Chapter 2
Basic Mathematical Concepts

In this chapter we introduce the mathematical concepts that form the basis for the developments in the following chapters. We begin with sets and basic mathematical logic. Then we consider maps between sets and their most important properties. Finally we discuss relations and in particular equivalence relations on a set.

2.1 Sets and Mathematical Logic

We begin our development with the concept of a set and use the following definition of Cantor.[1]

Definition 2.1 A *set* is a collection M of *well determined* and *distinguishable* objects x of our perception or our thinking. The objects are called the *elements* of M.

The objects x in this definition are well determined, and therefore we can uniquely decide whether x belongs to a set M or not. We write $x \in M$ if x is an element of the set M, otherwise we write $x \notin M$. Furthermore, the elements are distinguishable, which means that all elements of M are (pairwise) distinct.

If two objects x and y are equal, then we write $x = y$, otherwise $x \neq y$. For mathematical objects we usually have to give a formal definition of *equality*. As an example consider the equality of sets; see Definition 2.2 below.

We describe sets with curly brackets { } that contain either a list of the elements, for example

$$\{\text{red, yellow, green}\}, \quad \{1, 2, 3, 4\}, \quad \{2, 4, 6, \dots\},$$

[1] Georg Cantor (1845–1918), one of the founders of set theory. Cantor published this definition in the journal "Mathematische Annalen" in 1895.

J. Liesen and V. Mehrmann, *Linear Algebra*, Springer Undergraduate Mathematics Series, DOI 10.1007/978-3-319-24346-7_2

or a defining property, for example

$$\{x \mid x \text{ is a positive even number}\},$$
$$\{x \mid x \text{ is a person owning a bike}\}.$$

Some of the well known sets of numbers are denoted as follows:

$\mathbb{N} = \{1, 2, 3, \dots\}$	(the natural numbers),
$\mathbb{N}_0 = \{0, 1, 2, \dots\}$	(the natural numbers including zero),
$\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$	(the integers),
$\mathbb{Q} = \{x \mid x = a/b \text{ with } a \in \mathbb{Z} \text{ and } b \in \mathbb{N}\}$	(the rational numbers),
$\mathbb{R} = \{x \mid x \text{ is a real number}\}$	(the real numbers).

The construction and characterization of the real numbers $\mathbb{R}$ is usually done in an introductory course in Real Analysis.

To describe a set via its defining property we formally write $\{x \mid P(x)\}$. Here P is a *predicate* which may hold for an object x or not, and $P(x)$ is the *assertion* "P holds for x".

In general, an assertion is a statement that can be classified as either "true" or "false". For instance the statement "The set $\mathbb{N}$ has infinitely many elements" is true. The sentence "Tomorrow the weather will be good" is not an assertion, since the meaning of the term "good weather" is unclear and the weather prediction in general is uncertain.

The *negation* of an assertion A is the assertion "not A", which we denote by $\neg A$. This assertion is true if and only if A is false, and false if and only if A is true. For instance, the negation of the true assertion "The set $\mathbb{N}$ has infinitely many elements" is given by "The set $\mathbb{N}$ does not have infinitely many elements" (or "The set $\mathbb{N}$ has finitely many elements"), which is false.

Two assertions A and B can be combined via logical compositions to a new assertion. The following is a list of the most common logical compositions, together with their mathematical short hand notation:

Composition	Notation	Wording
conjunction	$\wedge$	A and B
disjunction	$\vee$	A or B
implication	$\Rightarrow$	A implies B
		If A then B
		A is a sufficient condition for B
		B is a necessary condition for A
equivalence	$\Leftrightarrow$	A and B are equivalent
		A is true if and only if B is true
		A is necessary and sufficient for B
		B is necessary and sufficient for A

For example, we can write the assertion "x is a real number and x is negative" as $x \in \mathbb{R} \wedge x < 0$. Whether an assertion that is composed of two assertions A and B is true or false, depends on the logical values of A and B. We have the following *table of logical values* ("t" and "f" denote true and false, respectively):

A	B	$A \wedge B$	$A \vee B$	$A \Rightarrow B$	$A \Leftrightarrow B$
t	t	t	t	t	t
t	f	f	t	f	f
f	t	f	t	t	f
f	f	f	f	t	t

For example, the assertion $A \wedge B$ is true only when A and B are both true. The assertion $A \Rightarrow B$ is false only when A is true and B is false. In particular, if A is false, then $A \Rightarrow B$ is true, independent of the logical value of B.

