Calculus I
for Computer Science and Statistics Students

Peter Philip*

Lecture Notes

Originally Created for the Class of Winter Semester 2010/2011 at LMU Munich,
Revised and Extended for Several Subsequent Classes

November 14, 2018

Contents

*E-Mail: philip@math.lmu.de

1 Foundations: Mathematical Logic and Set Theory

1.1 Introductory Remarks

The task of *mathematics* is to establish the truth or falsehood of (formalizable) statements using rigorous logic, and to provide methods for the solution of classes of (e.g. applied) problems, ideally including rigorous logical proofs verifying the validity of the methods (proofs that the method under consideration will, indeed, provide a correct solution).

The topic of this class is *calculus*, which is short for *infinitesimal calculus*, usually understood (as it is here) to mean differential and integral calculus of real and complex numbers (more generally, calculus may refer to any method or system of calculation guided by the symbolic manipulation of expressions, we will briefly touch on another example in Sec. 1.2 below). In that sense, calculus is the beginning part of the broader field of (mathematical) *analysis*, the section of mathematics concerned with the notion of a limit (for us, the most important examples will be limits of sequences (Def. 7.1 below) and limits of functions (Def. 8.17 below)).

Before we can properly define our first limit, however, it still needs some preparatory work. In modern mathematics, the objects under investigation are almost always so-called *sets*. So one aims at deriving (i.e. proving) true (and interesting and useful) statements about sets from other statements about sets known or assumed to be true. Such a derivation or proof means applying logical rules that guarantee the truth of the derived (i.e. proved) statement.

However, unfortunately, a proper definition of the notion of set is not easy, and neither is an appropriate treatment of logic and proof theory. Here, we will only be able to briefly touch on the bare necessities from logic and set theory needed to proceed to the core matter of this class. We begin with logic in Sec. 1.2, followed by set theory in Sec. 1.3, combining both in Sec. 1.4. The interested student can find an introductory presentation of axiomatic set theory in [Phi16, Sec. A] and he/she should consider taking a separate class on set theory, logic, and proof theory at a later time.

1.2 Propositional Calculus

1.2.1 Statements

Mathematical logic is a large field in its own right and, as indicated above, a thorough introduction is beyond the scope of this class – the interested reader may refer to [EFT07], [Kun12], and references therein. Here, we will just introduce some basic concepts using common English (rather than formal symbolic languages – a concept explained in books like [EFT07]).

As mentioned before, mathematics establishes the truth or falsehood of statements. By a *statement* or *proposition* we mean any sentence (any sequence of symbols) that can

reasonably be assigned a *truth value*, i.e. a value of either *true*, abbreviated T, or *false*, abbreviated F. The following example illustrates the difference between statements and sentences that are not statements:

Example 1.1. (a) Sentences that are statements:

Every dog is an animal. (T)
Every animal is a dog. (F)
The number 4 is odd. (F)
$2 + 3 = 5$. (T)
$\sqrt{2} < 0$. (F)
$x + 1 > 0$ holds for each natural number x. (T)

(b) Sentences that are *not* statements:

Let's study calculus!
Who are you?
$3 \cdot 5 + 7$.
$x + 1 > 0$.
All natural numbers are green.

The fourth sentence in Ex. 1.1(b) is not a statement, as it can not be said to be either true or false without any further knowledge on x. The fifth sentence in Ex. 1.1(b) is not a statement as it lacks any meaning and can, hence, not be either true or false. It would become a statement if given a definition of what it means for a natural number to be green.

1.2.2 Logical Operators

The next step now is to *combine* statements into new statements using *logical operators*, where the truth value of the combined statements depends on the truth values of the original statements and on the type of logical operator facilitating the combination.

The simplest logical operator is *negation*, denoted $\neg$. It is actually a so-called *unary* operator, i.e. it does not combine statements, but is merely applied to one statement. For example, if A stands for the statement "Every dog is an animal.", then $\neg A$ stands for the statement "Not every dog is an animal."; and if B stands for the statement "The number 4 is odd.", then $\neg B$ stands for the statement "The number 4 is not odd.", which can also be expressed as "The number 4 is even."

To completely understand the action of a logical operator, one usually writes what is known as a *truth table*. For negation, the truth table is

A	$\neg A$
T	F
F	T

(1.1)

that means if the input statement A is true, then the output statement $\neg A$ is false; if the input statement A is false, then the output statement $\neg A$ is true.

We now proceed to discuss *binary* logical operators, i.e. logical operators combining precisely two statements. The following four operators are essential for mathematical reasoning:

Conjunction: A *and* B, usually denoted $A \wedge B$.

Disjunction: A *or* B, usually denoted $A \vee B$.

Implication: A *implies* B, usually denoted $A \Rightarrow B$.

Equivalence: A is *equivalent* to B, usually denoted $A \Leftrightarrow B$.

Here is the corresponding truth table:

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

(1.2)

When first seen, some of the assignments of truth values in (1.2) might not be completely intuitive, due to the fact that logical operators are often used somewhat differently in common English. Let us consider each of the four logical operators of (1.2) in sequence:

For the use in subsequent examples, let $A_1, \ldots, A_6$ denote the six statements from Ex. 1.1(a).

Conjunction: Most likely the easiest of the four, basically identical to common language use: $A \wedge B$ is true if, and only if, both A and B are true. For example, using Ex. 1.1(a), $A_1 \wedge A_4$ is the statement "Every dog is an animal and $2 + 3 = 5$.", which is true since both A_1 and A_4 are true. On the other hand, $A_1 \wedge A_3$ is the statement "Every dog is an animal and the number 4 is odd.", which is false, since A_3 is false.

Disjunction: The disjunction $A \vee B$ is true if, and only if, at least one of the statements A, B is true. Here one already has to be a bit careful – $A \vee B$ defines the *inclusive* or, whereas "or" in common English is often understood to mean the exclusive or (which is false if both input statements are true). For example, using Ex. 1.1(a), $A_1 \vee A_4$ is the statement "Every dog is an animal or $2 + 3 = 5$.", which is true since both A_1 and A_4 are true. The statement $A_1 \vee A_3$, i.e. "Every dog is an animal or the number 4 is odd." is also true, since A_1 is true. However, the statement $A_2 \vee A_5$, i.e. "Every animal is a dog or $\sqrt{2} < 0$." is false, as both A_2 and A_5 are false.

As you will have noted in the above examples, logical operators can be applied to combine statements that have no obvious contents relation. While this might seem strange, introducing contents-related restrictions is unnecessary as well as undesirable, since it is often not clear which seemingly unrelated statements might suddenly appear in a common context in the future. The same occurs when considering implications and equivalences, where it might seem even more obscure at first.

Implication: Instead of A implies B, one also says *if A then B*, *B is a consequence of A*, *B is concluded or inferred from A*, *A is sufficient for B*, or *B is necessary for A*. The implication $A \Rightarrow B$ is always true, except if A is true and B is false. At first glance, it might be surprising that $A \Rightarrow B$ is defined to be true for A false and B true, however, there are many examples of incorrect statements implying correct statements. For instance, squaring the (false) equality of integers $-1 = 1$, implies the (true) equality of integers $1 = 1$. However, as with conjunction and disjunction, it is perfectly valid to combine statements without any obvious context relation: For example, using Ex. 1.1(a), the statement $A_1 \Rightarrow A_6$, i.e. "Every dog is an animal implies $x + 1 > 0$ holds for each natural number x." is true, since A_6 is true, whereas the statement $A_4 \Rightarrow A_2$, i.e. "$2 + 3 = 5$ implies every animal is a dog." is false, as A_4 is true and A_2 is false.

Of course, the implication $A \Rightarrow B$ is not really useful in situations, where the truth values of both A and B are already known. Rather, in a typical application, one tries to establish the truth of A to prove the truth of B (a strategy that will fail if A happens to be false).

Example 1.2. Suppose we know Sasha to be a member of a group of children. Then the statement A "Sasha is a girl." implies the statement B "There is at least one girl in the group." A priori, we might not know if Sasha is a girl or a boy, but if we can establish Sasha to be a girl, then we also know B to be true. If we find Sasha to be a boy, then we do not know, whether B is true or false.

—

Equivalence: $A \Leftrightarrow B$ means A is true if, and only if, B is true. Once again, using input statements from Ex. 1.1(a), we see that $A_1 \Leftrightarrow A_4$, i.e. "Every dog is an animal is equivalent to $2 + 3 = 5$.", is true as well as $A_2 \Leftrightarrow A_3$, i.e. "Every animal is a dog is equivalent to the number 4 is odd.". On the other hand, $A_4 \Leftrightarrow A_5$, i.e. "$2 + 3 = 5$ is equivalent to $\sqrt{2} < 0$, is false.

Analogous to the situation of implications, $A \Leftrightarrow B$ is not really useful if the truth values of both A and B are known a priori, but can be a powerful tool to prove B to be true or false by establishing the truth value of A. It is obviously more powerful than the implication as illustrated by the following example (compare with Ex. 1.2):

Example 1.3. Suppose we know Sasha is the tallest member of a group of children. Then the statement A "Sasha is a girl." is equivalent to the statement B "The tallest kid in the group is a girl." As in Ex. 1.2, if we can establish Sasha to be a girl, then we also know B to be true. However, in contrast to Ex. 1.2, if we find Sasha to be a boy, we know B to be false.

Remark 1.4. In computer science, the truth value T is often coded as 1 and the truth value F is often coded as 0.

1.2.3 Rules

Note that the expressions in the first row of the truth table (1.2) (e.g. $A \wedge B$) are *not* statements in the sense of Sec. 1.2.1, as they contain the *statement variables* (also known

as *propositional variables*) A or B. However, the expressions become statements if all statement variables are substituted with actual statements. We will call expressions of this form *propositional formulas*. Moreover, if a truth value is assigned to each statement variable of a propositional formula, then this uniquely determines the truth value of the formula. In other words, the truth value of the propositional formula can be *calculated* from the respective truth values of its statement variables – a first justification for the name *propositional calculus*.

Example 1.5. (a) Consider the propositional formula $(A \wedge B) \vee (\neg B)$. Suppose A is true and B is false. The truth value of the formula is obtained according to the following truth table:

A	B	$A \wedge B$	$\neg B$	$(A \wedge B) \vee (\neg B)$
T	F	F	T	T

(1.3)

(b) The propositional formula $A \vee (\neg A)$, also known as the *law of the excluded middle*, has the remarkable property that its truth value is T for every possible choice of truth values for A:

A	$\neg A$	$A \vee (\neg A)$
T	F	T
F	T	T

(1.4)

Formulas with this property are of particular importance.

Definition 1.6. A propositional formula is called a *tautology* or *universally true* if, and only if, its truth value is T for all possible assignments of truth values to all the statement variables it contains.

Notation 1.7. We write $\phi(A_1, \ldots, A_n)$ if, and only if, the propositional formula ϕ contains precisely the n statement variables $A_1, \ldots, A_n$.

Definition 1.8. The propositional formulas $\phi(A_1, \ldots, A_n)$ and $\psi(A_1, \ldots, A_n)$ are called *equivalent* if, and only if, $\phi(A_1, \ldots, A_n) \Leftrightarrow \psi(A_1, \ldots, A_n)$ is a tautology.

Lemma 1.9. *The propositional formulas $\phi(A_1, \ldots, A_n)$ and $\psi(A_1, \ldots, A_n)$ are equivalent if, and only if, they have the same truth value for all possible assignments of truth values to $A_1, \ldots, A_n$.*

Proof. If $\phi(A_1, \ldots, A_n)$ and $\psi(A_1, \ldots, A_n)$ are equivalent and A_i is assigned the truth value t_i, $i = 1, \ldots, n$, then $\phi(A_1, \ldots, A_n) \Leftrightarrow \psi(A_1, \ldots, A_n)$ being a tautology implies it has truth value T. From (1.2) we see that either $\phi(A_1, \ldots, A_n)$ and $\psi(A_1, \ldots, A_n)$ both have truth value T or they both have truth value F.

If, on the other hand, we know $\phi(A_1, \ldots, A_n)$ and $\psi(A_1, \ldots, A_n)$ have the same truth value for all possible assignments of truth values to $A_1, \ldots, A_n$, then, given such an assignment, either $\phi(A_1, \ldots, A_n)$ and $\psi(A_1, \ldots, A_n)$ both have truth value T or both have truth value F, i.e. $\phi(A_1, \ldots, A_n) \Leftrightarrow \psi(A_1, \ldots, A_n)$ has truth value T in each case, showing it is a tautology. ■

For all logical purposes, two equivalent formulas are exactly the same – it does not matter if one uses one or the other. The following theorem provides some important equivalences of propositional formulas. As too many parentheses tend to make formulas less readable, we first introduce some precedence conventions for logical operators:

Convention 1.10. $\neg$ takes precedence over $\wedge, \vee$, which take precedence over $\Rightarrow, \Leftrightarrow$. So, for example,

$$(A \vee \neg B \Rightarrow \neg B \wedge \neg A) \Leftrightarrow \neg C \wedge (A \vee \neg D)$$

is the same as

$$\Big(\big(A \vee (\neg B)\big) \Rightarrow \big((\neg B) \wedge (\neg A)\big)\Big) \Leftrightarrow \Big((\neg C) \wedge \big(A \vee (\neg D)\big)\Big).$$

Theorem 1.11. (a) $(A \Rightarrow B) \Leftrightarrow \neg A \vee B$. *This means one can actually define implication via negation and disjunction.*

(b) $(A \Leftrightarrow B) \Leftrightarrow \big((A \Rightarrow B) \wedge (B \Rightarrow A)\big)$, *i.e. A and B are equivalent if, and only if, A is both necessary and sufficient for B. One also calls the implication $B \Rightarrow A$ the* converse *of the implication $A \Rightarrow B$. Thus, A and B are equivalent if, and only if, both $A \Rightarrow B$ and its converse hold true.*

(c) *Commutativity of Conjunction:* $A \wedge B \Leftrightarrow B \wedge A$.

(d) *Commutativity of Disjunction:* $A \vee B \Leftrightarrow B \vee A$.

(e) *Associativity of Conjunction:* $(A \wedge B) \wedge C \Leftrightarrow A \wedge (B \wedge C)$.

(f) *Associativity of Disjunction:* $(A \vee B) \vee C \Leftrightarrow A \vee (B \vee C)$.

(g) *Distributivity I:* $A \wedge (B \vee C) \Leftrightarrow (A \wedge B) \vee (A \wedge C)$.

(h) *Distributivity II:* $A \vee (B \wedge C) \Leftrightarrow (A \vee B) \wedge (A \vee C)$.

(i) *De Morgan's Law I:* $\neg(A \wedge B) \Leftrightarrow \neg A \vee \neg B$.

(j) *De Morgan's Law II:* $\neg(A \vee B) \Leftrightarrow \neg A \wedge \neg B$.

(k) *Double Negative:* $\neg\neg A \Leftrightarrow A$.

(l) *Contraposition:* $(A \Rightarrow B) \Leftrightarrow (\neg B \Rightarrow \neg A)$.

Proof. Each equivalence is proved by providing a truth table and using Lem. 1.9.

(a):

A	B	$\neg A$	$A \Rightarrow B$	$\neg A \vee B$
T	T	F	T	T
T	F	F	F	F
F	T	T	T	T
F	F	T	T	T

(b) – (h): Exercise.

(i):

A	B	$\neg A$	$\neg B$	$A \wedge B$	$\neg(A \wedge B)$	$\neg A \vee \neg B$
T	T	F	F	T	F	F
T	F	F	T	F	T	T
F	T	T	F	F	T	T
F	F	T	T	F	T	T

(j): Exercise.

(k):

A	$\neg A$	$\neg\neg A$
T	F	T
F	T	F

(l):

A	B	$\neg A$	$\neg B$	$A \Rightarrow B$	$\neg B \Rightarrow \neg A$
T	T	F	F	T	T
T	F	F	T	F	F
F	T	T	F	T	T
F	F	T	T	T	T

Having checked all the rules completes the proof of the theorem. ■

The importance of the rules provided by Th. 1.11 lies in their providing *proof techniques*, i.e. methods for establishing the truth of statements from statements known or assumed to be true. The rules of Th. 1.11 will be used frequently in proofs throughout this class.

In subsequent proofs, we will also frequently use so-called transitivity of implication as well as transitivity of equivalence (we will encounter equivalence again in the context of relations in Sec. 1.3 below). In preparation for the transitivity rules, we generalize implication to propositional formulas:

Definition 1.12. In generalization of the implication operator defined in (1.2), we say the propositional formula $\phi(A_1, \ldots, A_n)$ *implies* the propositional formula $\psi(A_1, \ldots, A_n)$ (denoted $\phi(A_1, \ldots, A_n) \Rightarrow \psi(A_1, \ldots, A_n)$) if, and only if, each assignment of truth values to the $A_1, \ldots, A_n$ that makes $\phi(A_1, \ldots, A_n)$ true, makes $\psi(A_1, \ldots, A_n)$ true as well.

Theorem 1.13. (a) *Transitivity of Implication:* $(A \Rightarrow B) \wedge (B \Rightarrow C) \Rightarrow (A \Rightarrow C)$.

(b) *Transitivity of Equivalence:* $(A \Leftrightarrow B) \wedge (B \Leftrightarrow C) \Rightarrow (A \Leftrightarrow C)$.

Proof. According to Def. 1.12, the rules can be verified by providing truth tables that show that, for all possible assignments of truth values to the propositional formulas on the left-hand side of the implications, either the left-hand side is false or both sides are

true. (a):

A	B	C	$A \Rightarrow B$	$B \Rightarrow C$	$(A \Rightarrow B) \wedge (B \Rightarrow C)$	$A \Rightarrow C$
T	T	T	T	T	T	T
T	F	T	F	T	F	T
F	T	T	T	T	T	T
F	F	T	T	T	T	T
T	T	F	T	F	F	F
T	F	F	F	T	F	F
F	T	F	T	F	F	T
F	F	F	T	T	T	T

(b):

A	B	C	$A \Leftrightarrow B$	$B \Leftrightarrow C$	$(A \Leftrightarrow B) \wedge (B \Leftrightarrow C)$	$A \Leftrightarrow C$
T	T	T	T	T	T	T
T	F	T	F	F	F	T
F	T	T	F	T	F	F
F	F	T	T	F	F	F
T	T	F	T	F	F	F
T	F	F	F	T	F	F
F	T	F	F	F	F	T
F	F	F	T	T	T	T

Having checked both rules, the proof is complete. ■

Definition and Remark 1.14. A *proof* of the statement B is a finite sequence of statements $A_1, A_2, \ldots, A_n$ such that A_1 is true; for $1 \leq i < n$, A_i implies A_{i+1}, and A_n implies B. If there exists a proof for B, then Th. 1.13(a) guarantees that B is true.

1.3 Set Theory

In the previous section, we have had a first glance at statements and corresponding truth values. In the present section, we will move our focus to the objects such statements are about. Reviewing Example 1.1(a), and recalling that this is a mathematics class rather than one in zoology, the first two statements of Example 1.1(a) are less relevant for us than statements 3–6. As in these examples, we will nearly always be interested in statements involving numbers or collections of numbers or collections of such collections etc.

In modern mathematics, the term one usually uses instead of "collection" is "set". In 1895, Georg Cantor defined a set as "any collection into a whole M of definite and separate objects m of our intuition or our thought". The objects m are called the *elements* of the set M. As explained in [Phi16, Sec. A], without restrictions and refinements, Cantor's set theory is not free of contradictions and, thus, not viable to be used in the foundation of mathematics. Axiomatic set theory provides these necessary restrictions and refinements and an introductory treatment can also be found in [Phi16,

Sec. A]. However, it is possible to follow and understand the rest of this class, without having studied axiomatic set theory.

Notation 1.15. We write $m \in M$ for the statement "m is an element of the set M".

Definition 1.16. The sets M and N are equal, denoted $M = N$, if, and only if, M and N have precisely the same elements.

—

Definition 1.16 means we know everything about a set M if, and only if, we know all its elements.

