{-1}(\psi(x \circ nR)) &= \psi^{-1}(x \circ n_1 R, \ldots, x \circ n_k R) = \left(\sum_{i=1}^k (x \circ (n_i \diamond r_i)) \diamond c_i\right) \circ nR \\ &= \left(\sum_{i=1}^k ((x \diamond c_i) \circ ((n_i \diamond r_i) \diamond (a_i \diamond l_i)))\right) \circ nR = x \sum_{i=1}^k c_i \circ nR.\end{aligned}$$

To show that $\sum_{i=1}^k c_i \circ nR = e_\diamond \circ nR$ we show that $n \left| \left(\left(\sum_{i=1}^k c_i\right) \circ \mathrm{inv}_\circ(e_\diamond)\right)\right.$. By definition of $c_i = a_i \diamond l_i$ we have for every factor n_j of n that $n_j | a_i \diamond l_i$ for $i \neq j$ and $n_j | a_j \diamond l_j \circ \mathrm{inv}_\circ(e_\diamond)$. So for every $1 \leq j \leq k$ we have $n_j \left| \left(\left(\sum_{i=1}^k c_i\right) \circ \mathrm{inv}_\circ(e_\diamond)\right)\right.$. Since the n_j are co-prime the claim follows from Lemma 77. □

Exercise 94 *1. Prove Lemma 91.*

1.7 Fields

Fields are special rings in which also the second operation $\diamond$ is commutative and in which every element $\neq e_\circ$ has an inverse with respect to $\diamond$. Familiar examples are the rational numbers, the reals and the complex numbers. This section is kept very short since most of the concepts are only needed for finite fields with are studied separately in Chapter **??**.

Definition 95 (Field)
A set K is a field *with respect to two operations $\circ, \diamond$ denoted by $(K, \circ, \diamond)$ if*

1. *$(K, \circ)$ is an abelian group.*
2. *$(K^*, \diamond)$ is an abelian group, where $K^* = K \backslash \{e_\circ\}$ is all of K except for the neutral element with respect to $\circ$.*
3. *The distributive law holds in K:*

$$a \diamond (b \circ c) = a \diamond b \circ a \diamond c \text{ for all } a, b, c \in K.$$

Let L be a field and $K \subseteq L$. If K is a field itself it is a subfield of L *and L is an* extension field of K.

An alternative definition is to say that a field is a commutative ring with unity in which every element in K^* has an inverse with respect to $\diamond$.
We start with an easy but important observation

Lemma 96 *Let $(K, \circ, \diamond)$ be a field and let $e_\circ$ be the neutral element with respect to $\circ$. For any $a \in K$ we have:*

$$a \diamond e_\circ = e_\circ.$$

Fields are free of zero divisors, i.e. if for $a, b \in K$ one has $a \diamond b = e_\circ$ then either $a = e_\circ$ or $b = e_\circ$ or both.

Proof. The first part was shown already in Lemma 63. To prove the second part assume $a \neq e_\circ$. Thus $a \in K^*$ has an inverse $\mathrm{inv}_\diamond(a) \neq e_\circ$ since K^* is closed under $\diamond$. So we get:

$$\begin{aligned} e_\circ &= \mathrm{inv}_\diamond(a) \diamond (a \diamond b) \\ &= (\mathrm{inv}_\diamond(a) \diamond a) \diamond b = b, \end{aligned}$$

i.e. $e_\circ = b$. □

Example 97 *1. The rational numbers $(\mathbb{Q}, +, \cdot)$ form a field. We have already seen that they form a commutative ring with unity so the only thing to show is that in $(\mathbb{Q}^*, \cdot)$ every element has an inverse. By the very construction of the rationals the inverse of $0 \neq \frac{a}{b}$ is given by $\frac{b}{a}$ since $\frac{a}{b} \cdot \frac{b}{a} = 1$. If $a \neq 0$ then the inverse exists and since 0 is the neutral element of addition it is not in $\mathbb{Q}^*$.*

2. Further fields are $(\mathbb{C}, +, \cdot)$ and $(\mathbb{R}, +, \cdot)$, where $\mathbb{R}$ is an extension field of $\mathbb{Q}$ and a subfield of $\mathbb{C}$ while $\mathbb{C}$ is an extension field of both.