Thus, $3 < 5 \Rightarrow 2 < 4$ is true, since $3 < 5$ and $2 < 4$ are both true. But $3 < 5 \Rightarrow 2 > 4$ is false, since $2 > 4$ is false. On the other hand, the assertions $4 < 2 \Rightarrow 3 > 5$ and $4 < 2 \Rightarrow 3 < 5$ are both true, since $4 < 2$ is false.

In the following we often have to prove that certain implications $A \Rightarrow B$ are true. As the table of logical values shows and the example illustrates, we then only have to prove that under the assumption that A is true the assertion B is true as well. Instead of "Assume that A is true" we will often write "Let A hold".

It is easy to see that

$$(A \Rightarrow B) \quad \Leftrightarrow \quad (\neg B \Rightarrow \neg A).$$

(As an exercise create the table of logical values for $\neg B \Rightarrow \neg A$ and compare it with the table for $A \Rightarrow B$.) The truth of $A \Rightarrow B$ can therefore be proved by showing that the truth of $\neg B$ implies the truth of $\neg A$, i.e., that "B is false" implies "A is false". The assertion $\neg B \Rightarrow \neg A$ is called the *contraposition* of the assertion $A \Rightarrow B$ and the conclusion from $A \Rightarrow B$ to $\neg B \Rightarrow \neg A$ is called proof by contraposition.

Together with assertions we also often use so-called *quantifiers*:

Quantifier	Notation	Wording
universal	$\forall$	For all
existential	$\exists$	There exists

Now we return to set theory and introduce subsets and the equality of sets.

Definition 2.2 Let M, N be sets.

(1) M is called a *subset* of N, denoted by $M \subseteq N$, if every element of M is also an element of N. We write $M \nsubseteq N$, if this does not hold.
(2) M and N are called *equal*, denoted by $M = N$, if $M \subseteq N$ and $N \subseteq M$. We write $M \neq N$ is this does not hold.

(3) M is called a *proper subset* of N, denoted by $M \subset N$, if both $M \subseteq N$ and $M \neq N$ hold.

Using the notation of mathematical logic we can write this definition as follows:

(1) $M \subseteq N \quad \Leftrightarrow \quad (\forall x : x \in M \Rightarrow x \in N)$.
(2) $M = N \quad \Leftrightarrow \quad (M \subseteq N \wedge N \subseteq M)$.
(3) $M \subset N \quad \Leftrightarrow \quad (M \subseteq N \wedge M \neq N)$.

The assertion on the right side of the equivalence in (1) reads as follows: For all objects x the truth of $x \in M$ implies the truth of $x \in N$. Or shorter: For all x, if $x \in M$ holds, then $x \in N$ holds.

A very special set is the set with no elements, which we define formally as follows.

Definition 2.3 The set $\emptyset := \{x \mid x \neq x\}$ is called the *empty set*.

The notation ":=" means *is defined as*. We have introduced the empty set by a defining property: Every object x with $x \neq x$ is any element of $\emptyset$. This cannot hold for any object, and hence $\emptyset$ does not contain any element. A set that contains at least one element is called *nonempty*.

Theorem 2.4 *For every set M the following assertions hold:*

(1) $\emptyset \subseteq M$.
(2) $M \subseteq \emptyset \Rightarrow M = \emptyset$.

Proof

(1) We have to show that the assertion "$\forall x : x \in \emptyset \Rightarrow x \in M$" is true. Since there is no $x \in \emptyset$, the assertion "$x \in \emptyset$" is false, and therefore "$x \in \emptyset \Rightarrow x \in M$" is true for every x (cp. the remarks on the implication $A \Rightarrow B$).
(2) Let $M \subseteq \emptyset$. From (1) we know that $\emptyset \subseteq M$ and hence $M = \emptyset$ follows by (2) in Definition 2.2. □

Theorem 2.5 *Let M, N, L be sets. Then the following assertions hold for the subset relation "$\subseteq$":*

(1) $M \subseteq M$ *(reflexivity).*
(2) *If $M \subseteq N$ and $N \subseteq L$, then $M \subseteq L$ (transitivity).*

Proof

(1) We have to show that the assertion "$\forall x : x \in M \Rightarrow x \in M$" is true. If "$x \in M$" is true, then "$x \in M \Rightarrow x \in M$" is an implication with two true assertions, and hence it is true.
(2) We have to show that the assertion "$\forall x : x \in M \Rightarrow x \in L$" is true. If "$x \in M$" is true, then also "$x \in N$" is true, since $M \subseteq N$. The truth of "$x \in N$" implies that "$x \in L$" is true, since $N \subseteq L$. Hence the assertion "$x \in M \Rightarrow x \in L$" is true. □

Definition 2.6 Let M, N be sets.