Definition 1.17. The set with no elements is called the *empty set*; it is denoted by the symbol $\emptyset$.

Example 1.18. For finite sets, we can simply write down all its elements, for example, $A := \{0\}$, $B := \{0, 17.5\}$, $C := \{5, 1, 5, 3\}$, $D := \{3, 5, 1\}$, $E := \{2, \sqrt{2}, -2\}$, where the symbolism ":=" is to be read as "is defined to be equal to".

Note $C = D$, since both sets contain precisely the same elements. In particular, the order in which the elements are written down plays no role and a set does not change if an element is written down more than once.

If a set has many elements, instead of writing down all its elements, one might use abbreviations such as $F := \{-4, -2, \ldots, 20, 22, 24\}$, where one has to make sure the meaning of the dots is clear from the context.

Definition 1.19. The set A is called a *subset* of the set B (denoted $A \subseteq B$ and also referred to as the *inclusion* of A in B) if, and only if, every element of A is also an element of B (one sometimes also calls B a *superset* of A and writes $B \supseteq A$). Please note that $A = B$ is allowed in the above definition of a subset. If $A \subseteq B$ and $A \neq B$, then A is called a *strict* subset of B, denoted $A \subsetneq B$.

If B is a set and $P(x)$ is a statement about an element x of B (i.e., for each $x \in B$, $P(x)$ is either true or false), then we can define a subset A of B by writing

$$A := \{x \in B : P(x)\}. \tag{1.5}$$

This notation is supposed to mean that the set A consists precisely of those elements of B such that $P(x)$ is true (has the truth value T in the language of Sec. 1.2).

Example 1.20. (a) For each set A, one has $A \subseteq A$ and $\emptyset \subseteq A$.

(b) If $A \subseteq B$, then $A = \{x \in B : x \in A\}$.

(c) We have $\{3\} \subseteq \{6.7, 3, 0\}$. Letting $A := \{-10, -8, \ldots, 8, 10\}$, we have $\{-2, 0, 2\} = \{x \in A : x^3 \in A\}$, $\emptyset = \{x \in A : x + 21 \in A\}$.

Remark 1.21. As a consequence of Def. 1.16, the sets A and B are equal if, and only if, one has both inclusions, namely $A \subseteq B$ and $B \subseteq A$. Thus, when proving the equality of sets, one often divides the proof into two parts, first proving one inclusion, then the other.

Definition 1.22. **(a)** The *intersection* of the sets A and B, denoted $A \cap B$, consists of all elements that are in A and in B. The sets A, B are said to be *disjoint* if, and only if, $A \cap B = \emptyset$.

(b) The *union* of the sets A and B, denoted $A \cup B$, consists of all elements that are in A or in B (as in the logical disjunction in (1.2), the or is meant nonexclusively). If A and B are disjoint, one sometimes writes $A \dot\cup B$ and speaks of the *disjoint union* of A and B.

(c) The *difference* of the sets A and B, denoted $A \setminus B$ (read "A minus B" or "A without B"), consists of all elements of A that are not elements of B, i.e. $A \setminus B := \{x \in A : x \notin B\}$. If B is a subset of a given set A (sometimes called the *universe* in this context), then $A \setminus B$ is also called the *complement* of B with respect to A. In that case, one also writes $B^c := A \setminus B$ (note that this notation suppresses the dependence on A).

Example 1.23. **(a)** Examples of Intersections:

$$\{1,2,3\} \cap \{3,4,5\} = \{3\}, \tag{1.6a}$$

$$\{\sqrt{2}\} \cap \{1,2,\dots,10\} = \emptyset, \tag{1.6b}$$

$$\{-1,2,-3,4,5\} \cap \{-10,-9,\dots,-1\} \cap \{-1,7,-3\} = \{-1,-3\}. \tag{1.6c}$$

(b) Examples of Unions:

$$\{1,2,3\} \cup \{3,4,5\} = \{1,2,3,4,5\}, \tag{1.7a}$$

$$\{1,2,3\} \dot\cup \{4,5\} = \{1,2,3,4,5\}, \tag{1.7b}$$

$$\begin{aligned}\{-1,2,-3,4,5\} &\cup \{-99,-98,\dots,-1\} \cup \{-1,7,-3\} \\ &= \{-99,-98,\dots,-2,-1,2,4,5,7\}.\end{aligned} \tag{1.7c}$$

(c) Examples of Differences:

$$\{1,2,3\} \setminus \{3,4,5\} = \{1,2\}, \tag{1.8a}$$

$$\{1,2,3\} \setminus \{3,2,1,\sqrt{5}\} = \emptyset, \tag{1.8b}$$

$$\{-10,-9,\dots,9,10\} \setminus \{0\} = \{-10,-9,\dots,-1\} \cup \{1,2,\dots,9,10\}. \tag{1.8c}$$

With respect to the universe $\{1,2,3,4,5\}$, it is

$$\{1,2,3\}^c = \{4,5\}; \tag{1.8d}$$

with respect to the universe $\{0,1,\dots,20\}$, it is

$$\{1,2,3\}^c = \{0\} \cup \{4,5,\dots,20\}. \tag{1.8e}$$

As mentioned earlier, it will often be unavoidable to consider sets of sets. Here are first examples: $\big\{\emptyset, \{0\}, \{0,1\}\big\}$, $\big\{\{0,1\}, \{1,2\}\big\}$.

Definition 1.24. Given a set A, the set of all subsets of A is called the *power set* of A, denoted $\mathcal{P}(A)$ (for reasons explained later (cf. Prop. 2.17), the power set is sometimes also denoted as 2^A).

Example 1.25. Examples of Power Sets:

$$\mathcal{P}(\emptyset) = \{\emptyset\}, \tag{1.9a}$$

$$\mathcal{P}(\{0\}) = \big\{\emptyset, \{0\}\big\}, \tag{1.9b}$$

$$\mathcal{P}\big(\mathcal{P}(\{0\})\big) = \mathcal{P}\big(\big\{\emptyset, \{0\}\big\}\big) = \big\{\emptyset, \{\emptyset\}, \{\{0\}\}, \mathcal{P}(\{0\})\big\}. \tag{1.9c}$$

—

So far, we have restricted our set-theoretic examples to finite sets. However, not surprisingly, many sets of interest to us will be infinite (we will have to postpone a mathematically precise definition of finite and infinite to Sec. 3.2). We will now introduce the most simple infinite set.

Definition 1.26. The set $\mathbb{N} := \{1, 2, 3, \dots\}$ is called the set of *natural numbers*. Moreover, we define $\mathbb{N}_0 := \{0\} \cup \mathbb{N}$.

Remark 1.27. Mathematicians tend to desire as few fundamental objects as possible. One of the consequences is the idea to actually *define* numbers as special sets: $0 := \emptyset$, $1 := \{0\}$, $2 := \{0, 1\}$; in general, define the natural number $n := \{0, 1, \dots, n-1\} = (n-1) \cup \{n-1\}$.

—

The following theorem compiles important set-theoretic rules:

Theorem 1.28. *Let A, B, C, U be sets.*

(a) *Commutativity of Intersections: $A \cap B = B \cap A$.*

(b) *Commutativity of Unions: $A \cup B = B \cup A$.*

(c) *Associativity of Intersections: $(A \cap B) \cap C = A \cap (B \cap C)$.*

(d) *Associativity of Unions: $(A \cup B) \cup C = A \cup (B \cup C)$.*

(e) *Distributivity I: $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.*

(f) *Distributivity II: $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.*

(g) *De Morgan's Law I: $U \setminus (A \cap B) = (U \setminus A) \cup (U \setminus B)$.*

(h) *De Morgan's Law II: $U \setminus (A \cup B) = (U \setminus A) \cap (U \setminus B)$.*

(i) *Double Complement: If $A \subseteq U$, then $U \setminus (U \setminus A) = A$.*

Proof. In each case, the proof results from the corresponding rule of Th. 1.11:
(a):

$$x \in A \cap B \Leftrightarrow x \in A \wedge x \in B \overset{\text{Th. 1.11(c)}}{\Leftrightarrow} x \in B \wedge x \in A \Leftrightarrow x \in B \cap A.$$

(g): Under the general assumption of $x \in U$, we have the following equivalences:

$$x \in U \setminus (A \cap B) \Leftrightarrow \neg(x \in A \cap B) \Leftrightarrow \neg\big(x \in A \wedge x \in B\big) \overset{\text{Th. 1.11(i)}}{\Leftrightarrow} \neg(x \in A) \vee \neg(x \in B)$$
$$\Leftrightarrow x \in U \setminus A \vee x \in U \setminus B \Leftrightarrow x \in (U \setminus A) \cup (U \setminus B).$$

The proofs of the remaining rules are left as an exercise. ■

Remark 1.29. The correspondence between Th. 1.11 and Th. 1.28 is no coincidence. One can actually prove that, starting with an equivalence of propositional formulas $\phi(A_1, \ldots, A_n) \Leftrightarrow \psi(A_1, \ldots, A_n)$, where both formulas contain only the operators $\wedge, \vee, \neg$, one obtains a set-theoretic rule (stating an equality of sets) by reinterpreting all statement variables $A_1, \ldots, A_n$ as variables for sets, all subsets of a universe U, and replacing $\wedge$ by $\cap$, $\vee$ by $\cup$, and $\neg$ by $U\setminus$ (if there are no multiple negations, then we do not need the hypothesis that $A_1, \ldots, A_n$ are subsets of U). The procedure also works in the opposite direction – one can start with a set-theoretic formula for an equality of sets and translate it into two equivalent propositional formulas.

1.4 Predicate Calculus

Now that we have introduced sets in the previous section, we have to return to the subject of mathematical logic once more. As it turns out, propositional calculus, which we discussed in Sec. 1.2, does not quite suffice to develop the theory of calculus (nor most other mathematical theories). The reason is that we need to consider statements such as

$x + 1 > 0$ holds for each natural number x. (T)	(1.10a)
All real numbers are positive. (F)	(1.10b)
There exists a natural number bigger than 10. (T)	(1.10c)
There exists a real number x such that $x^2 = -1$. (F)	(1.10d)
For all natural numbers n, there exists a natural number bigger than n. (T)	(1.10e)

That means we are interested in statements involving *universal quantification* via the quantifier "for all" (one also often uses "for each" or "for every" instead), *existential quantification* via the quantifier "there exists", or both. The quantifier of universal quantification is denoted by $\forall$ and the quantifier of existential quantification is denoted by $\exists$. Using these symbols as well as $\mathbb{N}$ and $\mathbb{R}$ to denote the sets of natural and real

numbers, respectively, we can restate (1.10) as

$$\underset{x\in\mathbb{N}}{\forall} x+1>0. \text{ (T)} \tag{1.11a}$$

$$\underset{x\in\mathbb{R}}{\forall} x>0. \text{ (F)} \tag{1.11b}$$

$$\underset{n\in\mathbb{N}}{\exists} n>10. \text{ (T)} \tag{1.11c}$$

$$\underset{x\in\mathbb{R}}{\exists} x^2=-1. \text{ (F)} \tag{1.11d}$$

$$\underset{n\in\mathbb{N}}{\forall}\underset{m\in\mathbb{N}}{\exists} m>n. \text{ (T)} \tag{1.11e}$$

Definition 1.30. A *universal statement* has the form

$$\underset{x\in A}{\forall} P(x), \tag{1.12a}$$

whereas an *existential statement* has the form

$$\underset{x\in A}{\exists} P(x). \tag{1.12b}$$

In (1.12), A denotes a set and $P(x)$ is a sentence involving the variable x, a so-called *predicate* of x, that becomes a statement (i.e. becomes either true or false) if x is substituted with any concrete element of the set A (in particular, $P(x)$ is allowed to contain further quantifiers, but it must not contain any other quantifier involving x – one says x must be a *free* variable in $P(x)$, not bound by any quantifier in $P(x)$).

The universal statement (1.12a) has the truth value T if, and only if, $P(x)$ has the truth value T for *all* elements $x\in A$; the existential statement (1.12b) has the truth value T if, and only if, $P(x)$ has the truth value T for *at least one* element $x\in A$.

Remark 1.31. Some people prefer to write $\bigwedge_{x\in A}$ instead of $\underset{x\in A}{\forall}$ and $\bigvee_{x\in A}$ instead of $\underset{x\in A}{\exists}$. Even though this notation has the advantage of emphasizing that the universal statement can be interpreted as a big logical conjunction and the existential statement can be interpreted as a big logical disjunction, it is significantly less common. So we will stick to $\forall$ and $\exists$ in this class.

Remark 1.32. According to Def. 1.30, the existential statement (1.12b) is true if, and only if, $P(x)$ is true for at least one $x\in A$. So if there is precisely one such x, then (1.12b) is true; and if there are several different $x\in A$ such that $P(x)$ is true, then (1.12b) is still true. Uniqueness statements are often of particular importance, and one sometimes writes

$$\underset{x\in A}{\exists!} P(x) \tag{1.13}$$

for the statement "there exists a unique $x\in A$ such that $P(x)$ is true". This notation can be defined as an abbreviation for

$$\underset{x\in A}{\exists}\left(P(x)\wedge\underset{y\in A}{\forall}\big(P(y)\Rightarrow x=y\big)\right). \tag{1.14}$$

Example 1.33. Here are some examples of uniqueness statements:

$$\exists!_{n\in\mathbb{N}}\ n > 10. \text{ (F)} \tag{1.15a}$$

$$\exists!_{n\in\mathbb{N}}\ 12 > n > 10. \text{ (T)} \tag{1.15b}$$

$$\exists!_{n\in\mathbb{N}}\ 11 > n > 10. \text{ (F)} \tag{1.15c}$$

$$\exists!_{x\in\mathbb{R}}\ x^2 = -1. \text{ (F)} \tag{1.15d}$$

$$\exists!_{x\in\mathbb{R}}\ x^2 = 1. \text{ (F)} \tag{1.15e}$$

$$\exists!_{x\in\mathbb{R}}\ x^2 = 0. \text{ (T)} \tag{1.15f}$$

Remark 1.34. As for propositional calculus, we also have some important rules for predicate calculus:

(a) Consider the negation of a universal statement, $\neg \underset{x\in A}{\forall} P(x)$, which is true if, and only if, $P(x)$ does *not* hold for each $x \in A$, i.e. if, and only if, there exists at least one $x \in A$ such that $P(x)$ is false (such that $\neg P(x)$ is true). We have just proved the rule

$$\neg \underset{x\in A}{\forall} P(x) \ \Leftrightarrow\ \underset{x\in A}{\exists} \neg P(x). \tag{1.16a}$$

Similarly, consider the negation of an existential statement. We claim the corresponding rule is

$$\neg \underset{x\in A}{\exists} P(x) \ \Leftrightarrow\ \underset{x\in A}{\forall} \neg P(x). \tag{1.16b}$$

Indeed, we can prove (1.16b) from (1.16a):

$$\neg \underset{x\in A}{\exists} P(x) \overset{\text{Th. 1.11(k)}}{\Leftrightarrow} \neg \underset{x\in A}{\exists} \neg\neg P(x) \overset{(1.16a)}{\Leftrightarrow} \neg\neg \underset{x\in A}{\forall} \neg P(x) \overset{\text{Th. 1.11(k)}}{\Leftrightarrow} \underset{x\in A}{\forall} \neg P(x). \tag{1.17}$$

One can interpret (1.16) as a generalization of the De Morgan's laws Th. 1.11(i),(j).

One can actually generalize (1.16) even a bit more: If a statement starts with several quantifiers, then one negates the statement by replacing each $\forall$ with $\exists$ and vice versa plus negating the predicate after the quantifiers (see the example in (1.20e) below).

(b) If A, B are sets and $P(x, y)$ denotes a predicate of both x and y, then $\underset{x\in A}{\forall} \underset{y\in B}{\forall} P(x, y)$ and $\underset{y\in B}{\forall} \underset{x\in A}{\forall} P(x, y)$ both hold true if, and only if, $P(x, y)$ holds true for each $x \in A$ and each $y \in B$, i.e. the order of two consecutive universal quantifiers does not matter:

$$\underset{x\in A}{\forall} \underset{y\in B}{\forall} P(x, y) \ \Leftrightarrow\ \underset{y\in B}{\forall} \underset{x\in A}{\forall} P(x, y) \tag{1.18a}$$

In the same way, we obtain the following rule:

$$\underset{x\in A}{\exists} \underset{y\in B}{\exists} P(x, y) \ \Leftrightarrow\ \underset{y\in B}{\exists} \underset{x\in A}{\exists} P(x, y). \tag{1.18b}$$

If $A = B$, one also uses abbreviations of the form

$$\underset{x,y\in A}{\forall} P(x,y) \quad \text{for} \quad \underset{x\in A}{\forall}\,\underset{y\in A}{\forall} P(x,y), \tag{1.19a}$$

$$\underset{x,y\in A}{\exists} P(x,y) \quad \text{for} \quad \underset{x\in A}{\exists}\,\underset{y\in A}{\exists} P(x,y). \tag{1.19b}$$

Generalizing rules (1.18), we can always commute *identical* quantifiers. Caveat: Quantifiers that are not identical must not be commuted (see Ex. 1.35(d) below).

Example 1.35. (a) Negation of universal and existential statements:

$$\text{Negation of (1.11a):} \quad \underset{x\in\mathbb{N}}{\exists} \overbrace{x+1\le 0}^{\neg(x+1>0)}. \text{ (F)} \tag{1.20a}$$

$$\text{Negation of (1.11b):} \quad \underset{x\in\mathbb{R}}{\exists} \overbrace{x\le 0}^{\neg(x>0)}. \text{ (T)} \tag{1.20b}$$

$$\text{Negation of (1.11c):} \quad \underset{n\in\mathbb{N}}{\forall} \overbrace{n\le 10}^{\neg(n>10)}. \text{ (F)} \tag{1.20c}$$

$$\text{Negation of (1.11d):} \quad \underset{x\in\mathbb{R}}{\forall} \overbrace{x^2\ne -1}^{\neg(x^2=-1)}. \text{ (T)} \tag{1.20d}$$

$$\text{Negation of (1.11e):} \quad \underset{n\in\mathbb{N}}{\exists}\,\underset{m\in\mathbb{N}}{\forall} \overbrace{m\le n}^{\neg(m>n)}. \text{ (F)} \tag{1.20e}$$

(b) As a more complicated example, consider the negation of the uniqueness statement (1.13), i.e. of (1.14):

$$\begin{aligned}
\neg\,\underset{x\in A}{\exists!}\,P(x) \quad &\Leftrightarrow \quad \neg\,\underset{x\in A}{\exists}\Big(P(x)\wedge\underset{y\in A}{\forall}\big(P(y)\Rightarrow x=y\big)\Big)\\
&\overset{\text{(1.16b), Th. 1.11(a)}}{\Leftrightarrow} \underset{x\in A}{\forall}\neg\Big(P(x)\wedge\underset{y\in A}{\forall}\big(\neg P(y)\vee x=y\big)\Big)\\
&\overset{\text{Th. 1.11(i)}}{\Leftrightarrow} \underset{x\in A}{\forall}\Big(\neg P(x)\vee\neg\underset{y\in A}{\forall}\big(\neg P(y)\vee x=y\big)\Big)\\
&\overset{\text{(1.16a)}}{\Leftrightarrow} \underset{x\in A}{\forall}\Big(\neg P(x)\vee\underset{y\in A}{\exists}\neg\big(\neg P(y)\vee x=y\big)\Big)\\
&\overset{\text{Th. 1.11(j),(k)}}{\Leftrightarrow} \underset{x\in A}{\forall}\Big(\neg P(x)\vee\underset{y\in A}{\exists}\big(P(y)\wedge x\ne y\big)\Big)\\
&\overset{\text{Th. 1.11(a)}}{\Leftrightarrow} \underset{x\in A}{\forall}\Big(P(x)\Rightarrow\underset{y\in A}{\exists}\big(P(y)\wedge x\ne y\big)\Big).
\end{aligned} \tag{1.21}$$

So how to decode the expression, we have obtained at the end? It states that if $P(x)$ holds for some $x\in A$, then there must be at least a second, different, element $y\in A$ such that $P(y)$ is true. This is, indeed, precisely the negation of $\underset{x\in A}{\exists!}\,P(x)$.