3. The integers form a commutative ring with unity but not a field since only 1 and -1 are invertible.

4. Let $p \in \mathbb{N}$ be a prime number. The set of residue classes modulo p $(\mathbb{Z}/p\mathbb{Z}, +, \cdot)$ is a field:
We have seen that $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ is a commutative ring with unity for any integer n. By Lemma 33 we have that the invertible elements $a + p\mathbb{Z}$ are exactly those classes for which a is coprime to p. Since p is prime these are all nonzero classes, so $(\mathbb{Z}/p\mathbb{Z})^\times = \mathbb{Z}/p\mathbb{Z} \setminus \{0\}$ and so $(\mathbb{Z}/p\mathbb{Z}, +, \cdot)$ is a field.

This is the first example of a finite field. *We will study finite fields in much more detail in Chapter* **??**.

For those readers who read the previous section on ideals we would like to add the following lemma.

Lemma 98 *Let $(K, \circ, \diamond)$ be a field and let $I \subset K$ be an ideal. Then $I = K$ or $I = \{e_\circ\}$.*

Proof. We first note that a field is also a ring, so speaking of an ideal makes sense. Let us first consider the case that there is an element $a \neq e_\circ$ in I. Since K is a field there exists $\mathrm{inv}_\diamond(a) \in K$ and by the multiplicative property of ideals we must have $a \diamond \mathrm{inv}_\diamond(a) = e_\diamond \in I$. Again by the multiplicative property every $b \in K$ is also in I as $b \diamond e_\diamond = b$, so $I = K$.
We have seen earlier that $I = \{e_\circ\}$ is an ideal for any ring with unity, so this also holds for a field. □

Exercise 99 *Consider the subset $\mathbb{Q}(i) \subset \mathbb{C}$ defined by*

$$\mathbb{Q}(i) = \{a + bi | a, b \in \mathbb{Q}\}.$$

Show that $(\mathbb{Q}(i), +, \cdot)$ is a field, where addition and multiplication are defined as in $\mathbb{C}$.

1.8 Polynomials

Polynomials become very important in the construction of finite fields in the following chapter. They are also a nice example of a ring and share many properties with the ring of integers.

Definition 100 (Polynomial)
Let K be a field. A polynomial in one variable x over K *is a finite sum of powers of x with* coefficients f_i *in the field K*

$$f(x) = \sum_{i=0}^{n} f_i x^i, \ f_i \in K.$$

We denote the set of polynomials in x over K by $K[x]$ and have

$$K[x] = \left\{ \sum_{i=0}^{n} f_i x^i | n \in \mathbb{N}, f_i \in K \right\}.$$

Example 101 *$f(x) = 3x^7 + \sqrt{2}x^4 - 27x^3 + 2x + 100$ and $g(x) = 1024x^{10} + 256x^8 + 32x^5 + 16x^4 + 4x^2 + 1$ are polynomials over the reals $f(x), g(x) \in \mathbb{R}[x]$.*
Instead of calling the variable x one can also define $K[y]$ or $K[t]$, e.g. $h(t) = 23t^{12} - 4t + 3 \in \mathbb{Q}[t]$.

Note that $\sum_{i=0}^{n} f_i x^i$ and $0 \cdot x^{n+1} + \sum_{i=0}^{n} f_i x^i$ define the same polynomial just as one can also write 0127 instead of 127. It would be more correct to introduce polynomials as equivalence classes which can be filled up with leading zeros. We usually omit leading zeros.

Definition 102 (Degree and leading term)
Let $f \in K[x]$ be a nonzero polynomial over a field K. Let n be the largest integer with $f_n \neq 0$, then n is called the degree of f, *denoted by* $\deg(f) = n$, *and f_n is called the* leading coefficient of f, *denoted by $LC(f) = f_n$. The* leading term of f *is $LT(f) = f_n x^n$. A polynomial f is called* monic *if $LC(f) = 1$.*

All the definitions carry through for the case that the coefficients are from a ring R rather than from a field K. However, if K is a field one can normalize each polynomial to make it monic by dividing by $LC(f)$. Over a ring the leading term need not be invertible.