(1) The *union*[2] of M and N is $M \cup N := \{x \mid x \in M \ \vee \ x \in N\}$.
(2) The *intersection* of M and N is $M \cap N := \{x \mid x \in M \ \wedge \ x \in N\}$.
(3) The *difference* of M and N is $M \setminus N := \{x \mid x \in M \ \wedge \ x \notin N\}$.

If $M \cap N = \emptyset$, then the sets M and N are called *disjoint*. The set operations union and intersection can be extended to more than two sets: If $I \neq \emptyset$ is a set and if for all $i \in I$ there is a set M_i, then

$$\bigcup_{i \in I} M_i := \{x \mid \exists\, i \in I \text{ with } x \in M_i\} \quad \text{and} \quad \bigcap_{i \in I} M_i := \{x \mid \forall\, i \in I \text{ we have } x \in M_i\}.$$

The set I is called an *index set*. For $I = \{1, 2, \ldots, n\} \subset \mathbb{N}$ we write the union and intersection of the sets $M_1, M_2, \ldots, M_n$ as

$$\bigcup_{i=1}^{n} M_i \quad \text{and} \quad \bigcap_{i=1}^{n} M_i.$$

Theorem 2.7 *Let $M \subseteq N$ for two sets M, N. Then the following are equivalent:*

(1) $M \subset N$.
(2) $N \setminus M \neq \emptyset$.

Proof We show that (1) $\Rightarrow$ (2) and (2) $\Rightarrow$ (1) hold.

(1) $\Rightarrow$ (2): Since $M \neq N$, there exists an $x \in N$ with $x \notin M$. Thus $x \in N \setminus M$, so that $N \setminus M \neq \emptyset$ holds.
(2) $\Rightarrow$ (1): There exists an $x \in N$ with $x \notin M$, and hence $N \neq M$. Since $M \subseteq N$ holds, we see that $M \subset N$ holds. □

Theorem 2.8 *Let M, N, L be sets. Then the following assertions hold:*

(1) *$M \cap N \subseteq M$ and $M \subseteq M \cup N$.*
(2) *Commutativity: $M \cap N = N \cap M$ and $M \cup N = N \cup M$.*
(3) *Associativity: $M \cap (N \cap L) = (M \cap N) \cap L$ and $M \cup (N \cup L) = (M \cup N) \cup L$.*
(4) *Distributivity: $M \cup (N \cap L) = (M \cup N) \cap (M \cup L)$ and $M \cap (N \cup L) = (M \cap N) \cup (M \cap L)$.*
(5) *$M \setminus N \subseteq M$.*
(6) *$M \setminus (N \cap L) = (M \setminus N) \cup (M \setminus L)$ and $M \setminus (N \cup L) = (M \setminus N) \cap (M \setminus L)$.*

Proof Exercise. □

[2]The notations $M \cup N$ and $M \cap N$ for union and intersection of sets M and N were introduced in 1888 by Giuseppe Peano (1858–1932), one of the founders of formal logic. The notation of the "smallest common multiple $\mathfrak{M}(M, N)$" and "largest common divisor $\mathfrak{D}(M, N)$" of the sets M and N suggested by Georg Cantor (1845–1918) did not catch on.

Definition 2.9 Let M be a set.

(1) The *cardinality* of M, denoted by $|M|$, is the number of elements of M.
(1) The *power set* of M, denoted by $\mathcal{P}(M)$, is the set of all subsets of M, i.e., $\mathcal{P}(M) := \{N \mid N \subseteq M\}$.

The empty set $\emptyset$ has cardinality zero and $\mathcal{P}(\emptyset) = \{\emptyset\}$, thus $|\mathcal{P}(\emptyset)| = 1$. For $M = \{1, 3\}$ the cardinality is $|M| = 2$ and

$$\mathcal{P}(M) = \{\emptyset, \{1\}, \{3\}, M\},$$

and hence $|\mathcal{P}(M)| = 4 = 2^{|M|}$. One can show that for every set M with finitely many elements, i.e., finite cardinality, $|\mathcal{P}(M)| = 2^{|M|}$ holds.