(c) Identical quantifiers commute:

$$\underset{x\in\mathbb{R}}{\forall}\,\underset{n\in\mathbb{N}}{\forall}\,x^{2n}\ge 0 \;\Leftrightarrow\; \underset{n\in\mathbb{N}}{\forall}\,\underset{x\in\mathbb{R}}{\forall}\,x^{2n}\ge 0, \tag{1.22a}$$

$$\underset{x\in\mathbb{R}}{\forall}\,\underset{y\in\mathbb{R}}{\exists}\,\underset{n\in\mathbb{N}}{\exists}\,ny>x^2 \;\Leftrightarrow\; \underset{x\in\mathbb{R}}{\forall}\,\underset{n\in\mathbb{N}}{\exists}\,\underset{y\in\mathbb{R}}{\exists}\,ny>x^2. \tag{1.22b}$$

(d) The following example shows that different quantifiers do, in general, not commute (i.e. do not yield equivalent statements when commuted): While the statement

$$\underset{x\in\mathbb{R}}{\forall}\ \underset{y\in\mathbb{R}}{\exists}\ y > x \tag{1.23a}$$

is true (for each real number x, there is a bigger real number y, e.g. $y := x + 1$ will do the job), the statement

$$\underset{y\in\mathbb{R}}{\exists}\ \underset{x\in\mathbb{R}}{\forall}\ y > x \tag{1.23b}$$

is false (for example, since $y > y$ is false). In particular, (1.23a) and (1.23b) are not equivalent.

(e) Even though (1.13) provides useful notation, it is better not to think of $\exists!$ as a quantifier. It is really just an abbreviation for (1.14), and it behaves very differently from $\exists$ and $\forall$: The following examples show that, in general, $\exists!$ commutes neither with $\exists$, nor with itself:

$$\underset{n\in\mathbb{N}}{\exists}\ \underset{m\in\mathbb{N}}{\exists!}\ m < n \not\Leftrightarrow \underset{m\in\mathbb{N}}{\exists!}\ \underset{n\in\mathbb{N}}{\exists}\ m < n$$

(the statement on the left is true, as one can choose $n = 2$, but the statement on the right is false, as $\underset{n\in\mathbb{N}}{\exists}\ m < n$ holds for every $m \in \mathbb{N}$). Similarly,

$$\underset{n\in\mathbb{N}}{\exists!}\ \underset{m\in\mathbb{N}}{\exists!}\ m < n \not\Leftrightarrow \underset{m\in\mathbb{N}}{\exists!}\ \underset{n\in\mathbb{N}}{\exists!}\ m < n$$

(the statement on the left is still true and the statement on the right is still false (there is no $m \in \mathbb{N}$ such that $\underset{n\in\mathbb{N}}{\exists!}\ m < n$)).

Remark 1.36. One can make the following observations regarding the strategy for proving universal and existential statements:

(a) To prove that $\underset{x\in A}{\forall}\ P(x)$ is true, one must check the truth of $P(x)$ for every element $x \in A$ – examples are *not* enough!

(b) To prove that $\underset{x\in A}{\forall}\ P(x)$ is false, it suffices to find *one* $x \in A$ such that $P(x)$ is false – such an x is then called a *counterexample* and *one* counterexample is always enough to prove $\underset{x\in A}{\forall}\ P(x)$ is false!

(c) To prove that $\underset{x\in A}{\exists}\ P(x)$ is true, it suffices to find *one* $x \in A$ such that $P(x)$ is true – such an x is then called an *example* and *one* example is always enough to prove $\underset{x\in A}{\exists}\ P(x)$ is true!

—

The subfield of mathematical logic dealing with quantified statements is called *predicate calculus*. In general, one does not restrict the quantified variables to range only over elements of sets (as we have done above). Again, we refer to [EFT07] for a deeper treatment of the subject.

As an application of quantified statements, let us generalize the notion of union and intersection:

Definition 1.37. Let $I \neq \emptyset$ be a nonempty set, usually called an *index set* in the present context. For each $i \in I$, let A_i denote a set (some or all of the A_i can be identical).

(a) The *intersection*

$$\bigcap_{i\in I} A_i := \left\{ x : \underset{i\in I}{\forall}\, x \in A_i \right\} \tag{1.24a}$$

consists of all elements x that belong to every A_i.

(b) The *union*

$$\bigcup_{i\in I} A_i := \left\{ x : \underset{i\in I}{\exists}\, x \in A_i \right\} \tag{1.24b}$$

consists of all elements x that belong to at least one A_i. The union is called *disjoint* if, and only if, for each $i, j \in I$, $i \neq j$ implies $A_i \cap A_j = \emptyset$.

Proposition 1.38. *Let $I \neq \emptyset$ be an index set, let M denote a set, and, for each $i \in I$, let A_i denote a set. The following set-theoretic rules hold:*

(a) $\left(\bigcap_{i\in I} A_i\right) \cap M = \bigcap_{i\in I} (A_i \cap M)$.

(b) $\left(\bigcup_{i\in I} A_i\right) \cup M = \bigcup_{i\in I} (A_i \cup M)$.

(c) $\left(\bigcap_{i\in I} A_i\right) \cup M = \bigcap_{i\in I} (A_i \cup M)$.

(d) $\left(\bigcup_{i\in I} A_i\right) \cap M = \bigcup_{i\in I} (A_i \cap M)$.

(e) $M \setminus \bigcap_{i\in I} A_i = \bigcup_{i\in I} (M \setminus A_i)$.

(f) $M \setminus \bigcup_{i\in I} A_i = \bigcap_{i\in I} (M \setminus A_i)$.

Proof. We prove (c) and (e) and leave the remaining proofs as an exercise.

(c):

$$x \in \Big(\bigcap_{i\in I} A_i\Big) \cup M \;\Leftrightarrow\; x \in M \vee \underset{i\in I}{\forall}\, x \in A_i \overset{(*)}{\Leftrightarrow} \underset{i\in I}{\forall} \big(x \in A_i \vee x \in M\big)$$
$$\Leftrightarrow\; x \in \bigcap_{i\in I} (A_i \cup M).$$

To justify the equivalence at $(*)$, we make use of Th. 1.11(b) and verify $\Rightarrow$ and $\Leftarrow$. For $\Rightarrow$ note that the truth of $x \in M$ implies $x \in A_i \vee x \in M$ is true for each $i \in I$. If $x \in A_i$ is true for each $i \in I$, then $x \in A_i \vee x \in M$ is still true for each $i \in I$. To verify $\Leftarrow$, note that the existence of $i \in I$ such that $x \in M$ implies the truth of $x \in M \vee \underset{i\in I}{\forall}\, x \in A_i$. If $x \in M$ is false for each $i \in I$, then $x \in A_i$ must be true for each $i \in I$, showing $x \in M \vee \underset{i\in I}{\forall}\, x \in A_i$ is true also in this case.

(e):

$$x \in M \setminus \bigcap_{i\in I} A_i \Leftrightarrow\; x \in M \wedge \neg \underset{i\in I}{\forall}\, x \in A_i \;\Leftrightarrow\; x \in M \wedge \underset{i\in I}{\exists}\, x \notin A_i$$
$$\Leftrightarrow\; \underset{i\in I}{\exists}\, x \in M \setminus A_i \;\Leftrightarrow\; x \in \bigcup_{i\in I} (M \setminus A_i),$$

completing the proof. ■

Example 1.39. We have the following identities of sets:

$$\bigcap_{x\in\mathbb{R}} \mathbb{N} = \mathbb{N}, \tag{1.25a}$$
$$\bigcap_{n\in\mathbb{N}} \{1, 2, \dots, n\} = \{1\}, \tag{1.25b}$$
$$\bigcup_{x\in\mathbb{R}} \mathbb{N} = \mathbb{N}, \tag{1.25c}$$
$$\bigcup_{n\in\mathbb{N}} \{1, 2, \dots, n\} = \mathbb{N}, \tag{1.25d}$$
$$\mathbb{N} \setminus \bigcup_{n\in\mathbb{N}} \{2n\} = \{1, 3, 5, \dots\} = \bigcap_{n\in\mathbb{N}} \big(\mathbb{N} \setminus \{2n\}\big). \tag{1.25e}$$

Comparing with the notation of Def. 1.37, in (1.25a), for example, we have $I = \mathbb{R}$ and $A_i = \mathbb{N}$ for each $i \in I$ (where, in (1.25a), we have written x instead of i). Similarly, in (1.25b), we have $I = \mathbb{N}$ and $A_n = \{1, 2, \dots, n\}$ for each $n \in I$.

2 Functions and Relations

2.1 Functions

Definition 2.1. Let A, B be sets. Given $x \in A$, $y \in B$, the set

$$(x, y) := \Big\{\{x\}, \{x, y\}\Big\} \tag{2.1}$$

is called the *ordered pair* (often shortened to just *pair*) consisting of x and y. The set of all such pairs is called the Cartesian product $A \times B$, i.e.

$$A \times B := \{(x, y) : x \in A \wedge y \in B\}. \tag{2.2}$$

Example 2.2. Let A be a set.

$$A \times \emptyset = \emptyset \times A = \emptyset, \tag{2.3a}$$
$$\{1, 2\} \times \{1, 2, 3\} = \{(1, 1), (1, 2), (1, 3), (2, 1), (2, 2), (2, 3)\} \tag{2.3b}$$
$$\neq \{1, 2, 3\} \times \{1, 2\} = \{(1, 1), (1, 2), (2, 1), (2, 2), (3, 1), (3, 2)\}. \tag{2.3c}$$

Also note that, for $x \neq y$,

$$(x, y) = \big\{\{x\}, \{x, y\}\big\} \neq \big\{\{y\}, \{x, y\}\big\} = (y, x). \tag{2.4}$$

Definition 2.3. Given sets A, B, a *function* or *map* f is an assignment rule that assigns to each $x \in A$ a unique $y \in B$. One then also writes $f(x)$ for the element y. The set A is called the *domain* of f, denoted $\mathcal{D}(f)$, and B is called the *range* of f, denoted $\mathcal{R}(f)$. The information about a map f can be concisely summarized by the notation

$$f : A \longrightarrow B, \quad x \mapsto f(x), \tag{2.5}$$

where $x \mapsto f(x)$ is called the *assignment rule* for f, $f(x)$ is called the *image* of x, and x is called a *preimage* of $f(x)$ (the image must be unique, but there might be several preimages). The set

$$\operatorname{graph}(f) := \big\{(x, y) \in A \times B : y = f(x)\big\} \tag{2.6}$$

is called the *graph* of f (not to be confused with pictures visualizing the function f, which are also called graph of f). If one wants to be completely precise, then one identifies the function f with the ordered triple $(A, B, \operatorname{graph}(f))$.

The set of all functions with domain A and range B is denoted by $\mathcal{F}(A, B)$ or B^A, i.e.

$$\mathcal{F}(A, B) := B^A := \big\{(f : A \longrightarrow B) : A = \mathcal{D}(f) \wedge B = \mathcal{R}(f)\big\}. \tag{2.7}$$

Caveat: Some authors reserve the word *map* for continuous functions, but we use function and map synonymously.

Definition 2.4. Let A, B be sets and $f : A \longrightarrow B$ a function.

(a) If T is a subset of A, then

$$f(T) := \{f(x) \in B : x \in T\} \tag{2.8}$$

is called the *image* of T under f.

(b) If U is a subset of B, then

$$f^{-1}(U) := \{x \in A : f(x) \in U\} \tag{2.9}$$

is called the *preimage* or *inverse image* of U under f.

(c) f is called *injective* or *one-to-one* if, and only if, every $y \in B$ has at most one preimage, i.e. if, and only if, the preimage of $\{y\}$ has at most one element:

$$\begin{aligned} f \text{ injective} \quad &\Leftrightarrow \quad \underset{y\in B}{\forall} \left(f^{-1}\{y\} = \emptyset \vee \underset{x\in A}{\exists!}\, f(x) = y \right) \\ &\Leftrightarrow \quad \underset{x_1,x_2\in A}{\forall} \big(x_1 \neq x_2 \;\Rightarrow f(x_1) \neq f(x_2) \big). \end{aligned} \tag{2.10}$$

(d) f is called *surjective* or *onto* if, and only if, every element of the range of f has a preimage:

$$f \text{ surjective} \quad \Leftrightarrow \quad \underset{y\in B}{\forall}\, \underset{x\in A}{\exists}\, y = f(x) \quad \Leftrightarrow \quad \underset{y\in B}{\forall}\, f^{-1}\{y\} \neq \emptyset. \tag{2.11}$$

(e) f is called *bijective* if, and only if, f is injective and surjective.

Example 2.5. Examples of Functions:

$$f : \{1,2,3,4,5\} \longrightarrow \{1,2,3,4,5\}, \qquad f(x) := -x + 6, \tag{2.12a}$$

$$g : \mathbb{N} \longrightarrow \mathbb{N}, \qquad g(n) := 2n, \tag{2.12b}$$

$$h : \mathbb{N} \longrightarrow \{2,4,6,\dots\}, \qquad h(n) := 2n, \tag{2.12c}$$

$$\tilde{h} : \mathbb{N} \longrightarrow \{2,4,6,\dots\}, \qquad \tilde{h}(n) := \begin{cases} n & \text{for } n \text{ even}, \\ n+1 & \text{for } n \text{ odd}, \end{cases} \tag{2.12d}$$

$$G : \mathbb{N} \longrightarrow \mathbb{R}, \qquad G(n) := n/(n+1), \tag{2.12e}$$

$$F : \mathcal{P}(\mathbb{N}) \longrightarrow \mathcal{P}\big(\mathcal{P}(\mathbb{N})\big), \qquad F(A) := \mathcal{P}(A). \tag{2.12f}$$

Instead of $f(x) := -x + 6$ in (2.12a), one can also write $x \mapsto -x + 6$ and analogously in the other cases. Also note that, in the strict sense, functions g and h are different, since their ranges are different (however, using the following Def. 2.4(a), they have the same *image* in the sense that $g(\mathbb{N}) = h(\mathbb{N})$). Furthermore,

$$f(\{1,2\}) = \{5,4\} = f^{-1}(\{1,2\}), \quad \tilde{h}^{-1}(\{2,4,6\}) = \{1,2,3,4,5,6\}, \tag{2.13}$$

f is bijective; g is injective, but not surjective; h is bijective; $\tilde{h}$ is surjective, but not injective. Can you figure out if G and F are injective and/or surjective?

Example 2.6. (a) For each nonempty set A, the map $\mathrm{Id} : A \longrightarrow A$, $\mathrm{Id}(x) := x$, is called the *identity* on A. If one needs to emphasize that Id operates on A, then one also writes Id_A instead of Id. The identity is clearly bijective.

(b) Let A, B be nonempty sets. A map $f : A \longrightarrow B$ is called *constant* if, and only if, there exists $c \in B$ such that $f(x) = c$ for each $x \in A$. In that case, one also writes $f \equiv c$, which can be read as "f is identically equal to c". If $f \equiv c$, $\emptyset \neq T \subseteq A$, and $U \subseteq B$, then

$$f(T) = \{c\}, \quad f^{-1}(U) = \begin{cases} A & \text{for } c \in U, \\ \emptyset & \text{for } c \notin U. \end{cases} \tag{2.14}$$

f is injective if, and only if, $A = \{x\}$; f is surjective if, and only if, $B = \{c\}$.

(c) Given $A \subseteq X$, the map

$$\iota : A \longrightarrow X, \quad \iota(x) := x, \tag{2.15}$$

is called *inclusion* (also *embedding* or *imbedding*). An inclusion is always injective; it is surjective if, and only if $A = X$, i.e. if, and only if, it is the identity on A.

(d) Given $A \subseteq X$ and a map $f : X \longrightarrow B$, the map $g : A \longrightarrow B$, $g(x) = f(x)$, is called the *restriction* of f to A; f is called the *extension* of g to X. In this situation, one also uses the notation $f\restriction_A$ for g (some authors prefer the notation $f|_A$ or $f|A$).

There are several important rules regarding functions and set-theoretic operations. However, we will not make use of them in this class, and the interested student can find them in [Phi16, Th. 2.7].

Definition 2.7. The *composition* of maps f and g with $f : A \longrightarrow B$, $g : C \longrightarrow D$, and $f(A) \subseteq C$ is defined to be the map

$$g \circ f : A \longrightarrow D, \quad (g \circ f)(x) := g\big(f(x)\big). \tag{2.16}$$

The expression $g \circ f$ is read as "g after f" or "g composed with f".

Example 2.8. Consider the maps

$$f : \mathbb{N} \longrightarrow \mathbb{R}, \qquad n \mapsto n^2, \tag{2.17a}$$
$$g : \mathbb{N} \longrightarrow \mathbb{R}, \qquad n \mapsto 2n. \tag{2.17b}$$

We obtain $f(\mathbb{N}) = \{1, 4, 9, \dots\} \subseteq \mathcal{D}(g)$, $g(\mathbb{N}) = \{2, 4, 6, \dots\} \subseteq \mathcal{D}(f)$, and the compositions

$$(g \circ f) : \mathbb{N} \longrightarrow \mathbb{R}, \qquad (g \circ f)(n) = g(n^2) = 2n^2, \tag{2.18a}$$
$$(f \circ g) : \mathbb{N} \longrightarrow \mathbb{R}, \qquad (f \circ g)(n) = f(2n) = 4n^2, \tag{2.18b}$$

showing that composing functions is, in general, not commutative, even if the involved functions have the same domain and the same range.

Proposition 2.9. *Consider maps $f : A \longrightarrow B$, $g : C \longrightarrow D$, $h : E \longrightarrow F$, satisfying $f(A) \subseteq C$ and $g(C) \subseteq E$.*

(a) *Associativity of Compositions:*

$$h \circ (g \circ f) = (h \circ g) \circ f. \tag{2.19}$$

(b) *One has the following law for forming preimages:*

$$\underset{W \in \mathcal{P}(D)}{\forall} (g \circ f)^{-1}(W) = f^{-1}(g^{-1}(W)). \tag{2.20}$$

Proof. (a): Both $h \circ (g \circ f)$ and $(h \circ g) \circ f$ map A into F. So it just remains to prove $\big(h \circ (g \circ f)\big)(x) = \big((h \circ g) \circ f\big)(x)$ for each $x \in A$. One computes, for each $x \in A$,

$$\begin{aligned}\big(h \circ (g \circ f)\big)(x) &= h\big((g \circ f)(x)\big) = h\big(g(f(x))\big) = (h \circ g)(f(x)) \\ &= \big((h \circ g) \circ f\big)(x),\end{aligned} \tag{2.21}$$

establishing the case.

(b): Exercise. ■

Definition 2.10. A function $g : B \longrightarrow A$ is called a *right inverse* (resp. *left inverse*) of a function $f : A \longrightarrow B$ if, and only if, $f \circ g = \mathrm{Id}_B$ (resp. $g \circ f = \mathrm{Id}_A$). Moreover, g is called an *inverse* of f if, and only if, it is both a right and a left inverse. If g is an inverse of f, then one also writes f^{-1} instead of g. The map f is called (*right*, *left*) *invertible* if, and only if, there exists a (right, left) inverse for f.

Example 2.11. (a) Consider the map

$$f : \mathbb{N} \longrightarrow \mathbb{N}, \quad f(n) := 2n. \tag{2.22a}$$

The maps

$$g_1 : \mathbb{N} \longrightarrow \mathbb{N}, \quad g_1(n) := \begin{cases} n/2 & \text{if } n \text{ even}, \\ 1 & \text{if } n \text{ odd}, \end{cases} \tag{2.22b}$$

$$g_2 : \mathbb{N} \longrightarrow \mathbb{N}, \quad g_2(n) := \begin{cases} n/2 & \text{if } n \text{ even}, \\ 2 & \text{if } n \text{ odd}, \end{cases} \tag{2.22c}$$

both constitute left inverses of f. It follows from Th. 2.12(c) below that f does not have a right inverse.