Example 103 *Consider $f, g \in \mathbb{R}[x]$ as defined in Example 101. We have*

$$f(x) = 3x^7 + \sqrt{2}x^4 - 27x^3 + 2x + 100, \deg(f) = 7, LC(f) = 3$$

and

$$g(x) = 1024x^{10} + 256x^8 + 32x^5 + 16x^4 + 4x^2 + 1, \deg(g) = 10, LC(g) = 1024.$$

Lemma 104 *Let $(K,+,\cdot)$ be a field. The polynomials $K[x]$ form a ring with the operations*

$$\begin{aligned} f(x)+g(x)=\sum_{i=0}^{n} f_i x^i+\sum_{i=0}^{m} g_i x^i &= \sum_{i=0}^{\max\{n,m\}} (f_i+g_i)x^i, \\ f(x)\cdot g(x)=\sum_{i=0}^{n} f_i x^i\cdot\sum_{i=0}^{m} g_i x^i &= \sum_{i=0}^{n+m}\left(\sum_{j=0}^{i} f_j g_{i-j}\right)x^i, \end{aligned}$$

where $f,g\in K[x]$ and $f_i=0$ for $i>n$ and $g_i=0$ for $i>m$.
Furthermore, multiplication in $K[x]$ is commutative and $K[x]$ is a ring with unity, namely $1\in K\subset K[x]$ is the neutral element with respect to multiplication. There are no zero divisors in $K[x]$.

Proof. Obviously the results are sums of powers of x of finite lengths ($\max\{n,m\}$ and $n+m$). Since K is a field, the new coefficients (f_i+g_i) and $\sum_{j=0}^{i} f_j g_{i-j}$ are in K as well. So $K[x]$ is closed under addition and multiplication.
Associativity and commutativity of $+$ and $\cdot$ follow from the same properties of K. The neutral element of addition is $0\in K\subset K[x]$ and of multiplication $1\in K\subset K[x]$ as can be seen directly.
The additive inverse of $f(x)=\sum_{i=0}^{n} f_i x^i$ is $-f(x)=\sum_{i=0}^{n}(-f_i)x^i$ which is in $K[x]$ since $-f_i\in K$ for $0\le i\le n$.
The distributive laws can be checked by direct inspection. We leave that part of the proof as an exercise to the reader.
Let $f(x)\cdot g(x)=0$, i.e. $\sum_{j=0}^{i} f_j g_{i-j}=0$ for all $0\le i\le m+n$. Since K is a field we obtain for $i=0$ that either $g_0=0$ or $f_0=0$ or both. Assume first $f_0=0$ and $g_0\neq 0$. For $i=1$ we obtain that $f_0g_1+f_1g_0=f_1g_0=0$ and so $f_1=0$. For $i=2$ we obtain that $f_0g_2+f_1g_1+f_2g_0=f_2g_0=0$ and so $f_2=0$. Repeating the same argument leads to $f(x)=0$. If both $f_0=g_0=0$ then $i=1$ does not lead to any condition on f_1 or g_1. For $i=2$ we obtain that $f_0g_2+f_1g_1+f_2g_0=f_1g_1=0$ and so either $f_1=0$ or $g_1=0$ or both. Eventually we obtain $f(x)=0$ or $g(x)=0$ or both, so there are no zero divisors in $K[x]$. □

Example 105 *With $f,g\in\mathbb{R}[x]$ as in Example 101 we have*

$$f(x)+g(x)=1024x^{10}+256x^8+3x^7+32x^5+(16+\sqrt{2})x^4-27x^3+4x^2+2x+101.$$

and

$$\begin{aligned} f(x)\cdot g(x) &= 3072x^{17}+768x^{15}+1024\sqrt{2}x^{14}-27648x^{13}+(96+256\sqrt{2})x^{12}-4816x^{11}+ \\ &\quad 102400x^{10}+(524+32\sqrt{2})x^9+(24736+16\sqrt{2})x^8-429x^7+(64+4\sqrt{2})x^6+ \\ &\quad 3124x^5+(1600+\sqrt{2})x^4-19x^3+400x^2-2x+100. \end{aligned}$$