2.2 Maps

In this section we discuss maps between sets.

Definition 2.10 Let X, Y be nonempty sets.

(1) A *map* f from X to Y is a rule that assigns to each $x \in X$ exactly one $y = f(x) \in Y$. We write this as

$$f : X \to Y, \qquad x \mapsto y = f(x).$$

Instead of $x \mapsto y = f(x)$ we also write $f(x) = y$. The sets X and Y are called *domain* and *codomain* of f.
(2) Two maps $f : X \to Y$ and $g : X \to Y$ are called *equal* when $f(x) = g(x)$ holds for all $x \in X$. We then write $f = g$.

In Definition 2.10 we have assumed that X and Y are nonempty, since otherwise there can be no rule that assigns an element of Y to each element of X. If one of these sets is empty, one can define an *empty map*. However, in the following we will always assume (but not always explicitly state) that the sets between which a given map acts are nonempty.

Example 2.11 Two maps from $X = \mathbb{R}$ to $Y = \mathbb{R}$ are given by

$$f : X \to Y, \quad f(x) = x^2, \tag{2.1}$$

$$g : X \to Y, \quad x \mapsto \begin{cases} 0, & x \leq 0, \\ 1, & x > 0. \end{cases} \tag{2.2}$$

To analyze the properties of maps we need some further terminology.

Definition 2.12 Let X, Y be nonempty sets.

(1) The map $\mathrm{Id}_X : X \to X, x \mapsto x$, is called the *identity on* X.
(2) Let $f : X \to Y$ be a map and let $M \subseteq X$ and $N \subseteq Y$. Then

$$f(M) := \{ f(x) \mid x \in M \} \subseteq Y \quad \text{is called the } \textit{image} \text{ of } M \text{ under } f,$$
$$f^{-1}(N) := \{ x \in X \mid f(x) \in N \} \quad \text{is called the } \textit{pre-image} \text{ of } N \text{ under } f.$$

(3) If $f : X \to Y, x \mapsto f(x)$ is a map and $\emptyset \neq M \subseteq X$, then $f|_M : M \to Y$, $x \mapsto f(x)$, is called the *restriction of* f *to* M.

One should note that in this definition $f^{-1}(N)$ is a set, and hence the symbol f^{-1} here does not mean the inverse map of f. (This map will be introduced below in Definition 2.21.)

Example 2.13 For the maps with domain $X = \mathbb{R}$ in (2.1) and (2.2) we have the following properties:

$$f(X) = \{x \in \mathbb{R} \mid x \geq 0\}, \quad f^{-1}(\mathbb{R}_-) = \{0\}, \quad f^{-1}(\{-1\}) = \emptyset,$$
$$g(X) = \{0, 1\}, \quad g^{-1}(\mathbb{R}_-) = g^{-1}(\{0\}) = \mathbb{R}_-,$$

where $\mathbb{R}_- := \{x \in \mathbb{R} \mid x \leq 0\}$.

Definition 2.14 Let X, Y be nonempty sets. A map $f : X \to Y$ is called

(1) *injective*, if for all $x_1, x_2 \in X$ the equality $f(x_1) = f(x_2)$ implies that $x_1 = x_2$,
(2) *surjective*, if $f(X) = Y$,
(3) *bijective*, if f is injective and surjective.

For every nonempty set X the simplest example of a bijective map from X to X is Id_X, the identity on X.

Example 2.15 Let $\mathbb{R}_+ := \{x \in \mathbb{R} \mid x \geq 0\}$, then
$f : \mathbb{R} \to \mathbb{R}$, $f(x) = x^2$, is neither injective nor surjective.
$f : \mathbb{R} \to \mathbb{R}_+$, $f(x) = x^2$, is surjective but not injective.
$f : \mathbb{R}_+ \to \mathbb{R}$, $f(x) = x^2$, is injective but not surjective.
$f : \mathbb{R}_+ \to \mathbb{R}_+$, $f(x) = x^2$, is bijective.
In these assertions we have used the continuity of the map $f(x) = x^2$ that is discussed in the basic courses on analysis. In particular, we have used the fact that continuous functions map real intervals to real intervals. The assertions also show why it is important to include the domain and codomain in the definition of a map.