(b) Consider the map

$$f : \mathbb{N} \longrightarrow \mathbb{N}, \quad f(n) := \begin{cases} n/2 & \text{for } n \text{ even}, \\ (n+1)/2 & \text{for } n \text{ odd}. \end{cases} \tag{2.23a}$$

The maps

$$g_1 : \mathbb{N} \longrightarrow \mathbb{N}, \quad g_1(n) := 2n, \tag{2.23b}$$

$$g_2 : \mathbb{N} \longrightarrow \mathbb{N}, \quad g_2(n) := 2n - 1, \tag{2.23c}$$

both constitute right inverses of f. It follows from Th. 2.12(c) below that f does not have a left inverse.

(c) The map

$$f : \mathbb{N} \longrightarrow \mathbb{N}, \quad f(n) := \begin{cases} n - 1 & \text{for } n \text{ even}, \\ n + 1 & \text{for } n \text{ odd}, \end{cases} \tag{2.24a}$$

is its own inverse, i.e. $f^{-1} = f$. For the map

$$g : \mathbb{N} \longrightarrow \mathbb{N}, \quad g(n) := \begin{cases} 2 & \text{for } n = 1, \\ 3 & \text{for } n = 2, \\ 1 & \text{for } n = 3, \\ n & \text{for } n \notin \{1, 2, 3\}, \end{cases} \tag{2.24b}$$

the inverse is

$$g^{-1} : \mathbb{N} \longrightarrow \mathbb{N}, \quad g^{-1}(n) := \begin{cases} 3 & \text{for } n = 1, \\ 1 & \text{for } n = 2, \\ 2 & \text{for } n = 3, \\ n & \text{for } n \notin \{1, 2, 3\}. \end{cases} \tag{2.24c}$$

While Examples 2.11(a),(b) show that left and right inverses are usually not unique, they *are* unique provided f is bijective (see Th. 2.12(c)).

Theorem 2.12. *Let A, B be nonempty sets.*

(a) *$f : A \longrightarrow B$ is right invertible if, and only if, f is surjective.*

(b) *$f : A \longrightarrow B$ is left invertible if, and only if, f is injective.*

(c) *$f : A \longrightarrow B$ is invertible if, and only if, f is bijective. In this case, the right inverse and the left inverse are unique and both identical to the inverse.*

Proof. (a): If f is surjective, then, for each $y \in B$, there exists $x_y \in f^{-1}\{y\}$ such that $f(x_y) = y$. Define

$$g : B \longrightarrow A, \quad g(y) := x_y \tag{2.25}$$

(note to the interested reader: the definition of g is, in general, not as unproblematic as it might seem – g is a so-called *choice function*, and its definition makes use of the *axiom of choice*, see [Phi16, Sec. A.4]). Then, for each $y \in B$, $f(g(y)) = y$, showing g is a right inverse of f. Conversely, if $g : B \longrightarrow A$ is a right inverse of f, then, for each $y \in B$, it is $y = f(g(y))$, showing that $g(y) \in A$ is a preimage of y, i.e. f is surjective.

(b): Fix $a \in A$. If f is injective, then, for each $y \in B$ with $f^{-1}\{y\} \neq \emptyset$, let x_y denote the unique element in A satisfying $f(x_y) = y$. Define

$$g : B \longrightarrow A, \quad g(y) := \begin{cases} x_y & \text{for } f^{-1}\{y\} \neq \emptyset, \\ a & \text{otherwise.} \end{cases} \tag{2.26}$$

Then, for each $x \in A$, $g(f(x)) = x$, showing g is a left inverse of f. Conversely, if $g : B \longrightarrow A$ is a left inverse of f and $x_1, x_2 \in A$ with $f(x_1) = f(x_2) = y$, then $x_1 = (g \circ f)(x_1) = g(f(x_1)) = g(f(x_2)) = (g \circ f)(x_2) = x_2$, showing y has precisely one preimage and f is injective.

The first part of (c) follows immediately by combining (a) and (b). It merely remains to verify the uniqueness of right and left inverse for bijective maps. So let g be a left inverse of f, let h be a right inverse of f, and let f^{-1} be an inverse of f. Then, for each $y \in B$,

$$g(y) = \big(g \circ (f \circ f^{-1})\big)(y) = \big((g \circ f) \circ f^{-1}\big)(y) = f^{-1}(y), \tag{2.27a}$$
$$h(y) = \big((f^{-1} \circ f) \circ h\big)(y) = \big(f^{-1} \circ (f \circ h)\big)(y) = f^{-1}(y), \tag{2.27b}$$

thereby proving the uniqueness of left and right inverse for bijective maps. ■

Theorem 2.13. *Consider maps $f : A \longrightarrow B$, $g : B \longrightarrow C$. If f and g are both injective (resp. both surjective, both bijective), then so is $g \circ f$. Moreover, in the bijective case, one has*

$$(g \circ f)^{-1} = f^{-1} \circ g^{-1}. \tag{2.28}$$

Proof. Exercise. ■

Definition 2.14. (a) Given an index set I and a set A, a map $f : I \longrightarrow A$ is sometimes called a *family* (of elements in A), and is denoted in the form $f = (a_i)_{i \in I}$ with $a_i := f(i)$. When using this representation, one often does not even specify f and A, especially if the a_i are themselves sets.

(b) A *sequence* in a set A is a family of elements in A, where the index set is the set of natural numbers $\mathbb{N}$. In this case, one writes $(a_n)_{n \in \mathbb{N}}$ or $(a_1, a_2, \dots)$. More generally, a family is called a *sequence*, given a bijective map between the index set I and a subset of $\mathbb{N}$.

(c) Given a family of sets $(A_i)_{i \in I}$, we define the *Cartesian product* of the A_i to be the set of functions

$$\prod_{i \in I} A_i := \left\{ \left(f : I \longrightarrow \bigcup_{j \in I} A_j \right) : \underset{i \in I}{\forall} f(i) \in A_i \right\}. \tag{2.29}$$

If I has precisely n elements with $n \in \mathbb{N}$, then the elements of the Cartesian product $\prod_{i \in I} A_i$ are called (ordered) *n-tuples*, (ordered) *triples* for $n = 3$.

Example 2.15. (a) Using the notion of family, we can now say that the intersection $\bigcap_{i \in I} A_i$ and union $\bigcup_{i \in I} A_i$ as defined in Def. 1.37 are the intersection and union of the family of sets $(A_i)_{i \in I}$, respectively. As a concrete example, let us revisit (1.25b), where we have

$$(A_n)_{n \in \mathbb{N}}, \quad A_n := \{1, 2, \dots, n\}, \quad \bigcap_{n \in \mathbb{N}} A_n = \{1\}. \tag{2.30}$$

(b) Examples of Sequences:

$$\text{Sequence in } \{0,1\}: \qquad (1,0,1,0,1,0,\dots), \tag{2.31a}$$

$$\text{Sequence in } \mathbb{N}: \qquad (n^2)_{n\in\mathbb{N}} = (1,4,9,16,25,\dots), \tag{2.31b}$$

$$\text{Sequence in } \mathbb{R}: \qquad \left((-1)^n\sqrt{n}\right)_{n\in\mathbb{N}} = \left(-1,\sqrt{2},-\sqrt{3},\dots\right), \tag{2.31c}$$

$$\text{Sequence in } \mathbb{R}: \qquad (1/n)_{n\in\mathbb{N}} = \left(1,\frac{1}{2},\frac{1}{3},\dots\right), \tag{2.31d}$$

$$\text{Finite Sequence in } \mathcal{P}(\mathbb{N}): \qquad \big(\{3,2,1\},\{2,1\},\{1\},\emptyset\big). \tag{2.31e}$$

(c) The Cartesian product $\prod_{i\in I} A$, where all sets $A_i = A$, is the same as A^I, the set of all functions from I into A. So, for example, $\prod_{n\in\mathbb{N}} \mathbb{R} = \mathbb{R}^{\mathbb{N}}$ is the set of all sequences in $\mathbb{R}$. If $I = \{1,2,\dots,n\}$ with $n \in \mathbb{N}$, then

$$\prod_{i\in I} A = A^{\{1,2\dots,n\}} =: \prod_{i=1}^{n} A =: A^n \tag{2.32}$$

is the set of all n-tuples with entries from A.

—

In the following, we explain the common notation 2^A for the power set $\mathcal{P}(A)$ of a set A. It is related to a natural identification between subsets and their corresponding characteristic function.

Definition 2.16. Let A be a set and let $B \subseteq A$ be a subset of A. Then

$$\chi_B : A \longrightarrow \{0,1\}, \quad \chi_B(x) := \begin{cases} 1 & \text{if } x \in B, \\ 0 & \text{if } x \notin B, \end{cases} \tag{2.33}$$

is called the *characteristic function* of the set B (with respect to the universe A). One also finds the notations 1_B and $\mathbb{1}_B$ instead of χ_B (note that all the notations supress the dependence of the characteristic function on the universe A).

Proposition 2.17. *Let A be a set. Then the map*

$$\chi : \mathcal{P}(A) \longrightarrow \{0,1\}^A, \quad \chi(B) := \chi_B, \tag{2.34}$$

is bijective (recall that $\mathcal{P}(A)$ denotes the power set of A and $\{0,1\}^A$ denotes the set of all functions from A into $\{0,1\}$).

Proof. χ is injective: Let $B, C \in \mathcal{P}(A)$ with $B \neq C$. By possibly switching the names of B and C, we may assume there exists $x \in B$ such that $x \notin C$. Then $\chi_B(x) = 1$, whereas $\chi_C(x) = 0$, showing $\chi(B) \neq \chi(C)$, proving χ is injective.

χ is surjective: Let $f : A \longrightarrow \{0,1\}$ be an arbitrary function and define $B := \{x \in A : f(x) = 1\}$. Then $\chi(B) = \chi_B = f$, proving χ is surjective. ■

Proposition 2.17 allows one to identify the sets $\mathcal{P}(A)$ and $\{0,1\}^A$ via the bijective map χ. This fact together with the common practise of set theory to identify the number 2 with the set $\{0,1\}$ (cf. Rem. 1.27 above) explains the notation 2^A for $\mathcal{P}(A)$.

2.2 Relations

Definition 2.18. Given sets A and B, a *relation* is a subset R of $A \times B$ (if one wants to be completely precise, a relation is an ordered triple (A, B, R), where $R \subseteq A \times B$). If $A = B$, then we call R a relation on A. One says that $a \in A$ and $b \in B$ are *related* according to the relation R if, and only if, $(a, b) \in R$. In this context, one usually writes $a\,R\,b$ instead of $(a, b) \in R$.

Example 2.19. (a) The relations we are probably most familiar with are $=$ and $\leq$. The relation R of equality, usually denoted $=$, makes sense on every nonempty set A:

$$R := \Delta(A) := \{(x, x) \in A \times A : x \in A\}. \tag{2.35}$$

The set $\Delta(A)$ is called the *diagonal* of the Cartesian product, i.e., as a subset of $A \times A$, the relation of equality is identical to the diagonal:

$$x = y \;\Leftrightarrow\; x\,R\,y \Leftrightarrow\; (x, y) \in R = \Delta(A). \tag{2.36}$$

Similarly, the relation $\leq$ on $\mathbb{R}$ is identical to the set

$$R_{\leq} := \{(x, y) \in \mathbb{R}^2 : x \leq y\}. \tag{2.37}$$

(b) Every function $f : A \longrightarrow B$ is a relation, namely the relation

$$R_f = \{(x, y) \in A \times B : y = f(x)\} = \text{graph}(f). \tag{2.38}$$

Conversely, if $B \neq \emptyset$, then every relation $R \subseteq A \times B$ uniquely corresponds to the function

$$f_R : A \longrightarrow \mathcal{P}(B), \quad f_R(x) = \{y \in B : x\,R\,y\}. \tag{2.39}$$

Definition 2.20. Let R be a relation on the set A.

(a) R is called *reflexive* if, and only if,

$$\underset{x \in A}{\forall}\; x\,R\,x, \tag{2.40}$$

i.e. if, and only if, every element is related to itself.

(b) R is called *symmetric* if, and only if,

$$\underset{x,y \in A}{\forall}\; \big(x\,R\,y \;\Rightarrow\; y\,R\,x\big), \tag{2.41}$$

i.e. if, and only if, each x is related to y if, and only if, y is related to x.

(c) R is called *antisymmetric* if, and only if,

$$\underset{x,y \in A}{\forall}\; \big((x\,R\,y \;\wedge\; y\,R\,x) \;\Rightarrow\; x = y\big), \tag{2.42}$$

i.e. if, and only if, the only possibility for x to be related to y at the same time that y is related to x is in the case $x = y$.

(d) R is called *transitive* if, and only if,

$$\forall_{x,y,z\in A}\big((x\,R\,y\ \wedge\ y\,R\,z)\ \Rightarrow\ x\,R\,z\big), \tag{2.43}$$

i.e. if, and only if, the relatedness of x and y together with the relatedness of y and z implies the relatedness of x and z.

Example 2.21. The relations $=$ and $\leq$ on $\mathbb{R}$ (or $\mathbb{N}$) are reflexive, antisymmetric, and transitive; $=$ is also symmetric, whereas $\leq$ is not; $<$ is antisymmetric (since $x<y\wedge y<x$ is always false) and transitive, but neither reflexive nor symmetric. The relation

$$R := \big\{(x,y)\in\mathbb{N}^2 :\ (x,y \text{ are both even})\vee(x,y \text{ are both odd})\big\} \tag{2.44}$$

on $\mathbb{N}$ is not antisymmetric, but reflexive, symmetric, and transitive. The relation

$$S := \{(x,y)\in\mathbb{N}^2 :\ y=x^2\} \tag{2.45}$$

is not transitive (for example, $2\,S\,4$ and $4\,S\,16$, but not $2\,S\,16$), not reflexive, not symmetric; it is only antisymmetric.

Definition 2.22. A relation R on a set A is called an *equivalence relation* if, and only if, R is reflexive, symmetric, and transitive. If R is an equivalence relations, then one often writes $x\sim y$ instead of $x\,R\,y$.

Example 2.23. (a) The equality relation $=$ is an equivalence relation on each $A\neq\emptyset$.

(b) The relation R defined in (2.44) is an equivalence relation on $\mathbb{N}$.

(c) Given a disjoint union $A=\dot{\bigcup}_{i\in I}A_i$ with every $A_i\neq\emptyset$ (which is sometimes called a *decomposition* of A), an equivalence relation on A is defined by

$$x\sim y\ \Leftrightarrow\ \exists_{i\in I}\big(x\in A_i\wedge y\in A_i\big). \tag{2.46}$$

Conversely, given an equivalence relation $\sim$ on a nonempty set A, we can construct a decomposition $A=\bigcup_{i\in I}A_i$ such that (2.46) holds: For each $x\in A$, define

$$[x] := \{y\in A :\ x\sim y\}, \tag{2.47}$$

called the *equivalence class* of x; each $y\in[x]$ is called a *representative* of $[x]$. One verifies that the properties of $\sim$ guarantee

$$\big([x]=[y]\ \Leftrightarrow\ x\sim y\big)\quad\wedge\quad\big([x]\cap[y]=\emptyset\ \Leftrightarrow\ \neg(x\sim y)\big). \tag{2.48}$$

The set of all equivalence classes $I:=A/\sim:=\{[x] :\ x\in A\}$ is called the *quotient set* of A by $\sim$, and $A=\dot{\bigcup}_{i\in I}A_i$ with $A_i:=i$ for each $i\in I$ is the desired decomposition of A.

Definition 2.24. A relation R on a set A is called a *partial order* if, and only if, R is reflexive, antisymmetric, and transitive. If R is a partial order, then one usually writes $x\leq y$ instead of $x\,R\,y$. A partial order $\leq$ is called a *total* or *linear order* if, and only if, for each $x,y\in A$, one has $x\leq y$ or $y\leq x$.

Notation 2.25. Given a (partial or total) order $\leq$ on $A \neq \emptyset$, we write $x < y$ if, and only if, $x \leq y$ and $x \neq y$, calling $<$ the *strict* order corresponding to $\leq$ (note that the strict order is never a partial order).

Definition 2.26. Let $\leq$ be a partial order on $A \neq \emptyset$, $\emptyset \neq B \subseteq A$.

(a) $x \in A$ is called *lower* (resp. *upper*) *bound* for B if, and only if, $x \leq b$ (resp. $b \leq x$) for each $b \in B$. Moreover, B is called *bounded from below* (resp. from above) if, and only if, there exists a lower (resp. upper) bound for B; B is called *bounded* if, and only if, it is bounded from above and from below.

(b) $x \in B$ is called *minimum* or just *min* (resp. *maximum* or *max*) of B if, and only if, x is a lower (resp. upper) bound for B. One writes $x = \min B$ if x is minimum and $x = \max B$ if x is maximum.

(c) A maximum of the set of lower bounds of B (i.e. a largest lower bound) is called *infimum* of B, denoted $\inf B$; a minimum of the set of upper bounds of B (i.e. a smallest upper bound) is called *supremum* of B, denoted $\sup B$.

Example 2.27. (a) For each $A \subseteq \mathbb{R}$, the usual relation $\leq$ defines a total order on A. For $A = \mathbb{R}$, we see that $\mathbb{N}$ has 0 and 1 as lower bound with $1 = \min \mathbb{N} = \inf \mathbb{N}$. On the other hand, $\mathbb{N}$ is unbounded from above. The set $M := \{1, 2, 3\}$ is bounded with $\min M = 1$, $\max M = 3$. The positive real numbers $\mathbb{R}^+ := \{x \in \mathbb{R} : x > 0\}$ have $\inf \mathbb{R}^+ = 0$, but they do not have a minimum (if $x > 0$, then $0 < x/2 < x$).

(b) Consider $A := \mathbb{N} \times \mathbb{N}$. Then

$$(m_1, m_2) \leq (n_1, n_2) \;\Leftrightarrow\; m_1 \leq n_1 \;\wedge\; m_2 \leq n_2, \tag{2.49}$$

defines a partial order on A that is not a total order (for example, neither $(1, 2) \leq (2, 1)$ nor $(2, 1) \leq (1, 2)$). For the set

$$B := \big\{(1, 1), (2, 1), (1, 2)\big\}, \tag{2.50}$$

we have $\inf B = \min B = (1, 1)$, B does not have a max, but $\sup B = (2, 2)$ (if $(m, n) \in A$ is an upper bound for B, then $(2, 1) \leq (m, n)$ implies $2 \leq m$ and $(1, 2) \leq (m, n)$ implies $2 \leq n$, i.e. $(2, 2) \leq (m, n)$; since $(2, 2)$ is clearly an upper bound for B, we have proved $\sup B = (2, 2)$).

A different order on A is the so-called *lexicographic order* defined by

$$(m_1, m_2) \leq (n_1, n_2) \;\Leftrightarrow\; m_1 < n_1 \;\vee\; (m_1 = n_1 \;\wedge\; m_2 \leq n_2). \tag{2.51}$$

In contrast to the order from (2.49), the lexicographic order does define a total order on A.