Definition 106 (Roots)
One can consider a polynomial $f(x)=\sum_{i=0}^{n} f_i x^i\in K[x]$ as a function

$$f: K\to K, \alpha\mapsto f(\alpha)=\sum_{i=0}^{n} f_i\alpha^i.$$

Computing $f(\alpha)$ is called evaluating $f(x)$ in $x = \alpha$.
A root of f *is an element $\alpha \in K$ such that $f(\alpha) = 0$. So the roots form the kernel of the map f defined above.*

Lemma 107 *Let $f \in K[x]$. If $\alpha \in K$ is a root of f then*

$$(x - \alpha) | f(x).$$

The proof is left to the reader as Exercise 116. An immediate consequence of this lemma is the following corollary.

Corollary 108 *Let $f \in K[x]$ be a polynomial of degree n. It has at most n roots.*

Sometimes it is helpful to change the variables in a reversible way, e.g. in the polynomial $g(x)$ in Example 101 one can substitute $y = 2x$ and obtain $\tilde{g}(y) = y^{10}+y^8+y^5+y^4+y^2+1$. A transformation of the form $y = ax+b$ does not change the degree and there is a simple linear relation between the roots of the original and the resulting polynomial. In this example the relation between g and $\tilde{g}$ is particularly simple.

There are many similarities between the ring of integers and the ring of polynomials over a field, in particular we find "primes" and show that each polynomial can be factored uniquely into a product of them. These so-called "irreducible polynomials" play an important role in constructing finite fields as we will see in Chapter **??**.

Definition 109 (Irreducible polynomial)
Let K be a field. A polynomial $f(x) \in K[x]$ of degree at least 1 is irreducible *if it cannot be written as a product of polynomials of lower degree over the same field, i.e. if $u(x)|f(x)$ implies u is constant or $u(x) = f(x)$.*
Otherwise $f(x)$ is reducible.

Example 110 *Consider polynomials over the rational numbers $\mathbb{Q}$.*

a) $f(x) = x^2 + 2x - 8$ has roots 2 and -4 and thus splits as $f(x) = (x - 2)(x + 4)$. The factors $x - 2$ and $x + 4$ are both irreducible.

b) $g(x) = x^2 + 2x + 8$ does not split over $\mathbb{Q}$ but only over $\mathbb{C}$. Therefore, g is irreducible as polynomial in $\mathbb{Q}[x]$.

c) $h(x) = x^4 + 4x^3 + 20x^2 + 32x + 64$ does not have a root over $\mathbb{Q}$ but factors into $x^4 + 4x^3 + 20x^2 + 32x + 64 = (x^2 + 2x + 8)^2 = g(x)^2$.

Note that for a polynomial of degree less than 4 it is enough to check for roots to determine whether it is irreducible or not. For polynomials of larger degree there can be non-linear factors as in the last example.
A prominent example of Euclidean domains is the ring of integers which, as we mentioned in the introduction, shares many properties with the ring of polynomials over a field. We now show that the polynomial ring is also a Euclidean domain. That means that one can define division with remainder and has an algorithm to compute greatest common divisors, namely the Euclidean algorithm.

Lemma 111 *Let K be a field. The ring of polynomials over K is a Euclidean domain with respect to the degree function $v(f) = \deg(f)$, i.e. $K[x]$ is a ring with unity and without zero divisors, $\cdot$ is commutative and one can define division with remainder so that the remainder has smaller degree than the divisor or equals 0.*

Proof. We have already seen in Lemma 104 that $K[x]$ is a domain with unity 1 and that $\cdot$ is commutative. Consider the division with remainder of f by g, where both $f, g \in K[x]$. Let $r \in K[x]$ be the remainder. Let the leading term of f be $LT(f) = ax^n$ and of g be $LT(g) = bx^m$. If $n < m$ then $r = f$ is the remainder and obviously $\deg(r) < \deg(g)$. Otherwise there exists a polynomial $q \in K[x]$ with $LT(q) = (a/b)x^{n-m}$ (note that a/b is defined since $a, b \in K \setminus \{0\}$) such that f splits as $f = q \cdot g + r$. The coefficient of x^n in r equals $a - (a/b) \cdot b = 0$ and so the degree of r is strictly smaller than n. Clearly it is possible that more coefficients in r vanish and the degree drops dramatically, for example if $g|f$ then $r = 0$. □

This lemma implies in particular that greatest common divisors are defined and computable via the Euclidean algorithm.
As in the integers $\mathbb{Z}$ we have that in $K[x]$ irreducible is the same as prime.