Theorem 2.16 *A map $f : X \to Y$ is bijective if and only if for every $y \in Y$ there exists exactly one $x \in X$ with $f(x) = y$.*

Proof $\Rightarrow$: Let f be bijective and let $y_1 \in Y$. Since f is surjective, there exists an $x_1 \in X$ with $f(x_1) = y_1$. If some $x_2 \in X$ also satisfies $f(x_2) = y_1$, then $x_1 = x_2$

follows from the injectivity of f. Therefore, there exists a unique $x_1 \in X$ with $f(x_1) = y_1$.

$\Leftarrow$: Since for all $y \in Y$ there exists a unique $x \in X$ with $f(x) = y$, it follows that $f(X) = Y$. Thus, f surjective. Let now $x_1, x_2 \in X$ with $f(x_1) = f(x_2) = y \in Y$. Then the assumption implies $x_1 = x_2$, so that f is also injective. □

One can show that between two sets X and Y of finite cardinality there exists a bijective map if and only if $|X| = |Y|$.

Lemma 2.17 *For sets X, Y with $|X| = |Y| = m \in \mathbb{N}$, there exist exactly $m! := 1 \cdot 2 \cdot \ldots \cdot m$ pairwise distinct bijective maps between X and Y.*

Proof Exercise. □

Definition 2.18 Let $f : X \to Y, x \mapsto f(x)$, and $g : Y \to Z, y \mapsto g(y)$ be maps. Then the *composition* of f and g is the map

$$g \circ f : X \to Z, \qquad x \mapsto g(f(x)).$$

The expression $g \circ f$ should be read "g after f", which stresses the order of the composition: First f is applied to x and then g to $f(x)$. One immediately sees that $f \circ \mathrm{Id}_X = f = \mathrm{Id}_Y \circ f$ for every map $f : X \to Y$.

Theorem 2.19 *Let $f : W \to X$, $g : X \to Y$, $h : Y \to Z$ be maps. Then*

(1) *$h \circ (g \circ f) = (h \circ g) \circ f$, i.e., the composition of maps is associative.*
(2) *If f and g are injective/surjective/bijective, then $g \circ f$ is injective/surjective/bijective.*

Proof Exercise. □

Theorem 2.20 *A map $f : X \to Y$ is bijective if and only if there exists a map $g : Y \to X$ with*

$$g \circ f = \mathrm{Id}_X \quad \textit{and} \quad f \circ g = \mathrm{Id}_Y.$$

Proof $\Rightarrow$: If f is bijective, then by Theorem 2.16 for every $y \in Y$ there exists an $x = x_y \in X$ with $f(x_y) = y$. We define the map g by

$$g : Y \to X, \quad g(y) = x_y.$$

Let $\widetilde{y} \in Y$ be given, then

$$(f \circ g)(\widetilde{y}) = f(g(\widetilde{y})) = f(x_{\widetilde{y}}) = \widetilde{y}, \quad \text{hence} \quad f \circ g = \mathrm{Id}_Y.$$

If, on the other hand, $\widetilde{x} \in X$ is given, then $\widetilde{y} = f(\widetilde{x}) \in Y$. By Theorem 2.16, there exists a unique $x_{\widetilde{y}} \in X$ with $f(x_{\widetilde{y}}) = \widetilde{y}$ such that $\widetilde{x} = x_{\widetilde{y}}$. So with

$$(g \circ f)(\widetilde{x}) = (g \circ f)(x_{\widetilde{y}}) = g(f(x_{\widetilde{y}})) = g(\widetilde{y}) = x_{\widetilde{y}} = \widetilde{x},$$

we have $g \circ f = \mathrm{Id}_X$.

$\Leftarrow$: By assumption $g \circ f = \mathrm{Id}_X$, thus $g \circ f$ is injective and thus also f is injective (see Exercise 2.7). Moreover, $f \circ g = \mathrm{Id}_Y$, thus $f \circ g$ is surjective and hence also f is surjective (see Exercise 2.7). Therefore, f is bijective. □

The map $g : Y \to X$ that was characterized in Theorem 2.20 is unique: If there were another map $h : Y \to X$ with $h \circ f = \mathrm{Id}_X$ and $f \circ h = \mathrm{Id}_Y$, then

$$h = \mathrm{Id}_X \circ h = (g \circ f) \circ h = g \circ (f \circ h) = g \circ \mathrm{Id}_Y = g.$$

This leads to the following definition.

Definition 2.21 If $f : X \to Y$ is a bijective map, then the unique map $g : Y \to X$ from Theorem 2.20 is called the *inverse* (or *inverse map*) of f. We denote the inverse of f by f^{-1}.