Lemma 2.28. *Let $\leq$ be a partial order on $A \neq \emptyset$, $\emptyset \neq B \subseteq A$. Then the relation $\geq$, defined by*

$$x \geq y \;\Leftrightarrow y \leq x, \tag{2.52}$$

is also a partial order on A. Moreover, using obvious notation, we have, for each $x \in A$,

$$x \leq\text{-lower bound for } B \quad \Leftrightarrow \quad x \geq\text{-upper bound for } B, \tag{2.53a}$$
$$x \leq\text{-upper bound for } B \quad \Leftrightarrow \quad x \geq\text{-lower bound for } B, \tag{2.53b}$$
$$x = \min\nolimits_{\leq} B \quad \Leftrightarrow \quad x = \max\nolimits_{\geq} B, \tag{2.53c}$$
$$x = \max\nolimits_{\leq} B \quad \Leftrightarrow \quad x = \min\nolimits_{\geq} B, \tag{2.53d}$$
$$x = \inf\nolimits_{\leq} B \quad \Leftrightarrow \quad x = \sup\nolimits_{\geq} B, \tag{2.53e}$$
$$x = \sup\nolimits_{\leq} B \quad \Leftrightarrow \quad x = \inf\nolimits_{\geq} B. \tag{2.53f}$$

Proof. Reflexivity, antisymmetry, and transitivity of $\leq$ clearly imply the same properties for $\geq$, respectively. Moreover

$$x \leq\text{-lower bound for } B \;\Leftrightarrow\; \underset{b\in B}{\forall}\, x \leq b \;\Leftrightarrow\; \underset{b\in B}{\forall}\, b \geq x \;\Leftrightarrow\; x \geq\text{-upper bound for } B,$$

proving (2.53a). Analogously, we obtain (2.53b). Next, (2.53c) and (2.53d) are implied by (2.53a) and (2.53b), respectively. Finally, (2.53e) is proved by

$$\begin{aligned} x = \inf\nolimits_{\leq} B \;&\Leftrightarrow\; x = \max\nolimits_{\leq}\{y \in A :\, y \leq\text{-lower bound for } B\} \\ &\Leftrightarrow\; x = \min\nolimits_{\geq}\{y \in A :\, y \geq\text{-upper bound for } B\} \;\Leftrightarrow\; x = \sup\nolimits_{\geq} B, \end{aligned}$$

and (2.53f) follows analogously. ■

Proposition 2.29. *Let $\leq$ be a partial order on $A \neq \emptyset$, $\emptyset \neq B \subseteq A$. The elements $\max B$, $\min B$, $\sup B$, $\inf B$ are all unique, provided they exist.*

Proof. Exercise. ■

Definition 2.30. Let A, B be nonempty sets with partial orders, both denoted by $\leq$ (even though they might be different). A function $f : A \longrightarrow B$, is called (*strictly*) *isotone*, *order-preserving*, or *increasing* if, and only if,

$$\underset{x,y\in A}{\forall} \big(x < y \;\Rightarrow\; f(x) \leq f(y) \;\; (\text{resp. } f(x) < f(y))\big); \tag{2.54a}$$

f is called (*strictly*) *antitone*, *order-reversing*, or *decreasing* if, and only if,

$$\underset{x,y\in A}{\forall} \big(x < y \;\Rightarrow\; f(x) \geq f(y) \;\; (\text{resp. } f(x) > f(y))\big). \tag{2.54b}$$

Functions that are (strictly) isotone or antitone are called (strictly) *monotone*.

Proposition 2.31. *Let A, B be nonempty sets with partial orders, both denoted by $\leq$.*

(a) *A (strictly) isotone function $f : A \longrightarrow B$ becomes a (strictly) antitone function and vice versa if precisely one of the relations $\leq$ is replaced by $\geq$.*

(b) *If the order $\leq$ on A is total and $f : A \longrightarrow B$ is strictly isotone or strictly antitone, then f is one-to-one.*

(c) *If the order $\leq$ on A is total and $f : A \longrightarrow B$ is invertible and strictly isotone (resp. antitone), then f^{-1} is also strictly isotone (resp. antitone).*

Proof. (a) is immediate from (2.54).

(b): Due to (a), it suffices to consider the case that f is strictly isotone. If f is strictly isotone and $x \neq y$, then $x < y$ or $y < x$ since the order on A is total. Thus, $f(x) < f(y)$ or $f(y) < f(x)$, i.e. $f(x) \neq f(y)$ in every case, showing f is one-to-one.

(c): Again, due to (a), it suffices to consider the isotone case. If $u, v \in B$ such that $u < v$, then $u = f(f^{-1}(u))$, $v = f(f^{-1}(v))$, and the isotonicity of f imply $f^{-1}(u) < f^{-1}(v)$ (we are using that the order on A is total – otherwise, $f^{-1}(u)$ and $f^{-1}(v)$ need not be comparable). ■

Example 2.32. (a) $f : \mathbb{N} \longrightarrow \mathbb{N}$, $f(n) := 2n$, is strictly increasing, every constant map on $\mathbb{N}$ is both increasing and decreasing, but not strictly increasing or decreasing. All maps occurring in (2.24) are neither increasing nor decreasing.

(b) The map $f : \mathbb{R} \longrightarrow \mathbb{R}$, $f(x) := -2x$, is invertible and strictly decreasing, and so is $f^{-1} : \mathbb{R} \longrightarrow \mathbb{R}$, $f^{-1}(x) := -x/2$.

(c) The following counterexamples show that the assertions of Prop. 2.31(b),(c) are no longer correct if one does not assume the order on A is total. Let A be the set from (2.50) (where it had been called B) with the (nontotal) order from (2.49). The map

$$f : A \longrightarrow \mathbb{N}, \quad \begin{cases} f(1,1) := 1, \\ f(1,2) := 2, \\ f(2,1) := 2, \end{cases} \tag{2.55}$$

is strictly isotone, but not one-to-one. The map

$$f : A \longrightarrow \{1,2,3\}, \quad \begin{cases} f(1,1) := 1, \\ f(1,2) := 2, \\ f(2,1) := 3, \end{cases} \tag{2.56}$$

is strictly isotone and invertible, however f^{-1} is not isotone (since $2 < 3$, but $f^{-1}(2) = (1,2)$ and $f^{-1}(3) = (2,1)$ are not comparable, i.e. $f^{-1}(2) \leq f^{-1}(3)$ is *not* true).

3 Natural Numbers, Induction, and the Size of Sets

3.1 Induction and Recursion

One of the most useful proof techniques is the method of induction – it is used in situations, where one needs to verify the truth of statements $\phi(n)$ for each $n \in \mathbb{N}$, i.e. the truth of the statement

$$\bigwedge_{n \in \mathbb{N}} \phi(n). \tag{3.1}$$

Induction is based on the fact that $\mathbb{N}$ satisfies the so-called *Peano axioms*:

P1: $\mathbb{N}$ contains a special element called *one*, denoted 1.

P2: There exists an injective map $S : \mathbb{N} \longrightarrow \mathbb{N} \setminus \{1\}$, called the *successor function* (for each $n \in \mathbb{N}$, $S(n)$ is called the *successor* of n).

P3: If a subset A of $\mathbb{N}$ has the property that $1 \in A$ and $S(n) \in A$ for each $n \in A$, then A is equal to $\mathbb{N}$. Written as a formula, the third axiom is:

$$\underset{A \in \mathcal{P}(\mathbb{N})}{\forall} \big(1 \in A \ \wedge \ S(A) \subseteq A \ \Rightarrow \ A = \mathbb{N}\big).$$

Remark 3.1. In Def. 1.26, we had introduced the natural numbers $\mathbb{N} := \{1, 2, 3, \dots\}$. The successor function is $S(n) = n + 1$. In axiomatic set theory, one starts with the Peano axioms and shows that the axioms of set theory allow the construction of a set $\mathbb{N}$ which satisfies the Peano axioms. One then *defines* $2 := S(1)$, $3 := S(2)$, $\dots$, $n + 1 := S(n)$. The interested reader can find more details in [Phi16, Sec. D.1].

Theorem 3.2 (Principle of Induction)**.** *Suppose, for each $n \in \mathbb{N}$, $\phi(n)$ is a statement (i.e. a predicate of n in the language of Def.* 1.30*). If* (a) *and* (b) *both hold, where*

(a) $\phi(1)$ *is true,*

(b) $\underset{n \in \mathbb{N}}{\forall} \big(\phi(n) \ \Rightarrow \ \phi(n+1)\big)$,

then (3.1) *is true, i.e. $\phi(n)$ is true for every $n \in \mathbb{N}$.*

Proof. Let $A := \{n \in \mathbb{N} : \ \phi(n)\}$. We have to show $A = \mathbb{N}$. Since $1 \in A$ by (a), and

$$n \in A \ \Rightarrow \ \phi(n) \overset{\text{(b)}}{\Rightarrow} \ \phi(n+1) \Rightarrow \ S(n) = n + 1 \in A, \tag{3.2}$$

i.e. $S(A) \subseteq A$, the Peano axiom P3 implies $A = \mathbb{N}$. ∎

Remark 3.3. To prove some $\phi(n)$ for each $n \in \mathbb{N}$ by induction according to Th. 3.2 consists of the following two steps:

(a) Prove $\phi(1)$, the so-called *base case*.

(b) Perform the *inductive step*, i.e. prove that $\phi(n)$ (the *induction hypothesis*) implies $\phi(n + 1)$.

Example 3.4. We use induction to prove the statement

$$\underset{n \in \mathbb{N}}{\forall} \underbrace{\left(1 + 2 + \cdots + n = \frac{n(n+1)}{2}\right)}_{\phi(n)} : \tag{3.3}$$

Base Case ($n = 1$): $1 = \frac{1\cdot 2}{2}$, i.e. $\phi(1)$ is true.

Induction Hypothesis: Assume $\phi(n)$, i.e. $1 + 2 + \cdots + n = \frac{n(n+1)}{2}$ holds.

Induction Step: One computes

$$\begin{aligned} 1 + 2 + \cdots + n + (n+1) &\overset{(\phi(n))}{=} \frac{n(n+1)}{2} + n + 1 = \frac{n(n+1) + 2n + 2}{2} \\ &= \frac{n^2 + 3n + 2}{2} = \frac{(n+1)(n+2)}{2}, \end{aligned} \tag{3.4}$$

i.e. $\phi(n+1)$ holds and the induction is complete.

Corollary 3.5. *Theorem* 3.2 *remains true if* (b) *is replaced by*

$$\underset{n\in\mathbb{N}}{\forall} \left(\left(\underset{1\le m\le n}{\forall} \phi(m) \right) \Rightarrow \phi(n+1) \right). \tag{3.5}$$

Proof. If, for each $n \in \mathbb{N}$, we use $\psi(n)$ to denote $\underset{1\le m\le n}{\forall} \phi(m)$, then (3.5) is equivalent to $\underset{n\in\mathbb{N}}{\forall} \big(\psi(n) \Rightarrow \psi(n+1)\big)$, i.e. to Th. 3.2(b) with ϕ replaced by ψ. Thus, Th. 3.2 implies $\psi(n)$ holds true for each $n \in \mathbb{N}$, i.e. $\phi(n)$ holds true for each $n \in \mathbb{N}$. ■

Corollary 3.6. *Let I be an index set. Suppose, for each $i \in I$, $\phi(i)$ is a statement. If there is a bijective map $f : \mathbb{N} \longrightarrow I$ and* (a) *and* (b) *both hold, where*

(a) $\phi\big(f(1)\big)$ *is true,*

(b) $\underset{n\in\mathbb{N}}{\forall} \Big(\phi\big(f(n)\big) \Rightarrow \phi\big(f(n+1)\big)\Big)$,

then $\phi(i)$ is true for every $i \in I$.

Finite Induction: The above assertion remains true if $f : \{1, \ldots, m\} \longrightarrow I$ is bijective for some $m \in \mathbb{N}$ and $\mathbb{N}$ in (b) *is replaced by $\{1, \ldots, m-1\}$.*

Proof. If, for each $n \in \mathbb{N}$, we use $\psi(n)$ to denote $\phi\big(f(n)\big)$, then Th. 3.2 shows $\psi(n)$ is true for every $n \in \mathbb{N}$. Given $i \in I$, we have $n := f^{-1}(i) \in \mathbb{N}$ with $f(n) = i$, showing that $\phi(i) = \phi\big(f(n)\big) = \psi(n)$ is true.

For the finite induction, let $\psi(n)$ denote $\big(n \le m \wedge \phi\big(f(n)\big)\big) \vee n > m$. Then, for $1 \le n < m$, we have $\psi(n) \Rightarrow \psi(n+1)$ due to (b). For $n \ge m$, we also have $\psi(n) \Rightarrow \psi(n+1)$ due to $n \ge m \Rightarrow n + 1 > m$. Thus, Th. 3.2 shows $\psi(n)$ is true for every $n \in \mathbb{N}$. Given $i \in I$, it is $n := f^{-1}(i) \in \{1, \ldots, m\}$ with $f(n) = i$. Since $n \le m \wedge \psi(n) \Rightarrow \phi\big(f(n)\big)$, we obtain that $\phi(i)$ is true. ■

Apart from providing a widely employable proof technique, the most important application of Th. 3.2 is the possibility to define sequences inductively, using so-called recursion:

Theorem 3.7 (Recursion Theorem)**.** *Let A be a nonempty set and $x \in A$. Given a sequence of functions $(f_n)_{n\in\mathbb{N}}$, where $f_n : A^n \longrightarrow A$, there exists a unique sequence $(x_n)_{n\in\mathbb{N}}$ in A satisfying the following two conditions:*

(i) $x_1 = x$.

(ii) $\underset{n\in\mathbb{N}}{\forall} x_{n+1} = f_n(x_1, \ldots, x_n)$.

The same holds if $\mathbb{N}$ is replaced by an index set I as in Cor. 3.6.

Proof. To prove uniqueness, let $(x_n)_{n\in\mathbb{N}}$ and $(y_n)_{n\in\mathbb{N}}$ be sequences in A, both satisfying (i) and (ii), i.e.

$$x_1 = y_1 = x \quad \text{and} \tag{3.6a}$$

$$\underset{n\in\mathbb{N}}{\forall} \big(x_{n+1} = f_n(x_1, \ldots, x_n) \wedge y_{n+1} = f_n(y_1, \ldots, y_n)\big). \tag{3.6b}$$

We prove by induction (in the form of Cor. 3.5) that $(x_n)_{n\in\mathbb{N}} = (y_n)_{n\in\mathbb{N}}$, i.e.

$$\underset{n\in\mathbb{N}}{\forall} \underbrace{x_n = y_n}_{\phi(n)} : \tag{3.7}$$

Base Case ($n = 1$): $\phi(1)$ is true according to (3.6a).

Induction Hypothesis: Assume $\phi(m)$ for each $m \in \{1, \ldots, n\}$, i.e. $x_m = y_m$ holds for each $m \in \{1, \ldots, n\}$.

Induction Step: One computes

$$x_{n+1} \overset{(3.6b)}{=} f_n(x_1, \ldots, x_n) \overset{\big(\phi(1),\ldots,\phi(n)\big)}{=} f_n(y_1, \ldots, y_n) \overset{(3.6b)}{=} y_{n+1}, \tag{3.8}$$

i.e. $\phi(n+1)$ holds and the induction is complete.

To prove existence, we have to show that there is a function $F : \mathbb{N} \longrightarrow A$ such that the following two conditions hold:

$$F(1) = x, \tag{3.9a}$$

$$\underset{n\in\mathbb{N}}{\forall} F(n+1) = f_n\big(F(1), \ldots, F(n)\big). \tag{3.9b}$$

To this end, let

$$\mathcal{F} := \left\{ B \subseteq \mathbb{N} \times A : (1, x) \in B \wedge \underset{\substack{n\in\mathbb{N},\\ (1,a_1),\ldots,(n,a_n)\in B}}{\forall} \big(n+1, f_n(a_1, \ldots, a_n)\big) \in B \right\} \tag{3.10}$$

and

$$G := \bigcap_{B\in\mathcal{F}} B. \tag{3.11}$$

Note that G is well-defined, as $\mathbb{N} \times A \in \mathcal{F}$. Also, clearly, $G \in \mathcal{F}$. We would like to define F such that $G = \text{graph}(F)$. For this to be possible, we will show, by induction,

$$\underset{n\in\mathbb{N}}{\forall} \underbrace{\underset{x_n\in A}{\exists!}\, (n, x_n) \in G}_{\phi(n)}. \tag{3.12}$$

Base Case ($n = 1$): From the definition of G, we know $(1, x) \in G$. If $(1, a) \in G$ with $a \neq x$, then $H := G \setminus \{(1, a)\} \in \mathcal{F}$, implying $G \subseteq H$ in contradiction to $(1, a) \notin H$. This shows $a = x$ and proves $\phi(1)$.

Induction Hypothesis: Assume $\phi(m)$ for each $m \in \{1, \ldots, n\}$.

Induction Step: From the induction hypothesis, we know

$$\underset{(x_1,\ldots,x_n)\in A^n}{\exists!}\, (1, x_1), \ldots, (n, x_n) \in G.$$

Thus, if we let $x_{n+1} := f_n(x_1, \ldots, x_n)$, then $(n + 1, x_{n+1}) \in G$ by the definition of G. If $(n + 1, a) \in G$ with $a \neq x_{n+1}$, then $H := G \setminus \{(n + 1, a)\} \in \mathcal{F}$ (using the uniqueness of the $(1, x_1), \ldots, (n, x_n) \in G$), implying $G \subseteq H$ in contradiction to $(n + 1, a) \notin H$. This shows $a = x_{n+1}$, proves $\phi(n + 1)$, and completes the induction.

Due to (3.12), we can now define $F : \mathbb{N} \longrightarrow A$, $F(n) := x_n$, and the definition of G then guarantees the validity of (3.9). ■

Example 3.8. In many applications of Th. 3.7, one has functions $g_n : A \longrightarrow A$ and uses

$$\underset{n\in\mathbb{N}}{\forall} \big(f_n : A^n \longrightarrow A, \quad f_n(a_1, \ldots, a_n) := g_n(a_n)\big). \tag{3.13}$$

Here are some important concrete examples:

(a) The *factorial function* $F : \mathbb{N}_0 \longrightarrow \mathbb{N}$, $n \mapsto n!$, is defined recursively by

$$0! := 1, \quad 1! := 1, \quad \underset{n\in\mathbb{N}}{\forall} (n + 1)! := (n + 1) \cdot n!, \tag{3.14a}$$

i.e. we have $A = \mathbb{N}$ and $g_n(x) := (n + 1) \cdot x$. So we obtain

$$(n!)_{n\in\mathbb{N}_0} = (1, 1, 2, 6, 24, 120, \ldots). \tag{3.14b}$$

(b) For each $a \in \mathbb{R}$ and each $d \in \mathbb{R}$, we define the following *arithmetic progression* (also called *arithmetic sequence*) recursively by

$$a_1 := a, \quad \underset{n\in\mathbb{N}}{\forall} a_{n+1} := a_n + d, \tag{3.15a}$$

i.e. we have $A = \mathbb{R}$ and $g_n = g$ with $g(x) := x + d$. For example, for $a = 2$ and $d = -0.5$, we obtain

$$(a_n)_{n\in\mathbb{N}} = (2,\ 1.5,\ 1,\ 0.5,\ 0,\ -0.5,\ -1,\ -1.5,\ \ldots). \tag{3.15b}$$

(c) For each $a \in \mathbb{R}$ and each $q \in \mathbb{R} \setminus \{0\}$, we define the following *geometric progression* (also called *geometric sequence*) recursively by

$$x_1 := a, \quad \underset{n\in\mathbb{N}}{\forall} x_{n+1} := x_n \cdot q, \tag{3.16a}$$

i.e. we have $A = \mathbb{R}$ and $g_n = g$ with $g(x) := x \cdot q$. For example, for $a = 3$ and $q = -2$, we obtain

$$(x_n)_{n\in\mathbb{N}} = (3,\, -6,\, 12,\, -24,\, 48,\, \dots). \tag{3.16b}$$

For the time being, we will continue to always specify A and the g_n or f_n in subsequent recursive definitions, but in the literature, most of the time, the g_n or f_n are not provided explicitly.