Lemma 112 *Let $p, f, g \in K[x]$ and let p be irreducible. Then one has*

$$p|f \cdot g \Rightarrow p|f \text{ or } p|g.$$

Proof. Let $d = \gcd(p, f)$, then $d|p$. Since p is irreducible, we must have $d = 1$ or $d = p$, where we use the convention that the gcd is monic.
If $d = p$ then $p|f$ by the definition of gcd. So $p|f$ and we are done.
In case $d = 1$ we use Lemma 75 and know that there exist $u, v \in K[x]$ with $d = 1 = u \cdot p + v \cdot f$. Multiplying both sides by g gives the expression

$$g = u \cdot p \cdot g + v \cdot f \cdot g.$$

Both summands on the right are divisible by p. For the second one note that by assumption $p|f \cdot g$. Thus also the left hand side must be divisible by p and thus $p|g$. □

We are used to factoring integers $n \in \mathbb{Z}$ into powers of primes in a unique manner. The following lemma shows that the ring of polynomials over a field has the same property of unique factorization that every non-zero element can be written as a product of irreducible elements.

Lemma 113 *For all $f \in K[x]$ there exist monic irreducible polynomials $p_1, \ldots, p_r \in K[x]$ all distinct and exponents $e_1, \ldots, e_r \in \mathbb{N}$ so that f can be written as*

$$f = k \prod_{i=1}^{r} p_i^{e_i},$$

where $k \in K$.

Proof. We first show that such a representation exists and then consider uniqueness. There are two cases, either f itself is irreducible, in which case we put $p_1 = f/LC(f)$ and $k = LC(f)$, or it splits as $f = a \cdot b$ with $\deg(a), \deg(b) < \deg(f)$ and we continue separately with $f = a$ and $f = b$. In the latter case both parts have strictly smaller degree than f which means that this process terminates with *some* factorization into irreducible polynomials

$$f = k \prod p_i^{e_i}.$$

We now assume that the representation is not unique, i.e. there exist monic irreducible polynomials $q_1, \ldots, q_s \in K[x]$, exponents $a_1, \ldots, a_s \in \mathbb{N}$, and a field element $l \in K$ so that f can be written as

$$f = k \prod_{i=1}^{r} p_i^{e_i} = l \prod_{j=1}^{s} q_j^{a_j}.$$

The irreducible polynomial p_1 must divide one of the polynomials on the right hand side by Lemma 112. So there is some q_j with $p_1 | q_j$. Since q_j is also irreducible they must be equal up to constants from K and since both are monic we even have $p_1 = q_j$. The left side is divisible by $p_1^{e_1}$ and so must be the right hand side. Since the q_j are all distinct we must have $e_1 \leq a_j$. By reversing the arguments we obtain the opposite inclusion and thus $e_1 = a_j$. We divide both sides by $p_1^{e_1}$ and repeat the same considerations for p_2. Since the exponents coincide we must have $r = s$ which concludes the proof. □

Remark 114 *It is worth mentioning that the property of having unique factorization is weaker than being Euclidean. In fact every Euclidean ring has unique factorization. Since we did not show the general statement we had to prove the result in the special case of polynomial rings.*

Example 115 *Let $K = \mathbb{Z}/2\mathbb{Z}$ be the field of integers modulo 2. We consider the residue classes of $K[x]$ modulo $f(x) = x^n + 1$ for some integer n, $R = K[x]/(x^n + 1)K[x]$. In this important example we show that R is a commutative ring with unity.*
We represent each residue class in R by the polynomial of smallest degree in it

$$R = \left\{ a_0 + a_1 x + a_2 x^2 + \cdots + a_{n-1} x^{n-1} \mid a_i \in K \right\}.$$

1. *$(K[x]/fK[x], +)$ is a group: obviously it is closed under addition, associativity is inherited from $K[x]$, the neutral element is $0 + fK[x]$, and additive inverses exist* $\operatorname{inv}\left(\left(\sum_{i=0}^{n-1} a_i x^i\right) + fK[x]\right) = \left(\sum_{i=0}^{n-1} (-a_i)\, x^i\right) + fK[x]$.