To show that a given map $g : Y \to X$ is the unique inverse of the bijective map $f : X \to Y$, it is sufficient to show one of the equations $g \circ f = \mathrm{Id}_X$ or $f \circ g = \mathrm{Id}_Y$. Indeed, if f is bijective and $g \circ f = \mathrm{Id}_X$, then

$$g = g \circ \mathrm{Id}_Y = g \circ (f \circ f^{-1}) = (g \circ f) \circ f^{-1} = \mathrm{Id}_X \circ f^{-1} = f^{-1}.$$

In the same way $g = f^{-1}$ follows from the assumption $f \circ g = \mathrm{Id}_Y$.

Theorem 2.22 *If $f : X \to Y$ and $g : Y \to Z$ are bijective maps, then the following assertions hold:*

(1) *f^{-1} is bijective with $(f^{-1})^{-1} = f$.*
(2) *$g \circ f$ is bijective with $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.*

Proof

(1) Exercise.
(2) We know from Theorem 2.19 that $g \circ f : X \to Z$ is bijective. Therefore, there exists a (unique) inverse of $g \circ f$. For the map $f^{-1} \circ g^{-1}$ we have

$$\begin{aligned}(f^{-1} \circ g^{-1}) \circ (g \circ f) &= f^{-1} \circ \big(g^{-1} \circ (g \circ f)\big) = f^{-1} \circ \big((g^{-1} \circ g) \circ f\big) \\ &= f^{-1} \circ (\mathrm{Id}_Y \circ f) = f^{-1} \circ f = \mathrm{Id}_X.\end{aligned}$$

Hence, $f^{-1} \circ g^{-1}$ is the inverse of $g \circ f$. □

2.3 Relations

We first introduce the cartesian product[3] of two sets.

[3] Named after René Descartes (1596–1650), the founder of Analytic Geometry. Georg Cantor (1845–1918) used in 1895 the name "connection set of M and N" and the notation $(M.N) = \{(m, n)\}$.

Definition 2.23 If M, N are nonempty sets, then the set

$$M \times N := \{(x, y) \mid x \in M \ \wedge \ y \in N\}$$

is the *cartesian product* of M and N. An element $(x, y) \in M \times N$ is called an *(ordered) pair*.

We can easily generalize this definition to $n \in \mathbb{N}$ nonempty sets $M_1, \ldots, M_n$:

$$M_1 \times \ldots \times M_n \ := \ \{(x_1, \ldots, x_n) \mid x_i \in M_i \ \text{ for } \ i = 1, \ldots, n\},$$

where an element $(x_1, \ldots, x_n) \in M_1 \times \cdots \times M_n$ is called an *(ordered) n-tuple*. The n-fold cartesian product of a single nonempty set M is

$$M^n := \underbrace{M \times \ldots \times M}_{n \text{ times}} = \{(x_1, \ldots, x_n) \mid x_i \in M \ \text{ for } \ i = 1, \ldots, n\}.$$

If in these definitions at least one of the sets is empty, then the resulting cartesian product is the empty set as well.

Definition 2.24 If M, N are nonempty sets then a set $R \subseteq M \times N$ is called a *relation* between M and N. If $M = N$, then R is called a relation on M. Instead of $(x, y) \in R$ we also write $x \sim_R y$ or $x \sim y$, if it is clear which relation is considered.

If in this definition at least one of the sets M and N is empty, then every relation between M and N is also the empty set, since then $M \times N = \emptyset$.

If, for instance $M = \mathbb{N}$ and $N = \mathbb{Q}$, then

$$R = \{(x, y) \in M \times N \mid xy = 1\}$$

is a relation between M and N that can be expressed as

$$R = \{(1, 1), (2, 1/2), (3, 1/3), \ldots\} = \{(n, 1/n) \mid n \in \mathbb{N}\}.$$

Definition 2.25 A relation R on a set M is called

(1) *reflexive*, if $x \sim x$ holds for all $x \in M$,
(2) *symmetric*, if $(x \sim y) \Rightarrow (y \sim x)$ holds for all $x, y \in M$,
(3) *transitive*, if $(x \sim y \ \wedge \ y \sim z) \Rightarrow (x \sim z)$ holds for all $x, y, z \in M$.

If R is reflexive, transitive and symmetric, then it is called an *equivalence relation* on M.