Example 3.9. (a) The *Fibonacci sequence* consists of the *Fibonacci numbers*, defined recursively by

$$F_0 := 0, \quad F_1 := 1, \quad \underset{n\in\mathbb{N}}{\forall} F_{n+1} := F_n + F_{n-1}, \tag{3.17a}$$

i.e. we have $A = \mathbb{N}_0$ and

$$f_n :\, A^n \longrightarrow A, \quad f_n(a_1, \dots, a_n) := \begin{cases} 1 & \text{for } n = 1, \\ a_n + a_{n-1} & \text{for } n \geq 2. \end{cases} \tag{3.17b}$$

So we obtain

$$(F_n)_{n\in\mathbb{N}_0} = (0,\, 1,\, 1,\, 2,\, 3,\, 5,\, 8,\, 13,\, 21,\, 34,\, 55,\, 89,\, \dots). \tag{3.17c}$$

(b) For $A := \mathbb{N}$, $x := 1$, and

$$f_n :\, A^n \longrightarrow A, \quad f_n(a_1, \dots, a_n) := a_1 + \cdots + a_n, \tag{3.18a}$$

one obtains

$$\begin{gathered} x_1 = 1, \quad x_2 = f_1(1) = 1, \quad x_3 = f_2(1,1) = 2, \quad x_4 = f_3(1,1,2) = 4, \\ x_5 = f_4(1,1,2,4) = 8, \quad x_6 = f_5(1,1,2,4,8) = 16, \quad \dots \end{gathered} \tag{3.18b}$$

Definition 3.10. (a) *Summation Symbol:* On $A = \mathbb{R}$ (or, more generally, on every set where an addition $+ :\, A \times A \longrightarrow A$ is defined), define recursively, for each given (possibly finite) sequence $(a_1, a_2, \dots)$ in A:

$$\sum_{i=1}^{1} a_i := a_1, \quad \sum_{i=1}^{n+1} a_i := a_{n+1} + \sum_{i=1}^{n} a_i \text{ for } n \geq 1, \tag{3.19a}$$

i.e.

$$f_n :\, A^n \longrightarrow A, \quad f_n(x_1, \dots, x_n) := x_n + a_{n+1}. \tag{3.19b}$$

In (3.19a), one can also use other symbols for i, except a and n; for a finite sequence, n needs to be less than the maximal index of the finite sequence.

More generally, if I is an index set and $\phi : \{1, \dots, n\} \longrightarrow I$ a bijective map, then define

$$\sum_{i \in I} a_i := \sum_{i=1}^{n} a_{\phi(i)}. \tag{3.19c}$$

The commutativity of addition implies that the definition in (3.19c) is actually independent of the chosen bijective map ϕ. Also define

$$\sum_{i \in \emptyset} a_i := 0 \tag{3.19d}$$

(for a general A, 0 is meant to be an element such that $a + 0 = 0 + a = a$ for each $a \in A$ and we can even define this if $0 \notin A$).

(b) *Product Symbol:* On $A = \mathbb{R}$ (or, more generally, on every set where a multiplication $\cdot : A \times A \longrightarrow A$ is defined), define recursively, for each given (possibly finite) sequence $(a_1, a_2, \dots)$ in A:

$$\prod_{i=1}^{1} a_i := a_1, \quad \prod_{i=1}^{n+1} a_i := a_{n+1} \cdot \prod_{i=1}^{n} a_i \text{ for } n \geq 1, \tag{3.20a}$$

i.e.

$$f_n : A^n \longrightarrow A, \quad f_n(x_1, \dots, x_n) := x_n \cdot a_{n+1}. \tag{3.20b}$$

In (3.20a), one can also use other symbols for i, except a and n; for a finite sequence, n needs to be less than the maximal index of the finite sequence.

More generally, if I is an index set and $\phi : \{1, \dots, n\} \longrightarrow I$ a bijective map, then define

$$\prod_{i \in I} a_i := \prod_{i=1}^{n} a_{\phi(i)}. \tag{3.20c}$$

The commutativity of multiplication implies that the definition in (3.20c) is actually independent of the chosen bijective map ϕ. Also define

$$\prod_{i \in \emptyset} a_i := 1 \tag{3.20d}$$

(for a general A, 1 is meant to be an element such that $a \cdot 1 = 1 \cdot a = a$ for each $a \in A$ and we can even define this if $1 \notin A$).

Example 3.11. (a) Given $a, d \in \mathbb{R}$, let $(a_n)_{n \in \mathbb{N}}$ be the arithmetic sequence as defined in (3.15a). It is an exercise to prove by induction that

$$\underset{n \in \mathbb{N}}{\forall} \quad a_n = a + (n-1)d, \tag{3.21a}$$

$$\underset{n \in \mathbb{N}}{\forall} \quad S_n := \sum_{i=1}^{n} a_i = \frac{n}{2}\,(a_1 + a_n) = \frac{n}{2}\,\big(2\,a + (n-1)\,d\big), \tag{3.21b}$$

where the S_n are called *arithmetic sums*.

(b) Given $a \in \mathbb{R}$ and $q \in \mathbb{R} \setminus \{0\}$, let $(x_n)_{n\in\mathbb{N}}$ be the geometric sequence as defined in (3.16a). We will prove by induction that

$$\forall_{n\in\mathbb{N}} \quad x_n = a\,q^{n-1}, \tag{3.22a}$$

$$\forall_{n\in\mathbb{N}} \quad S_n := \sum_{i=1}^{n} x_i = \sum_{i=1}^{n} (a\,q^{i-1}) = a \sum_{i=0}^{n-1} q^i = \begin{cases} n\,a & \text{for } q = 1, \\ \frac{a\,(1-q^n)}{1-q} & \text{for } q \neq 1, \end{cases} \tag{3.22b}$$

where the S_n are called *geometric sums*.

For the induction proof of (3.22a), $\phi(n)$ is $x_n = a\,q^{n-1}$. The base case, $\phi(1)$, is the statement $x_1 = a\,q^0 = a$, which is true. For the induction step, we assume $\phi(n)$ and compute

$$x_{n+1} = x_n \cdot q \overset{(\phi(n))}{=} a\,q^{n-1} \cdot q = a\,q^n, \tag{3.23}$$

showing $\phi(n) \Rightarrow \phi(n+1)$ and completing the proof.

For $q = 1$, the sum S_n is actually arithmetic with $d = 0$, i.e. $S_n = na$ can be obtained from (3.21b). For the induction proof of (3.22b) with $q \neq 1$, $\phi(n)$ is $S_n = \frac{a(1-q^n)}{1-q}$. The base case, $\phi(1)$, is the statement $S_1 = \frac{a(1-q)}{1-q} = a$, which is true. For the induction step, we assume $\phi(n)$ and compute

$$S_{n+1} = S_n + x_{n+1} \overset{(\phi(n))}{=} \frac{a(1-q^n)}{1-q} + aq^n = \frac{a(1-q^n) + aq^n(1-q)}{1-q} = \frac{a(1-q^{n+1})}{1-q}, \tag{3.24}$$

showing $\phi(n) \Rightarrow \phi(n+1)$ and completing the proof.

3.2 Cardinality: The Size of Sets

Cardinality measures the size of sets. For a finite set A, it is precisely the number of elements in A. For an infinite set, it classifies the set's degree or level of infinity (it turns out that not all infinite sets have the same size).

Definition 3.12. (a) The sets A, B are defined to have the same *cardinality* or the same *size* if, and only if, there exists a bijective map $\varphi : A \longrightarrow B$. One can show that this defines an equivalence relation on every set of sets (see [Phi16, Th. A.53]).

(b) The *cardinality* of a set A is $n \in \mathbb{N}$ (denoted $\#A = n$) if, and only if, there exists a bijective map $\varphi : A \longrightarrow \{1, \ldots, n\}$. The cardinality of $\emptyset$ is defined as 0, i.e. $\#\emptyset := 0$. A set A is called *finite* if, and only if, there exists $n \in \mathbb{N}_0$ such that $\#A = n$; A is called *infinite* if, and only if, A is not finite, denoted $\#A = \infty$ (in the strict sense, this is an abuse of notation, since ∞ is *not* a cardinality – for example $\#\mathbb{N} = \infty$ and $\#\mathcal{P}(\mathbb{N}) = \infty$, but $\mathbb{N}$ and $\mathcal{P}(\mathbb{N})$ do *not* have the same cardinality, since the power set $\mathcal{P}(A)$ is always strictly bigger than A (see Th. 3.20 below) – $\#A = \infty$ is merely an abbreviation for the statement "A is infinite"). The interested student finds additional material regarding the uniqueness of finite cardinality in [Phi16, Th. A.61] and [Phi16, Cor. A.62], and regarding characterizations of infinite sets in [Phi16, Th. A.54].

(c) The set A is called *countable* if, and only if, A is finite or A has the same cardinality as $\mathbb{N}$. Otherwise, A is called *uncountable*.

Theorem 3.13. *Let $A \neq \emptyset$ be a finite set.*

(a) *If $B \subseteq A$ with $A \neq B$, then B is finite with $\#B < \#A$.*

(b) *If $a \in A$, then $\#\big(A \setminus \{a\}\big) = \#A - 1$.*

Proof. For $\#A = n \in \mathbb{N}$, we use induction to prove (a) and (b) simultaneously, i.e. we show

$$\underset{n\in\mathbb{N}}{\forall} \underbrace{\left(\#A = n \;\Rightarrow\; \underset{B\in\mathcal{P}(A)\setminus\{A\}}{\forall}\; \underset{a\in A}{\forall} \#B \in \{0,\ldots,n-1\} \wedge \#\big(A\setminus\{a\}\big) = n-1\right)}_{\phi(n)}.$$

Base Case ($n = 1$): In this case, A has precisely one element, i.e. $B = A \setminus \{a\} = \emptyset$, and $\#\emptyset = 0 = n - 1$ proves $\phi(1)$.

Induction Step: For the induction hypothesis, we assume $\phi(n)$ to be true, i.e. we assume (a) and (b) hold for each A with $\#A = n$. We have to prove $\phi(n+1)$, i.e., we consider A with $\#A = n+1$. From $\#A = n+1$, we conclude the existence of a bijective map $\varphi : A \longrightarrow \{1,\ldots,n+1\}$. We have to construct a bijective map $\psi : A \setminus \{a\} \longrightarrow \{1,\ldots,n\}$. To this end, set $k := \varphi(a)$ and define the auxiliary function

$$f : \{1,\ldots,n+1\} \longrightarrow \{1,\ldots,n+1\}, \quad f(x) := \begin{cases} n+1 & \text{for } x = k, \\ k & \text{for } x = n+1, \\ x & \text{for } x \notin \{k, n+1\}. \end{cases}$$

Then $f \circ \varphi : A \longrightarrow \{1,\ldots,n+1\}$ is bijective by Th. 2.13, and

$$(f \circ \varphi)(a) = f(\varphi(a)) = f(k) = n+1.$$

Thus, the restriction $\psi := f\restriction_{A\setminus\{a\}}$ is the desired bijective map $\psi : A\setminus\{a\} \longrightarrow \{1,\ldots,n\}$, proving $\#\big(A \setminus \{a\}\big) = n$. It remains to consider the strict subset B of A. Since B is a strict subset of A, there exists $a \in A \setminus B$. Thus, $B \subseteq A \setminus \{a\}$ and, as we have already shown $\#\big(A \setminus \{a\}\big) = n$, the induction hypothesis applies and yields B is finite with $\#B \leq \#\big(A \setminus \{a\}\big) = n$, i.e. $\#B \in \{0,\ldots,n\}$, proving $\phi(n+1)$, thereby completing the induction. ∎

Theorem 3.14. *For $\#A = \#B = n \in \mathbb{N}$ and $f : A \longrightarrow B$, the following statements are equivalent:*

(i) *f is injective.*

(ii) *f is surjective.*

(iii) *f is bijective.*

Proof. It suffices to prove the equivalence of (i) and (ii).

If f is injective, then $f : A \longrightarrow f(A)$ is bijective. Since $\#A = n$, there exists a bijective map $\varphi : A \longrightarrow \{1, \ldots, n\}$. Then $(\varphi \circ f^{-1}) : f(A) \longrightarrow \{1, \ldots, n\}$ is also bijective, showing $\#f(A) = n$, i.e., according to Th. 3.13(a), $f(A)$ can not be a strict subset of B, i.e. $f(A) = B$, proving f is surjective.

If f is surjective, then f has a right inverse $g : B \longrightarrow A$ by Th. 2.12(a), i.e. $f \circ g = \mathrm{Id}_B$. But this also means f is a left inverse for g, such that g must be injective by Th. 2.12(b). According to what we have already proved above, g injective implies g surjective, i.e. g must be bijective. From Th. 2.12(c), we then know the left inverse of g is unique, implying $f = g^{-1}$. In particular, f is injective. ■

Lemma 3.15. *For each finite set A (i.e. $\#A = n \in \mathbb{N}_0$) and each $B \subseteq A$, one has $\#(A \setminus B) = \#A - \#B$.*

Proof. For $B = \emptyset$, the assertion is true since $\#(A \setminus B) = \#A = \#A - 0 = \#A - \#B$.

For $B \neq \emptyset$, the proof is conducted over the size of B, i.e. as a finite induction (cf. Cor. 3.6) over the set $\{1, \ldots, n\}$, showing

$$\forall_{m \in \{1,\ldots,n\}} \underbrace{\big(\#B = m \;\Rightarrow\; \#(A \setminus B) = \#A - \#B\big)}_{\phi(m)}.$$

Base Case ($m = 1$): $\phi(1)$ is precisely the statement provided by Th. 3.13(b).

Induction Step: For the induction hypothesis, we assume $\phi(m)$ with $1 \leq m < n$. To prove $\phi(m+1)$, consider $B \subseteq A$ with $\#B = m + 1$. Fix an element $b \in B$ and set $B_1 := B \setminus \{b\}$. Then $\#B_1 = m$ by Th. 3.13(b), $A \setminus B = (A \setminus B_1) \setminus \{b\}$, and we compute

$$\begin{aligned} \#(A \setminus B) &= \#\big((A \setminus B_1) \setminus \{b\}\big) \overset{\text{Th. 3.13(b)}}{=} \#(A \setminus B_1) - 1 \overset{(\phi(m))}{=} \#A - \#B_1 - 1 \\ &= \#A - \#B, \end{aligned}$$

proving $\phi(m+1)$ and completing the induction. ■

Theorem 3.16. *If A, B are finite sets, then $\#(A \cup B) = \#A + \#B - \#(A \cap B)$.*

Proof. The assertion is clearly true if A or B is empty. If A and B are nonempty, then there exist $m, n \in \mathbb{N}$ such that $\#A = m$ and $\#B = n$, i.e. there are bijective maps $f : A \longrightarrow \{1, \ldots, m\}$ and $g : B \longrightarrow \{1, \ldots, n\}$.

We first consider the case $A \cap B = \emptyset$. We need to construct a bijective map $h : A \cup B \longrightarrow \{1, \ldots, m+n\}$. To this end, we define

$$h : A \cup B \longrightarrow \{1, \ldots, m+n\}, \quad h(x) := \begin{cases} f(x) & \text{for } x \in A, \\ g(x) + m & \text{for } x \in B. \end{cases}$$

The bijectivity of f and g clearly implies the bijectivity of h, proving $\#(A \cup B) = m + n = \#A + \#B$.

Finally, we consider the case of arbitrary A, B. Since $A \cup B = A \dot\cup (B \setminus A)$ and $B \setminus A = B \setminus (A \cap B)$, we can compute

$$\begin{aligned}\#(A \cup B) &= \#\big(A \dot\cup (B \setminus A)\big) = \#A + \#(B \setminus A) \\ &= \#A + \#\big(B \setminus (A \cap B)\big) \overset{\text{Lem. 3.15}}{=} \#A + \#B - \#(A \cap B),\end{aligned}$$

thereby establishing the case. ■

Theorem 3.17. *If $(A_1, \ldots, A_n)$, $n \in \mathbb{N}$, is a finite sequence of finite sets, then*

$$\#\prod_{i=1}^{n} A_i = \#\big(A_1 \times \cdots \times A_n\big) = \prod_{i=1}^{n} \#A_i. \tag{3.25}$$

Proof. If at least one A_i is empty, then (3.25) is true, since both sides are 0.

The case where all A_i are nonempty is proved by induction over n, i.e. we know $k_i := \#A_i \in \mathbb{N}$ for each $i \in \{1, \ldots, n\}$ and show by induction

$$\underset{n \in \mathbb{N}}{\forall} \underbrace{\#\prod_{i=1}^{n} A_i = \prod_{i=1}^{n} k_i}_{\phi(n)}.$$

Base Case ($n = 1$): $\prod_{i=1}^{1} A_i = \#A_1 = k_1 = \prod_{i=1}^{1} k_i$, i.e. $\phi(1)$ holds.

Induction Step: From the induction hypothesis $\phi(n)$, we obtain a bijective map $\varphi : A \longrightarrow \{1, \ldots, N\}$, where $A := \prod_{i=1}^{n} A_i$ and $N := \prod_{i=1}^{n} k_i$. To prove $\phi(n+1)$, we need to construct a bijective map $h : A \times A_{n+1} \longrightarrow \{1, \ldots, N \cdot k_{n+1}\}$. Since $\#A_{n+1} = k_{n+1}$, there exists a bijective map $f : A_{n+1} \longrightarrow \{1, \ldots, k_{n+1}\}$. We define

$$\begin{aligned} h : A \times A_{n+1} &\longrightarrow \{1, \ldots, N \cdot k_{n+1}\}, \\ h(a_1, \ldots, a_n, a_{n+1}) &:= \big(f(a_{n+1}) - 1\big) \cdot N + \varphi(a_1, \ldots, a_n). \end{aligned}$$

Since φ and f are bijective, and since every $m \in \{1, \ldots, N \cdot k_{n+1}\}$ has a unique representation in the form $m = a \cdot N + r$ with $a \in \{0, \ldots, k_{n+1} - 1\}$ and $r \in \{1, \ldots, N\}$ (exercise), h is also bijective. This proves $\phi(n+1)$ and completes the induction. ■

Theorem 3.18. *For each finite set A (i.e. $\#A = n \in \mathbb{N}_0$), one has $\#\mathcal{P}(A) = 2^n$.*

Proof. The proof is conducted by induction by showing

$$\underset{n \in \mathbb{N}_0}{\forall} \underbrace{\big(\#A = n \;\Rightarrow\; \#\mathcal{P}(A) = 2^n\big)}_{\phi(n)}.$$

Base Case ($n = 0$): For $n = 0$, we have $A = \emptyset$, i.e. $\mathcal{P}(A) = \{\emptyset\}$. Thus, $\#\mathcal{P}(A) = 1 = 2^0$, proving $\phi(0)$.

Induction Step: Assume $\phi(n)$ and consider A with $\#A = n + 1$. Then A contains at least one element a. For $B := A \setminus \{a\}$, we then know $\#B = n$ from Th. 3.13(b).

Moreover, setting $\mathcal{M} := \big\{C \cup \{a\} : C \in \mathcal{P}(B)\big\}$, we have the disjoint decomposition $\mathcal{P}(A) = \mathcal{P}(B) \dot\cup \mathcal{M}$. As the map $\varphi : \mathcal{P}(B) \longrightarrow \mathcal{M}$, $\varphi(C) := C \cup \{a\}$, is clearly bijective, $\mathcal{P}(B)$ and $\mathcal{M}$ have the same cardinality. Thus,

$$\#\mathcal{P}(A) \overset{\text{Th. 3.16}}{=} \#\mathcal{P}(B) + \#\mathcal{M} = \#\mathcal{P}(B) + \#\mathcal{P}(B) \overset{(\phi(n))}{=} 2 \cdot 2^n = 2^{n+1},$$

thereby proving $\phi(n+1)$ and completing the induction. ■

Remark 3.19. In the proof of the following Th. 3.20, we will encounter a new proof technique that we did not use before, the so-called *proof by contradiction*, also called *indirect proof*. It is based on the observation, called the *principle of contradiction*, that $A \wedge \neg A$ is always false:

A	$\neg A$	$A \wedge \neg A$
T	F	F
F	T	F

(3.26)

Thus, one possibility of proving a statement B to be true is to show $\neg B \Rightarrow A \wedge \neg A$ for some arbitrary statement A. Since the right-hand side of the implication is false, the left-hand side must also be false, proving B is true.