2. *$(K[x]/fK[x], \cdot)$ is a commutative monoid with 1: the product of two classes is another class, associativity is inherited from $K[x]$, and the neutral element with respect to multiplication is $1 + fK[x]$.*

3. *The distributive laws are inherited from $K[x]$.*

The same proof works for any field K and any polynomial f.

Exercise 116 *Prove Lemma 107. Hint: divide $f(x)$ by $x - \alpha$ and study the remainder.*

1.9 Vector spaces

The last algebraic concept we introduce in this chapter is one that most readers will be familiar with from introductory courses on linear algebra and solving of linear equations. Vector spaces also appear in daily life since we are living in a three dimensional space and thus positions can be specified by giving the height and extensions in width and length.

Definition 117 (Vector space)
A set V is a vector space *over a field $(K, \circ, \diamond)$ with respect to one operation $\oplus$ if*

1. *$(V, \oplus)$ is an abelian group.*
2. *$(K, \circ, \diamond)$ is a field. Let $e_\circ, e_\diamond$ be the neutral elements with respect to $\circ$ and $\diamond$.*
3. *There exists an operation $\odot : K \times V \to V$ such that for all $a, b \in K$ and for all $\underline{v}, \underline{w} \in V$ we have*

$$\begin{aligned} (a \circ b) \odot \underline{v} &= a \odot \underline{v} \oplus b \odot \underline{v} \\ a \odot (\underline{v} \oplus \underline{w}) &= a \odot \underline{v} \oplus a \odot \underline{w} \\ e_\diamond \odot \underline{v} &= \underline{v} \end{aligned}$$

Example 118 *Consider the field $(\mathbb{R}, +, \cdot)$ and define an operation on the 3-tuples $(x, y, z) \in \mathbb{R}^3$ by componentwise addition*

$$(x_1, y_1, z_1) \oplus (x_2, y_2, z_2) = (x_1 + x_2, y_1 + y_2, z_1 + z_2)$$

and for $a \in \mathbb{R}$ let

$$a \odot (x_1, y_1, z_1) = (ax_1, ay_1, az_1).$$

Since $\mathbb{R}$ is closed under addition and multiplication and since the distributive laws hold we have that $\mathbb{R}^3$ forms a vector space over $\mathbb{R}$ with these operations.
The same holds for $\mathbb{R}^n$ for any integer n.
To ease notation we replace $\oplus$ by $+$ and omit $\odot$ in $\mathbb{R}^n$.

Example 119 *The complex numbers $\mathbb{C}$ form a vector space over the reals $(\mathbb{R}, +, \cdot)$ where the operations are defined as follows:*
$\oplus$ is the standard addition of complex numbers, i.e.

$$(a + bi) \oplus (c + di) = (a + c) + (b + d)i,$$

and $\odot$ is the standard multiplication, i.e.

$$a \odot (b + ci) = (a \cdot b) + (a \cdot c)i,$$

in which the first argument is restricted to $\mathbb{R}$.
This fulfills the definition since we have already seen that $(\mathbb{R}, +, \cdot)$ and $(\mathbb{C}, +, \cdot)$ are both fields. The last three conditions are automatically satisfied since $\mathbb{C}$ is a field.

The previous section dealt extensively with polynomials. They are also a good example of vector spaces.

Example 120 *Let K be a field and consider the polynomial ring $K[x]$ over K. We define $\oplus$ to be the coefficientwise addition, i.e. the usual addition in $K[x]$ and $\odot$ as the multiplication of each coefficient by a scalar from K, i.e. polynomial multiplication restricted to the case that one input polynomial is constant.*
Since $K[x]$ forms a ring and K is a field, $K[x]$ also forms a vector space over K.

Example 121 *Let K be a field, $n \in \mathbb{N}$ and consider the subset P_n of $K[x]$ defined by*

$$P_n = \{f(x) \in K[x] | \deg(f) \leq n\}.$$

Since addition of polynomials and multiplication by constants do not increase the degree, P_n is closed under addition and multiplication by scalars from K and is thus a vector space over K.