Example 2.26

(1) Let $R = \{(x, y) \in \mathbb{Q}^2 \mid x = -y\}$. Then R is not reflexive, since $x = -x$ holds only for $x = 0$. If $x = -y$, then also $y = -x$, and hence R is symmetric. Finally, R is not transitive. For example, $(x, y) = (1, -1) \in R$ and $(y, z) = (-1, 1) \in R$, but $(x, z) = (1, 1) \notin R$.

(2) The relation $R = \{(x, y) \in \mathbb{Z}^2 \mid x \leq y\}$ is reflexive and transitive, but not symmetric.
(3) If $f : \mathbb{R} \to \mathbb{R}$ is a map, then $R = \{(x, y) \in \mathbb{R}^2 \mid f(x) = f(y)\}$ is an equivalence relation on $\mathbb{R}$.

Definition 2.27 let R be an equivalence relation on the set M. Then, for $x \in M$ the set

$$[x]_R := \{y \in M \mid (x, y) \in R\} = \{y \in M \mid x \sim y\}$$

is called the *equivalence class of* x with respect to R. The set of equivalence classes

$$M/R := \{[x]_R \mid x \in M\}$$

is called the *quotient set* of M with respect to R.

The equivalence class $[x]_R$ of elements $x \in M$ is never the empty set, since always $x \sim x$ (reflexivity) and therefore $x \in [x]_R$. If it is clear which equivalence relation R is meant, we often write $[x]$ instead oft $[x]_R$ and also skip the additional "with respect to R".

Theorem 2.28 *If R is an equivalence relation on the set M and if $x, y \in M$, then the following are equivalent:*

(1) $[x] = [y]$.
(2) $[x] \cap [y] \neq \emptyset$.
(3) $x \sim y$.

Proof

(1) $\Rightarrow$ (2) : Since $x \sim x$, it follows that $x \in [x]$. From $[x] = [y]$ it follows that $x \in [y]$ and thus $x \in [x] \cap [y]$.
(2) $\Rightarrow$ (3) : Since $[x] \cap [y] \neq \emptyset$, there exists a $z \in [x] \cap [y]$. For this element z we have $x \sim z$ and $y \sim z$, and thus $x \sim z$ and $z \sim y$ (symmetry) and, therefore, $x \sim y$ (transitivity).
(3) $\Rightarrow$ (1) : Let $x \sim y$ and $z \in [x]$, i.e., $x \sim z$. Using symmetry and transitivity, we obtain $y \sim z$, and hence $z \in [y]$. This means that $[x] \subseteq [y]$. In an analogous way one shows that $[y] \subseteq [x]$, and hence $[x] = [y]$ holds. □

Theorem 2.28 shows that for two equivalence classes $[x]$ and $[y]$ we have either $[x] = [y]$ or $[x] \cap [y] = \emptyset$. Thus every $x \in M$ is contained in exactly one equivalence class (namely in $[x]$), so that an equivalence relation R yields a partitioning or decomposition of M into mutually disjoint subsets. Every element of $[x]$ is called a *representative* of the equivalence class $[x]$. A very useful and general approach that we will often use in this book is to partition a set of objects (e.g. sets of matrices) into equivalence classes, and to find in each such class a representative with a particularly simple structure. Such a representative is called a *normal form* with respect to the given equivalence relation.

Example 2.29 For a given number $n \in \mathbb{N}$ the set

$$R_n := \{(a, b) \in \mathbb{Z}^2 \mid a - b \text{ is divisible by } n \text{ without remainder}\}$$

is an equivalence relation on $\mathbb{Z}$, since the following properties hold:

- Reflexivity: $a - a = 0$ is divisible by n without remainder.
- Symmetry: If $a - b$ is divisible by n without remainder, then also $b - a$.
- Transitivity: Let $a - b$ and $b - c$ be divisible by n without remainder and write $a - c = (a - b) + (b - c)$. Both summands on the right are divisible by n without remainder and hence this also holds for $a - c$.

For $a \in \mathbb{Z}$ the equivalence class $[a]$ is called *residue class of a modulo n*, and $[a] = a + n\mathbb{Z} := \{a + nz \mid z \in \mathbb{Z}\}$. The equivalence relation R_n yields a partitioning of $\mathbb{Z}$ into n mutually disjoint subsets. In particular, we have

$$[0] \cup [1] \cup \cdots \cup [n-1] \;=\; \bigcup_{a=0}^{n-1} [a] \;=\; \mathbb{Z}.$$

The set of all residue classes modulo n, i.e., the quotient set with respect to R_n, is often denoted by $\mathbb{Z}/n\mathbb{Z}$. Thus, $\mathbb{Z}/n\mathbb{Z} := \{[0], [1], \ldots, [n-1]\}$. This set plays an important role in the mathematical field of Number Theory.