Theorem 3.20. *Let A be a set. There can never exist a surjective map from A onto $\mathcal{P}(A)$ (in this sense, the size of $\mathcal{P}(A)$ is always strictly bigger than the size of A; in particular, A and $\mathcal{P}(A)$ can never have the same size).*

Proof. If $A = \emptyset$, then there is nothing to prove. For nonempty A, as mentioned above, the idea is to conduct a proof by contradiction. To this end, assume there does exist a surjective map $f : A \longrightarrow \mathcal{P}(A)$ and define

$$B := \{x \in A : x \notin f(x)\}. \tag{3.27}$$

Now B is a subset of A, i.e. $B \in \mathcal{P}(A)$ and the assumption that f is surjective implies the existence of $a \in A$ such that $f(a) = B$. If $a \in B$, then $a \notin f(a) = B$, i.e. $a \in B$ implies $a \in B \wedge \neg(a \in B)$, so that the principle of contradiction tells us $a \notin B$ must be true. However, $a \notin B$ implies $a \in f(a) = B$, i.e., this time, the principle of contradiction tells us $a \in B$ must be true. In conclusion, we have shown our original assumption that there exists a surjective map $f : A \longrightarrow \mathcal{P}(A)$ implies $a \in B \wedge \neg(a \in B)$, i.e., according to the principle of contradiction, no surjective map from A into $\mathcal{P}(A)$ can exist. ■

We conclude the section with a number of important results regarding the natural numbers and countability.

Theorem 3.21. **(a)** *Every nonempty finite subset of a totally ordered set has a minimum and a maximum.*

(b) *Every nonempty subset of $\mathbb{N}$ has a minimum.*

Proof. (a): Let A be a set and let $\leq$ denote a total order on A. Moreover, let $\emptyset \neq B \subseteq A$. We show by induction

$$\underset{n\in\mathbb{N}}{\forall} \underbrace{\big(\#B = n \;\Rightarrow\; B \text{ has a min}\big)}_{\phi(n)}.$$

Base Case ($n = 1$): For $n = 1$, B contains a unique element b, i.e. $b = \min B$, proving $\phi(1)$.

Induction Step: Suppose $\phi(n)$ holds and consider B with $\#B = n + 1$. Let b be one element from B. Then $C := B \setminus \{b\}$ has cardinality n and, according to the induction hypothesis, there exists $c \in C$ satisfying $c = \min C$. If $c \leq b$, then $c \leq x$ for each $x \in B$, proving $c = \min B$. If $b \leq c$, then $b \leq x$ for each $x \in B$, proving $b = \min B$. In each case, B has a min, proving $\phi(n + 1)$ and completing the induction.

(b): Let $\emptyset \neq A \subseteq \mathbb{N}$. We have to show A has a min. If A is finite, then A has a min by (a). If A is infinite, let n be an element from A. Then the finite set $B := \{k \in A : k \leq n\}$ must have a min m by (a). Since $m \leq x$ for each $x \in B$ and $m \leq n < x$ for each $x \in A \setminus B$, we have $m = \min A$. ■

Proposition 3.22. *Every subset A of $\mathbb{N}$ is countable.*

Proof. Since $\emptyset$ is countable, we may assume $A \neq \emptyset$. From Th. 3.21(b), we know that every nonempty subset of $\mathbb{N}$ has a min. We recursively define a sequence in A by

$$a_1 := \min A, \quad a_{n+1} := \begin{cases} \min A_n & \text{if } A_n := A \setminus \{a_i : 1 \leq i \leq n\} \neq \emptyset, \\ a_n & \text{if } A_n = \emptyset. \end{cases}$$

This sequence is the same as the function $f : \mathbb{N} \longrightarrow A$, $f(n) = a_n$. An easy induction shows that, for each $n \in \mathbb{N}$, $a_n \neq a_{n+1}$ implies the restriction $f\restriction_{\{1,\ldots,n+1\}}$ is injective. Thus, if there exists $n \in \mathbb{N}$ such that $a_n = a_{n+1}$, then $f\restriction_{\{1,\ldots,k\}}\colon \{1, \ldots, k\} \longrightarrow A$ is bijective, where $k := \min\{n \in \mathbb{N} : a_n = a_{n+1}\}$, showing A is finite, i.e. countable. If there does not exist $n \in \mathbb{N}$ with $a_n = a_{n+1}$, then f is injective. Another easy induction shows that, for each $n \in \mathbb{N}$, $f(\{1, \ldots, n\}) \supseteq \{k \in A : k \leq n\}$, showing f is also surjective, proving A is countable. ■

Proposition 3.23. *For each set $A \neq \emptyset$, the following three statements are equivalent:*

(i) *A is countable.*

(ii) *There exists an injective map $f : A \longrightarrow \mathbb{N}$.*

(iii) *There exists a surjective map $g : \mathbb{N} \longrightarrow A$.*

Proof. Directly from the definition of countable in Def. 3.12(c), one obtains (i)⇒(ii) and (i)⇒(iii). To prove (ii)⇒(i), let $f : A \longrightarrow \mathbb{N}$ be injective. Then $f : A \longrightarrow f(A)$ is bijective, and, since $f(A) \subseteq \mathbb{N}$, $f(A)$ is countable by Prop. 3.22, proving A is countable as well. To prove (iii)⇒(i), let $g : \mathbb{N} \longrightarrow A$ be surjective. According to Th. 2.12(a), g has a right inverse $f : A \longrightarrow \mathbb{N}$, i.e. $g \circ f = \mathrm{Id}_A$. But this means g is a left inverse for f, showing f is injective according to Th. 2.12(b). Then A is countable by an application of (ii). ■

Theorem 3.24. *If $(A_1, \ldots, A_n)$, $n \in \mathbb{N}$, is a finite family of countable sets, then $\prod_{i=1}^n A_i$ is countable.*

Proof. We first consider the special case $n = 2$ with $A_1 = A_2 = \mathbb{N}$ and show the map

$$\varphi : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}, \quad \varphi(m, n) := 2^m \cdot 3^n,$$

is injective: If $\varphi(m, n) = \varphi(p, q)$, then $2^m \cdot 3^n = 2^p \cdot 3^q$. Moreover $m \leq p$ or $p \leq m$. If $m \leq p$, then $3^n = 2^{p-m} \cdot 3^q$. Since 3^n is odd, $2^{p-m} \cdot 3^q$ must also be odd, implying $p - m = 0$, i.e. $m = p$. Moreover, we now have $3^n = 3^q$, implying $n = q$, showing $(m, n) = (p, q)$, i.e. φ is injective.

We now come back to the general case stated in the theorem. If at least one of the A_i is empty, then A is empty. So it remains to consider the case, where all A_i are nonempty. The proof is conducted by induction by showing

$$\underset{n\in\mathbb{N}}{\forall} \quad \underbrace{\prod_{i=1}^{n} A_i \ \text{ is countable}}_{\phi(n)}.$$

Base Case ($n = 1$): $\phi(1)$ is merely the hypothesis that A_1 is countable.

Induction Step: Assuming $\phi(n)$, Prop. 3.23(ii) provides injective maps $f_1 : \prod_{i=1}^n A_i \longrightarrow \mathbb{N}$ and $f_2 : A_{n+1} \longrightarrow \mathbb{N}$. To prove $\phi(n+1)$, we provide an injective map $h : \prod_{i=1}^{n+1} A_i \longrightarrow \mathbb{N}$: Define

$$h : \prod_{i=1}^{n+1} A_i \longrightarrow \mathbb{N}, \quad h(a_1, \ldots, a_n, a_{n+1}) := \varphi\big(f_1(a_1, \ldots, a_n), f_2(a_{n+1})\big).$$

The injectivity of f_1, f_2, and φ clearly implies the injectivity of h, thereby proving $\phi(n + 1)$ and completing the induction. ∎

Theorem 3.25. *If $(A_i)_{i\in I}$ is a countable family of countable sets (i.e. $\emptyset \neq I$ is countable and each A_i, $i \in I$, is countable), then the union $A := \bigcup_{i\in I} A_i$ is also countable.*

Proof. It suffices to consider the case that all A_i are nonempty. Moreover, according to Prop. 3.23(iii), it suffices to construct a surjective map $\varphi : \mathbb{N} \longrightarrow A$. Also according to Prop. 3.23(iii), the countability of I and the A_i provides us with surjective maps $f : \mathbb{N} \longrightarrow I$ and $g_i : \mathbb{N} \longrightarrow A_i$. Define

$$F : \mathbb{N} \times \mathbb{N} \longrightarrow A, \quad F(m, n) := g_{f(m)}(n).$$

Then F is surjective: Given $x \in A$, there exists $i \in I$ such that $x \in A_i$. Since f is surjective, there is $m \in \mathbb{N}$ satisfying $f(m) = i$. Moreover, since g_i is surjective, there exists $n \in \mathbb{N}$ with $g_i(n) = x$. Then $F(m, n) = g_i(n) = x$, verifying that F is surjective. As $\mathbb{N} \times \mathbb{N}$ is countable by Th. 3.24, there exists a surjective map $h : \mathbb{N} \longrightarrow \mathbb{N} \times \mathbb{N}$. Thus, $F \circ h$ is the desired surjective map from $\mathbb{N}$ onto A. Note: The axiom of choice (AC, see [Phi16, Sec. A.4]) is used when choosing each g_i from the set of all surjective maps from $\mathbb{N}$ onto A_i. It has actually been shown that it is impossible to prove the theorem without using AC (cf. [Phi16, Rem. 3.18]). ∎

4 Real Numbers

4.1 The Real Numbers as a Complete Totally Ordered Field

The set of real numbers, denoted $\mathbb{R}$, is a set with special properties, namely a so-called *complete totally ordered field*. We already know what totally ordered means, but we still need to explain what a field is, what an ordered field is, and what it means for a total order to be complete. We begin with the last part.

Definition 4.1. A total order $\leq$ on a nonempty set A is called *complete* if, and only if, every nonempty subset B of A that is bounded from above has a supremum, i.e.

$$\forall_{B\in\mathcal{P}(A)\setminus\{\emptyset\}} \left(\left(\exists_{x\in A} \ \forall_{b\in B} \ b \leq x \right) \quad \Rightarrow \quad \exists_{s\in A} \ s = \sup B \right). \tag{4.1}$$

Lemma 4.2. *A total order $\leq$ on a nonempty set A is complete if, and only if, every nonempty subset B of A that is bounded from below has an infimum.*

Proof. According to Lem. 2.28, it suffices to prove one implication. We show that (4.1) implies that every nonempty B bounded from below has an infimum: Define

$$C := \{x \in A : x \text{ is lower bound for } B\}. \tag{4.2}$$

Then every $b \in B$ is an upper bound for C and (4.1) implies there exists $s = \sup C \in A$. To verify $s = \inf B$, it remains to show $s \in C$, i.e. that s is a lower bound for B. However, every $b \in B$ is an upper bound for C and $s = \sup C$ is the min of all upper bounds for C, i.e. $s \leq b$ for each $b \in B$, showing $s \in C$. ∎

Definition 4.3. Let A be a nonempty set with a map

$$\circ : A \times A \longrightarrow A, \quad (x, y) \mapsto x \circ y \tag{4.3}$$

(called a *composition* on A, the examples we have in mind are addition and multiplication on $\mathbb{R}$). Then A is called a *group* with respect to $\circ$ if, and only if, the following three conditions are satisfied:

(i) Associativity: $x \circ (y \circ z) = (x \circ y) \circ z$ holds for all $x, y, z \in A$.

(ii) There exists a *neutral element* $e \in A$, i.e. an element $e \in A$ such that

$$\forall_{x\in A} \ x \circ e = x.$$

(iii) For each $x \in A$, there exists an *inverse element* $\overline{x} \in A$, i.e. an element $\overline{x} \in A$ such that

$$x \circ \overline{x} = e.$$

A is called a *commutative* or *abelian* group if, and only if, it is a group and satisfies the additional condition:

(iv) Commutativity: $x \circ y = y \circ x$ holds for all $x, y \in A$.

Definition 4.4. Let A be a nonempty set with two maps

$$\begin{aligned} + &: A \times A \longrightarrow A, \quad (x, y) \mapsto x + y, \\ \cdot &: A \times A \longrightarrow A, \quad (x, y) \mapsto x \cdot y \end{aligned} \tag{4.4}$$

($+$ is called *addition* and $\cdot$ is called *multiplication*; often one writes xy instead of $x \cdot y$). Then A is called a *field* if, and only if, the following three conditions are satisfied:

(i) A is a commutative group with respect to $+$. The neutral element with respect to $+$ is denoted 0.

(ii) $A \setminus \{0\}$ is a commutative group with respect to $\cdot$. The neutral element with respect to $\cdot$ is denoted 1.

(iii) Distributivity:

$$\underset{x,y,z \in A}{\forall} x \cdot (y + z) = x \cdot y + x \cdot z. \tag{4.5}$$

If A is a field and $\leq$ is a total order on A, then A is called a *totally ordered field* if, and only if, the following condition is satisfied:

(iv) Compatibility with Addition and Multiplication:

$$\underset{x,y,z \in A}{\forall} \big(x \leq y \;\Rightarrow\; x + z \leq y + z\big), \tag{4.6a}$$

$$\underset{x,y \in A}{\forall} \big(0 \leq x \wedge 0 \leq y \;\Rightarrow\; 0 \leq xy\big). \tag{4.6b}$$

Finally, A is called a *complete totally ordered field* if, and only if, A is a totally ordered field that is complete in the sense of Def. 4.1.

Theorem 4.5. *There exists a complete totally ordered field* $\mathbb{R}$ *(it is called the set of* real numbers*). Moreover,* $\mathbb{R}$ *is unique* up to isomorphism*, i.e. if* A *is a complete totally ordered field, then there exists an isomorphism* $\phi : A \longrightarrow \mathbb{R}$*, i.e. a bijective map* $\phi : A \longrightarrow \mathbb{R}$*, satisfying*

$$\underset{x,y \in A}{\forall} \phi(x + y) = \phi(x) + \phi(y), \tag{4.7a}$$

$$\underset{x,y \in A}{\forall} \phi(xy) = \phi(x)\phi(y), \tag{4.7b}$$

$$\underset{x,y \in A}{\forall} \big(x < y \;\Rightarrow\; \phi(x) < \phi(y)\big). \tag{4.7c}$$

It also turns out that the isomorphism is unique.

Proof. To really prove the existence of the real numbers by providing a construction is tedious and not easy. One possible construction is provided in [Phi16, Sec. D] (the existence proof is completed in [Phi16, Th. D.41], the results regarding the isomorphism can be found in [Phi16, Th. D.45]). ■

Theorem 4.6. *The following statements and rules are valid in the set of real numbers* $\mathbb{R}$ *(and, more generally, in every field):*

(a) *Inverse elements are unique. For each* $x \in \mathbb{R}$*, the unique inverse with respect to addition is denoted by* $-x$*. Also define* $y - x := y + (-x)$*. For each* $x \in \mathbb{R} \setminus \{0\}$*, the unique inverse with respect to multiplication is denoted by* x^{-1}*. For* $x \neq 0$*, define the* fractions $\frac{y}{x} := y/x := yx^{-1}$ *with* numerator y *and* denominator x*.*

(b) $-(-x) = x$ *and* $(x^{-1})^{-1} = x$ *for* $x \neq 0$*.*

(c) $(-x) + (-y) = -(x + y)$ *and* $x^{-1}y^{-1} = (xy)^{-1}$ *for* $x, y \neq 0$*.*

(d) $x + a = y + a \;\Rightarrow\; x = y$ *and, for* $a \neq 0$*,* $xa = ya \;\Rightarrow\; x = y$*.*

(e) $x \cdot 0 = 0$*.*

(f) $x(-y) = -(xy)$*.*

(g) $(-x)(-y) = xy$*.*

(h) $x(y - z) = xy - xz$*.*

(i) $xy = 0 \;\Rightarrow\; x = 0 \vee y = 0$*.*

(j) Rules for Fractions:

$$\frac{a}{c} + \frac{b}{d} = \frac{ad + bc}{cd}, \quad \frac{a}{c} \cdot \frac{b}{d} = \frac{ab}{cd}, \quad \frac{a/c}{b/d} = \frac{ad}{bc},$$

where all denominators are assumed $\neq 0$*.*

Proof. (a): Let a, b be additive inverses to x. Then $a = a + 0 = a + x + b = 0 + b = b$. The multiplicative case is proved completely analogously.

(b): $-x + x = 0$ already shows that x is the inverse to $-x$, i.e. $-(-x) = x$. The multiplicative case is proved completely analogously.

(c): $x + y + (-x) + (-y) = x - x + y - y = 0$, showing $(-x) + (-y)$ is the inverse to $(x + y)$. The multiplicative case is proved completely analogously.

(d): If $x + a = y + a$, then $x = x + a - a = y + a - a = y$. Again, the multiplicative case is proved completely analogously.

(e): One computes

$$x \cdot 0 + x \cdot 1 \overset{(4.5)}{=} x \cdot (0 + 1) = x \cdot 1 = 0 + x \cdot 1,$$

i.e. $x \cdot 0 = 0$ follows from (d).

(f): $xy + x(-y) = x(y - y) = x \cdot 0 = 0$, where we used (4.5) and (e). This shows $x(-y)$ is the additive inverse to xy.

(g): $xy = -(-(xy)) = -(x(-y)) = -((-y)x) = (-y)(-x)$, where (f) was used twice.

(h): $x(y-z) = x(y+(-z)) = xy + x(-z) = xy - xz$.

(i): If $xy = 0$ and $x \neq 0$, then $y = 1 \cdot y = x^{-1}xy = x^{-1} \cdot 0 = 0$.

(j): One computes

$$\frac{a}{c} + \frac{b}{d} = ac^{-1} + bd^{-1} = add^{-1}c^{-1} + bcc^{-1}d^{-1} = (ad+bc)(cd)^{-1} = \frac{ad+bc}{cd}$$

and

$$\frac{a}{c} \cdot \frac{b}{d} = ac^{-1}bd^{-1} = ab(cd)^{-1} = \frac{ab}{cd}$$

and

$$\frac{a/c}{b/d} = ac^{-1}(bd^{-1})^{-1} = ac^{-1}b^{-1}d = ad(bc)^{-1} = \frac{ad}{bc},$$

completing the proof. ■

Theorem 4.7. *The following statements and rules are valid in the set of real numbers* $\mathbb{R}$ *(and, more generally, in every totally ordered field):*

(a) $x \leq y \;\Rightarrow\; -x \geq -y$.

(b) $x \leq y \wedge z \geq 0 \;\Rightarrow\; xz \leq yz$ *holds as well as* $x \leq y \wedge z \leq 0 \;\Rightarrow\; xz \geq yz$.

(c) $x \neq 0 \;\Rightarrow\; x^2 := x \cdot x > 0$. *In particular* $1 > 0$.

(d) $x > 0 \;\Rightarrow\; 1/x > 0$, *whereas* $x < 0 \;\Rightarrow\; 1/x < 0$.

(e) *If* $0 < x < y$, *then* $x/y < 1$, $y/x > 1$, *and* $1/x > 1/y$.

(f) $x < y \wedge u < v \;\Rightarrow\; x + u < y + v$.

(g) $0 < x < y \wedge 0 < u < v \;\Rightarrow\; xu < yv$.

(h) $x < y \wedge 0 < \lambda < 1 \;\Rightarrow\; x < \lambda x + (1-\lambda)y < y$. *In particular* $x < \frac{x+y}{2} < y$.

Proof. (a): Using (4.6a): $x \leq y \;\Rightarrow\; 0 \leq y - x \;\Rightarrow\; -y \leq -x$.

(b): One argues, for $z \geq 0$,

$$x \leq y \;\Rightarrow\; 0 \leq y - x \overset{(4.6b)}{\Rightarrow} 0 \leq (y-x)z = yz - xz \;\Rightarrow\; xz \leq yz,$$

and, for $z \leq 0$,

$$x \leq y \;\Rightarrow\; 0 \leq y - x \overset{(4.6b)}{\Rightarrow} 0 \leq (y-x)(-z) = xz - yz \;\Rightarrow\; xz \geq yz.$$

(c): From (4.6b), one obtains $x^2 \geq 0$. From Th. 4.6(i), one then gets $x^2 > 0$.