The example of $\mathbb{C}$ being a vector space over $\mathbb{R}$ can be generalized to arbitrary extension fields.

Example 122 *Let $(K, \circ, \diamond)$ be a field and let $L \supseteq K$ be an extension field of K. Then L is a vector space over K, where $\oplus = \circ$ and $\odot = \diamond$.*

Definition 123 (Linear combination, basis, dimension)
Let V be a vector space over the field K and let $\underline{v}_1, \underline{v}_2, \ldots, \underline{v}_n \in V$.
A linear combination *of the vectors $\underline{v}_1, \underline{v}_2, \ldots, \underline{v}_n$ is given by*

$$\sum_{i=1}^{n} \lambda_i \odot \underline{v}_i,$$

for some $\lambda_1, \lambda_2, \ldots, \lambda_n \in K$, where the summation sign stands for repeated application of $\oplus$.
The elements $\underline{v}_1, \ldots, \underline{v}_n$ are linearly independent *if $\sum_{i=1}^{n} \lambda_i \odot \underline{v}_i = e_\oplus$ implies that for all $1 \leq i \leq n$ we have $\lambda_i = e_\circ$.*
A set $\{\underline{v}_1, \underline{v}_2, \ldots, \underline{v}_n\}$ is a basis of V *if $\underline{v}_1, \ldots, \underline{v}_n$ are linearly independent and each element can be represented as a linear combination of them, i.e.*

$$V = \left\{ \sum_{i=1}^{n} \lambda_i \odot \underline{v}_i \mid \lambda_i \in K \right\}.$$

The cardinality of the basis is the dimension of V*, denoted by* $\dim_K(V)$.

An alternative definition of basis are that $\{\underline{v}_1, \underline{v}_2, \ldots, \underline{v}_n\}$ is a minimal set of generators, meaning that there are no fewer elements of V such that each element can be represented as a linear combination of them.
Yet another definition states that a basis is a maximal set of linearly independent vectors.

Example 124 *Consider the vector space $\mathbb{R}^3$. The vectors $(1,0,0)$ and $(0,1,0)$ are linearly independent since*

$$\lambda_1(1,0,0) + \lambda_2(0,1,0) = (\lambda_1, \lambda_2, 0) \stackrel{!}{=} (0,0,0)$$

forces $\lambda_1 = \lambda_2 = 0$. *They do not form a basis since, e.g., the vector* $(0,0,3)$ *cannot be represented as a linear combination of them.*
Since $2(1,0,0) = (2,0,0)$ *the vectors* $(1,0,0)$ *and* $(2,0,0)$ *are linearly dependent.*
The vectors $(1,0,0), (0,1,0)$, *and* $(1,3,0)$ *are linearly dependent since a non-trivial linear combination is given by*

$$(1,0,0) + 3(0,1,0) - (1,3,0) = (0,0,0).$$

The vectors $(1,0,0), (0,1,0)$, *and* $(0,0,1)$ *are linearly independent and every other vector* $(x,y,z) \in \mathbb{R}^3$ *can be represented as a linear combination of them as*

$$(x,y,z) = x(1,0,0) + y(0,1,0) + z(0,0,1).$$

So we have that a basis of $\mathbb{R}^3$ *is given by* $\{(1,0,0), (0,1,0), (0,0,1)\}$ *and that the dimension is* $\dim_{\mathbf{R}}(\mathbb{R}^3) = 3$.
In general $\dim_{\mathbf{R}}(\mathbb{R}^n) = n$.

Example 125 *We have already seen that the complex numbers form a vector space over the reals. A basis is given by* $\{1, i\}$ *and so the dimension is* $\dim_{\mathbf{R}}(\mathbb{C}) = 2$.