Exercises

2.1 Let A, B, C be assertions. Show that the following assertions are true:

(a) For $\wedge$ and $\vee$ the associative laws

$$[(A \wedge B) \wedge C] \;\Leftrightarrow\; [A \wedge (B \wedge C)], \qquad [(A \vee B) \vee C] \;\Leftrightarrow\; [A \vee (B \vee C)]$$

hold.

(b) For $\wedge$ and $\vee$ the commutative laws

$$(A \wedge B) \;\Leftrightarrow\; (B \wedge A), \qquad (A \vee B) \;\Leftrightarrow\; (B \vee A)$$

hold.

(c) For $\wedge$ and $\vee$ the distributive laws

$$[(A \wedge B) \vee C] \;\Leftrightarrow\; [(A \vee C) \wedge (B \vee C)], \qquad [(A \vee B) \wedge C] \;\Leftrightarrow\; [(A \wedge C) \vee (B \wedge C)]$$

hold.

2.2 Let A, B, C be assertions. Show that the following assertions are true:

(a) $A \wedge B \Rightarrow A$.

(b) $[A \Leftrightarrow B] \;\Leftrightarrow\; [(A \Rightarrow B) \wedge (B \Rightarrow A)]$.

(c) $\neg(A \vee B) \Leftrightarrow [(\neg A) \wedge (\neg B)]$.
(d) $\neg(A \wedge B) \Leftrightarrow [(\neg A) \vee (\neg B)]$.
(e) $[(A \Rightarrow B) \wedge (B \Rightarrow C)] \Rightarrow [A \Rightarrow C]$.
(f) $[A \Rightarrow (B \vee C)] \Leftrightarrow [(A \wedge \neg B) \Rightarrow C]$.

(The assertions (c) and (d) are called the *De Morgan laws* for $\wedge$ and $\vee$.)

2.3 Prove Theorem 2.8.

2.4 Show that for two sets M, N the following holds:

$$N \subseteq M \quad \Leftrightarrow \quad M \cap N = N \quad \Leftrightarrow \quad M \cup N = M.$$

2.5 Let X, Y be nonempty sets, $U, V \subseteq Y$ nonempty subsets and let $f : X \to Y$ be a map. Show that $f^{-1}(U \cap V) = f^{-1}(U) \cap f^{-1}(V)$. Let $U, V \subseteq X$ be nonempty. Check whether $f(U \cup V) = f(U) \cup f(V)$ holds.

2.6 Are the following maps injective, surjective, bijective?

(a) $f_1 : \mathbb{R} \setminus \{0\} \to \mathbb{R},\ x \mapsto \frac{1}{x}$.
(b) $f_2 : \mathbb{R}^2 \to \mathbb{R},\ (x, y) \mapsto x + y$.
(c) $f_3 : \mathbb{R}^2 \to \mathbb{R},\ (x, y) \mapsto x^2 + y^2 - 1$.
(d) $f_4 : \mathbb{N} \to \mathbb{Z},\ n \mapsto \begin{cases} \frac{n}{2}, & n \text{ even}, \\ -\frac{n-1}{2}, & n \text{ odd}. \end{cases}$

2.7 Show that for two maps $f : X \to Y$ and $g : Y \to Z$ the following assertions hold:

(a) $g \circ f$ is surjective $\Rightarrow$ g is surjective.
(b) $g \circ f$ is injective $\Rightarrow$ f is injective.

2.8 Let $a \in \mathbb{Z}$ be given. Show that the map $f_a : \mathbb{Z} \to \mathbb{Z}$, $f_a(x) = x + a$ is bijective.

2.9 Prove Lemma 2.17.

2.10 Prove Theorem 2.19.

2.11 Prove Theorem 2.22 (1).

2.12 Find two maps $f, g : \mathbb{N} \to \mathbb{N}$, so that simultaneously

(a) f is not surjective,
(b) g is not injective, and
(c) $g \circ f$ is bijective.

2.13 Determine all equivalence relations on the set $\{1, 2\}$.

2.14 Determine a symmetric and transitive relation on the set $\{a, b, c\}$ that is not reflexive.