Example 126 *Let* K *be a field and let* $P_n \subset K[x]$ *be the set of polynomials of degree at most* n. *A basis is given by* $\{1, x, x^2, x^3, \ldots, x^n\}$ *and so the dimension is* $\dim_K(P_n) = n+1$.
Alternative bases are easy to give. Since K *is a field,* x^i *can be replaced by* $a_i x^i$ *for any nonzero* $a_i \in K$, *also linear combinations are possible. So another basis is given by* $\{5, 3x-1, -x^2, 2x^3+x, \ldots, x^n + x^{n-1} + x^{n-2} + \cdots + x + 1\}$, *since the degrees are all different and so none can be a linear combination of the others, while using linear algebra we can get every element as a linear combination.*

Definition 127 (Subspace)
Let V *be a vector space over the field* K. *A subset* $W \subseteq V$ *is a* subspace *if* W *is a vector space with respect to the same operations.*

Vector spaces will be an important tool in constructing finite fields. Our interest in their general properties is, however, rather limited. We state some results on fields that need the definition of vector spaces.

Definition 128 (Extension degree)
Let L *be a field and let* K *be a subfield of* L. *The* extension degree *of* L *over* K *is defined as* $[L : K] = \dim_K(L)$.
If $\dim_K(L)$ *is finite,* L *is a* finite extension of K. *Otherwise* L *is a* infinite extension of K.

Lemma 129 *Let* L *be a finite extension field of* K *and let* F *be a finite extension field of* L, *so* $K \subseteq L \subseteq F$. *Then*

$$[F : K] = [F : L] \cdot [L : K].$$

Let $[F : L] = n$ *and* $[L : K] = m$. *Let* $f_1, f_2, \ldots, f_n$ *be a basis of* F *over* L *and* $l_1, l_2, \ldots, l_m$ *be a basis of* L *over* K. *A basis of* F *over* K *is given by*

$$\{l_1 \diamond f_1, l_2 \diamond f_1, \ldots, l_m \diamond f_1, l_1 \diamond f_2, l_2 \diamond f_2, \ldots, l_m \diamond f_2, \ldots, l_1 \diamond f_n, l_2 \diamond f_n, \ldots, l_m \diamond f_n\}.$$

Proof. Once we have proved the second claim the first one follows automatically since the basis has $\dim_K(F) = nm = \dim_L(F)\dim_K(L)$ elements.
We first show that every element of F can be represented by a K-linear combination of $l_1 \diamond f_1, l_2 \diamond f_1, \ldots, l_m \diamond f_1, l_1 \diamond f_2, l_2 \diamond f_2, \ldots, l_m \diamond f_2, \ldots, l_1 \diamond f_n, l_2 \diamond f_n, \ldots, l_m \diamond f_n$. Since $f_1, f_2, \ldots, f_n$ is a basis of F over L, for every element $f \in F$ there exist $c_1, c_2, \ldots, c_n \in L$ so that $f = \sum_{i=1}^{n} c_i \diamond f_i$. Likewise every $c_i \in L$ can be written as a K-linear combination of $l_1, l_2, \ldots, l_m$ as $c_i = \sum_{j=1}^{m} d_{ij} \diamond l_j$ with coefficients $d_{ij} \in K$. So

$$f = \sum_{i=1}^{n} c_i \diamond f_i = \sum_{i=1}^{n} \left(\sum_{j=1}^{m} d_{ij} \diamond l_j \right) \diamond f_i = \sum_{i=1}^{n} \sum_{j=1}^{m} d_{ij} \diamond (l_j \diamond f_i).$$

Assume now that $l_1 \diamond f_1, l_2 \diamond f_1, \ldots, l_m \diamond f_1, l_1 \diamond f_2, l_2 \diamond f_2, \ldots, l_m \diamond f_2, \ldots, l_1 \diamond f_n, l_2 \diamond f_n, \ldots, l_m \diamond f_n$ are linear dependent, i.e. there exist a nontrivial linear combination

$$\sum_{i=1}^{n} \sum_{j=1}^{m} d_{ij} \diamond (l_j \diamond f_i) = e_\circ$$

and not all $d_{ij} = e_\circ$. Put $c_i = \sum_{j=1}^{m} d_{ij} \diamond l_j$ then $\sum_{i=1}^{n} c_i \diamond f_i = e_\circ$. Since the f_i form a basis and are thus linearly independent we must have $c_i = e_\circ$ for all $1 \leq i \leq n$. However, since $l_1, l_2, \ldots, l_m$ form a basis the equality $\sum_{j=1}^{m} d_{ij} \diamond l_j = e_\circ$ implies that all $d_{ij} = e_\circ$ which contradicts the assumption. $\square$