(d): If $x > 0$, then $x^{-1} < 0$ implies the false statement $1 = xx^{-1} < 0$, i.e. $x^{-1} > 0$. The case $x < 0$ is treated analogously.

(e): Using (d), we obtain from $0 < x < y$ that $x/y = xy^{-1} < yy^{-1} = 1$ and $1 = xx^{-1} < yx^{-1} = y/x$.

(f): $x < y \;\Rightarrow\; x + u < y + u$ and $u < v \;\Rightarrow\; y + u < y + v$; both combined yield $x + u < y + v$.

(g): $0 < x < y \wedge 0 < u < v \;\Rightarrow\; xu < yu \wedge yu < yv \;\Rightarrow\; xu < yv$.

(h): Since $0 < \lambda$ and $1 - \lambda > 0$, $x < y$ implies

$$\lambda x < \lambda y \quad \wedge \quad (1 - \lambda)x < (1 - \lambda)y.$$

Using (4.6a), we obtain

$$x = \lambda x + (1 - \lambda)x < \lambda x + (1 - \lambda)y < \lambda y + (1 - \lambda)y = y,$$

completing the proof of the theorem. ■

Theorem 4.8. *Let $\emptyset \neq A, B \subseteq \mathbb{R}$, $\lambda \in \mathbb{R}$, and define*

$$A + B := \{a + b : \; a \in A \wedge b \in B\}, \tag{4.8a}$$
$$\lambda A := \{\lambda a : \; a \in A\}. \tag{4.8b}$$

If A and B are bounded, then

$$\sup(A + B) = \sup A + \sup B, \tag{4.9a}$$
$$\inf(A + B) = \inf A + \inf B, \tag{4.9b}$$
$$\sup(\lambda A) = \begin{cases} \lambda \cdot \sup A & \text{for } \lambda \geq 0, \\ \lambda \cdot \inf A & \text{for } \lambda < 0, \end{cases} \tag{4.9c}$$
$$\inf(\lambda A) = \begin{cases} \lambda \cdot \inf A & \text{for } \lambda \geq 0, \\ \lambda \cdot \sup A & \text{for } \lambda < 0. \end{cases} \tag{4.9d}$$

Proof. Exercise. ■

4.2 Important Subsets

Remark 4.9. We would like to recover the natural numbers $\mathbb{N}$ as a subset of $\mathbb{R}$. Indeed, if we start with 1 as the neutral element of multiplication and define $2 := 1+1$, $3 := 2+1$, $\ldots$, then $\mathbb{N} := \{1, 2, \ldots\}$ is a subset of $\mathbb{R}$, satisfying the Peano axioms P1, P2, P3 of Sec. 3.1. However, if one does actually construct $\mathbb{R}$ according to the axioms of axiomatic set theory, then one starts by constructing $\mathbb{N}$ first (basically as we did in Rem. 1.27 and Def. 1.26), constructing $\mathbb{R}$ from $\mathbb{N}$ in several steps (cf. [Phi16, Sec. D]). Depending on the construction used, the original set of natural numbers will typically not be the same set as the natural numbers as a subset of $\mathbb{R}$. However, both sets will satisfy the Peano axioms and you will have a canonical bijection between the two sets. Which one you consider the "genuine" set of natural numbers depends on your personal taste

and philosophy and is completely irrelevant. Any two models of $\mathbb{N}$ will always produce equivalent results, since they must both satisfy the three Peano axioms.

—

We now introduce a zoo of important subsets of $\mathbb{R}$ together with corresponding notation:

$$\begin{aligned}
\mathbb{N} &:= \{1, 2, 3, \dots\} && \text{(natural numbers)}, && (4.10a)\\
\mathbb{N}_0 &:= \mathbb{N} \cup \{0\}, && && (4.10b)\\
\mathbb{Z}^- &:= \{-n : n \in \mathbb{N}\} && \text{(negative integers)}, && (4.10c)\\
\mathbb{Z} &:= \mathbb{Z}^- \cup \mathbb{N}_0 && \text{(integers)}, && (4.10d)\\
\mathbb{Q}^+ &:= \{m/n : m, n \in \mathbb{N}\} && \text{(positive rational numbers)}, && (4.10e)\\
\mathbb{Q}_0^+ &:= \mathbb{Q}^+ \cup \{0\} && \text{(nonnegative rational numbers)}, && (4.10f)\\
\mathbb{Q}^- &:= \{-q : q \in \mathbb{Q}^+\} && \text{(negative rational numbers)}, && (4.10g)\\
\mathbb{Q}_0^- &:= \mathbb{Q}^- \cup \{0\} && \text{(nonpositive rational numbers)}, && (4.10h)\\
\mathbb{Q} &:= \mathbb{Q}_0^+ \cup \mathbb{Q}^- && \text{(rational numbers)}, && (4.10i)\\
\mathbb{R}^+ &:= \{x \in \mathbb{R} : x > 0\} && \text{(positive real numbers)}, && (4.10j)\\
\mathbb{R}_0^+ &:= \{x \in \mathbb{R} : x \geq 0\} && \text{(nonnegative real numbers)}, && (4.10k)\\
\mathbb{R}^- &:= \{x \in \mathbb{R} : x < 0\} && \text{(negative real numbers)}, && (4.10l)\\
\mathbb{R}_0^- &:= \{x \in \mathbb{R} : x \leq 0\} && \text{(nonpositive real numbers)}. && (4.10m)
\end{aligned}$$

For $a, b \in \mathbb{R}$ with $a \leq b$, one also defines the following *intervals*:

$$\begin{aligned}
[a, b] &:= \{x \in \mathbb{R} : a \leq x \leq b\} && \text{(bounded closed interval)}, && (4.11a)\\
]a, b[&:= \{x \in \mathbb{R} : a < x < b\} && \text{(bounded open interval)}, && (4.11b)\\
]a, b] &:= \{x \in \mathbb{R} : a < x \leq b\} && \text{(bounded half-open interval)}, && (4.11c)\\
[a, b[&:= \{x \in \mathbb{R} : a \leq x < b\} && \text{(bounded half-open interval)}, && (4.11d)\\
]-\infty, b] &:= \{x \in \mathbb{R} : x \leq b\} && \text{(unbounded closed interval)}, && (4.11e)\\
]-\infty, b[&:= \{x \in \mathbb{R} : x < b\} && \text{(unbounded open interval)}, && (4.11f)\\
[a, \infty[&:= \{x \in \mathbb{R} : a \leq x\} && \text{(unbounded closed interval)}, && (4.11g)\\
]a, \infty[&:= \{x \in \mathbb{R} : a < x\} && \text{(unbounded open interval)}. && (4.11h)
\end{aligned}$$

For $a = b$, one says that the intervals defined by (4.11a) – (4.11d) are *degenerate* or *trivial*, where $[a, a] = \{a\}$, $]a, a[=]a, a] = [a, a[= \emptyset$ – it is sometimes convenient to have included the degenerate cases in the definition. It is sometimes also useful to abandon the restriction $a \leq b$, to let $c := \min\{a, b\}$, $d := \max\{a, b\}$, and to define

$$[a, b] := [c, d], \quad]a, b[:=]c, d[, \quad]a, b] := [c, d] \setminus \{a\}, \quad [a, b[:= [c, d] \setminus \{b\}. \tag{4.11i}$$

Theorem 4.10 (Archimedean Property)**.** *Let ϵ, x be real numbers. If $\epsilon > 0$ and $x > 0$, then there exists $n \in \mathbb{N}$ such that $n\,\epsilon > x$.*

Proof. We conduct the proof by contradiction: Suppose x is an upper bound for the set $A := \{n\,\epsilon : n \in \mathbb{N}\}$. Since the order $\leq$ on $\mathbb{R}$ is complete, according to (4.1), there exists $s \in \mathbb{R}$ such that $s = \sup A$. In particular, $s - \epsilon$ is not an upper bound for A, i.e. there exists $n \in \mathbb{N}$ satisfying $n\,\epsilon > s - \epsilon$. But then $(n+1)\,\epsilon > s$ in contradiction to $s = \sup A$. This shows x is not an upper bound for A, thereby establishing the case. ■

5 Complex Numbers

5.1 Definition and Basic Arithmetic

According to Th. 4.7(c), $x^2 \geq 0$ holds for every real number $x \in \mathbb{R}$, i.e. the equation $x^2 + 1 = 0$ has no solution in $\mathbb{R}$. This deficiency of the real numbers motivates the effort to try to extend the field of real numbers to a larger field $\mathbb{C}$, the so-called *complex numbers*. The two requirements that $\mathbb{C}$ is to be a field containing $\mathbb{R}$ and that there is to be some complex number $i \in \mathbb{C}$ satisfying $i^2 = -1$ already dictates the following laws of addition and multiplication for complex numbers $z = x + iy$ and $w = u + iv$ with $x, y, u, v \in \mathbb{R}$:

$$z + w = x + iy + u + iv = x + u + i(y + v), \tag{5.1a}$$

$$zw = (x + iy)(u + iv) = xu - yv + i(xv + yu). \tag{5.1b}$$

Moreover, if $x + iy = u + iv$, then $(x - u)^2 = -(v - y)^2$, i.e. $x - u = 0 = v - y$, implying $x = u$ and $y = v$. This suggests to try defining complex numbers as pairs of real numbers. Indeed, this works:

Definition 5.1. We define the set of *complex numbers* $\mathbb{C} := \mathbb{R} \times \mathbb{R}$, where, keeping in mind (5.1), *addition* on $\mathbb{C}$ is defined by

$$+ : \mathbb{C} \times \mathbb{C} \longrightarrow \mathbb{C}, \qquad \big((x, y), (u, v)\big) \mapsto (x, y) + (u, v) := (x + u, y + v), \tag{5.2}$$

and *multiplication* on $\mathbb{C}$ is defined by

$$\cdot : \mathbb{C} \times \mathbb{C} \longrightarrow \mathbb{C}, \qquad \big((x, y), (u, v)\big) \mapsto (x, y) \cdot (u, v) := (xu - yv,\, xv + yu). \tag{5.3}$$

Theorem 5.2. (a) *The set of complex numbers $\mathbb{C}$ with addition and multiplication as defined in Def.* 5.1 *forms a field, where $(0, 0)$ and $(1, 0)$ are the neutral elements with respect to addition and multiplication, respectively,*

$$-z := (-x, -y) \tag{5.4a}$$

is the additive inverse to $z = (x, y)$, whereas

$$z^{-1} := \frac{1}{z} := \left(\frac{x}{x^2 + y^2}, \frac{-y}{x^2 + y^2}\right) \tag{5.4b}$$

is the multiplicative inverse to $z = (x, y) \neq (0, 0)$.

(b) *Defining* subtraction *and* division *in the usual way, for each* $z, w \in \mathbb{C}$*, by* $w - z := w + (-z)$*, and* $w/z := wz^{-1}$ *for* $z \neq (0,0)$*, respectively, all the rules stated in Th.* 4.6 *are valid in* $\mathbb{C}$*.*

(c) *The map*

$$\iota : \mathbb{R} \longrightarrow \mathbb{C}, \quad \iota(x) := (x, 0), \tag{5.5}$$

is a monomorphism, i.e. it is injective and satisfies

$$\underset{x,y\in\mathbb{R}}{\forall} \quad \iota(x+y) = \iota(x) + \iota(y), \tag{5.6a}$$

$$\underset{x,y\in\mathbb{R}}{\forall} \quad \iota(xy) = \iota(x) \cdot \iota(y). \tag{5.6b}$$

It is customary to identify $\mathbb{R}$ *with* $\iota(\mathbb{R})$*, as it usually does not cause any confusion. One then just writes* x *instead of* $(x, 0)$*.*

Proof. All computations required for (a) and (c) are straightforward and are left as an exercise; (b) is a consequence of (a), since Th. 4.6 and its proof are valid in every field. ■

Notation 5.3. The number $i := (0, 1)$ is called the *imaginary unit* (note that, indeed, $i^2 = i \cdot i = (0, 1) \cdot (0, 1) = (0 \cdot 0 - 1 \cdot 1,\, 0 \cdot 1 + 1 \cdot 0) = (-1, 0) = -1$). Using i, one obtains the commonly used representation of a complex number $z = (x, y) \in \mathbb{C}$:

$$z = (x, y) = x \cdot (1, 0) + y \cdot (0, 1) = x + iy, \tag{5.7}$$

where one calls $\operatorname{Re} z := x$ the *real part* of z and $\operatorname{Im} z := y$ the *imaginary part* of z. Moreover, z is called *purely imaginary* if, and only if, $\operatorname{Re} z = 0$ (as a consequence of this convention, one has the (harmless) pathology that 0 is both real and purely imaginary).

Remark 5.4. There does not exist a total order $\leq$ on $\mathbb{C}$ that makes $\mathbb{C}$ into a totally ordered field (i.e. no total order on $\mathbb{C}$ can be compatible with addition and multiplication in the sense of (4.6)): Indeed, if there were such a total order $\leq$ on $\mathbb{C}$, then all the rules of Th. 4.7 had to be valid with respect to that total order $\leq$. In particular, $0 < 1^2 = 1$ and $0 < i^2 = -1$ had to be valid by Th. 4.7(c), and, then, $0 < 1 + (-1) = 0$ had to be valid by Th. 4.7(f). However, $0 < 0$ is false, showing that there is no total order on $\mathbb{C}$ that satisfies (4.6). Caveat: Of course, there *do* exist total orders on $\mathbb{C}$, just none compatible with addition and multiplication – for example, the lexicographic order on $\mathbb{R} \times \mathbb{R}$ (defined as it was in (2.51) for $\mathbb{N} \times \mathbb{N}$) constitutes a total order on $\mathbb{C}$.

Definition and Remark 5.5. Conjugation: For each complex number $z = x + iy$, we define its *complex conjugate* or just *conjugate* to be the complex number $\bar{z} := x - iy$. We then have the following rules that hold for each $z = x + iy, w = u + iv \in \mathbb{C}$:

(a) $\overline{z + w} = x+u-iy-iv = \bar{z}+\bar{w}$ and $\overline{zw} = xu-yv-(xv+yu)i = (x-iy)(u-iv) = \bar{z}\bar{w}$.

(b) $z + \bar{z} = 2x = 2 \operatorname{Re} z$ and $z - \bar{z} = 2yi = 2i \operatorname{Im} z$.

(c) $z = \bar{z} \;\Leftrightarrow\; x + iy = x - iy \;\Leftrightarrow\; y = 0 \;\Leftrightarrow\; z \in \mathbb{R}$.

(d) $z\bar{z} = (x+iy)(x-iy) = x^2+y^2 \in \mathbb{R}_0^+$.

Notation 5.6. Exponentiation with Integer Exponents: Define recursively for each $z \in \mathbb{C}$ and each $n \in \mathbb{N}_0$:

$$z^0 := 1, \quad \underset{n\in\mathbb{N}_0}{\forall} \quad z^{n+1} := z \cdot z^n, \quad \text{and for } z \neq 0: \quad z^{-n} := (z^{-1})^n. \tag{5.8}$$

Theorem 5.7. Exponentiation Rules: *Let $z, w \in \mathbb{C}$. For $z, w \neq 0$, the following rules hold for every $m, n \in \mathbb{Z}$; otherwise they hold for each $m, n \in \mathbb{N}_0$:*

(a) $z^{m+n} = z^m \cdot z^n$.

(b) $z^n w^n = (zw)^n$.

(c) $(z^m)^n = z^{m\,n}$.

Proof. (a): First, we prove the statement for each $m \in \mathbb{N}_0$ by induction: The base case ($m = 0$) is $z^n = z^n$, which is true. For the induction step, we compute

$$z^{m+1+n} \overset{(5.8)}{=} z \cdot z^{m+n} \overset{\text{ind. hyp.}}{=} z \cdot z^m \cdot z^n \overset{(5.8)}{=} z^{m+1} z^n,$$

completing the induction step. The above prove allows $n < 0$ for $z \neq 0$. Interchanging m and n covers the case $m < 0$ and $n \geq 0$. If $m < 0$ and $n < 0$, then

$$z^{m+n} = z^{-(-m-n)} \overset{(5.8)}{=} (z^{-1})^{-m-n} = (z^{-1})^{-m} \cdot (z^{-1})^{-n} \overset{(5.8)}{=} z^m \cdot z^n.$$

(b): For $n \in \mathbb{N}_0$, the statement is proved by induction: The base case ($n = 0$) is $z^0 w^0 = 1 = (zw)^0$, which is true. For the induction step, we compute

$$z^{n+1} w^{n+1} \overset{(5.8)}{=} z \cdot z^n \cdot w \cdot w^n \overset{\text{ind. hyp.}}{=} zw \cdot (zw)^n \overset{(5.8)}{=} (zw)^{n+1},$$

completing the induction step. For $n < 0$ and $z \neq 0$:

$$z^n w^n \overset{(5.8)}{=} (z^{-1})^{-n} (w^{-1})^{-n} = (z^{-1}w^{-1})^{-n} \overset{\text{Th. 4.6(c)}}{=} \big((zw)^{-1}\big)^{-n} \overset{(5.8)}{=} (zw)^n.$$

(c): First, we prove the statement for each $n \in \mathbb{N}_0$ by induction: The base case ($n = 0$) is $(z^m)^0 = 1 = z^0$, which is true. For the induction step, we compute

$$(z^m)^{n+1} \overset{(5.8)}{=} z^m \cdot (z^m)^n \overset{\text{ind. hyp.}}{=} z^m \cdot z^{m\,n} \overset{\text{(a)}}{=} z^{m\,n+m} = z^{m\,(n+1)},$$

completing the induction step. From (a), we also have $(z^m)^{-1} = z^{-m}$ for $z \neq 0$. Thus, for $n < 0$ and $z \neq 0$:

$$(z^m)^n \overset{(5.8)}{=} \big((z^m)^{-1}\big)^{-n} = (z^{-m})^{-n} = z^{(-m)(-n)} = z^{m\,n},$$

thereby completing the proof. ∎

5.2 Sign and Absolute Value (Modulus)

We face a certain conundrum regarding the handling of square roots. The problem is that we will need the notion of a continuous function to prove the existence of a unique square root $\sqrt{x}$ for every nonnegative real number x and, in consequence, we will have to wait until Section 7.2.5 below to carry out this proof. On the other hand, it is extremely desirable to present the theory of convergence simultaneously for real and for complex numbers, which requires the notion of the *absolute value* or *modulus* of a complex number, to be defined in Def. 5.9(b) below as the square root of a nonnegative real number.

Faced with this difficulty, we will introduce the notion of square root now, *assuming* the existence, until we can add the proof in Section 7.2.5. Some students might be worried that this might lead to a circular argument, where our later proof of the existence of square roots would somehow make use of our previous assumption of that existence. Of course, we will be careful not to make such a circular (and, thereby, logically invalid) argument. The point is that for *real numbers* the notion of absolute value does in no way depend on the notion of a square root (see Lem. 5.10 below).

Definition and Remark 5.8. We define a nonnegative real number $y \in \mathbb{R}_0^+$ to be the *square root* of the nonnegative real number $x \in \mathbb{R}_0^+$ if, and only if, $y^2 = x$. If y is the square root of x, then one uses the notation $\sqrt{x} := y$. We will see in Rem. and Def. 7.61 that every $x \in \mathbb{R}_0^+$ has a unique square root and that the function $f : \mathbb{R}_0^+ \longrightarrow \mathbb{R}_0^+$, $f(x) := \sqrt{x}$, is strictly increasing (in particular, injective).

Definition 5.9. (a) The *sign* function is defined by

$$\operatorname{sgn} : \mathbb{R} \longrightarrow \mathbb{R}, \quad \operatorname{sgn}(x) := \begin{cases} 1 & \text{for } x > 0, \\ 0 & \text{for } x = 0, \\ -1 & \text{for } x < 0. \end{cases} \tag{5.9}$$

It is emphasized that the sign function is only defined for *real* numbers (cf. Rem. 5.4)!

(b) The *absolute value* or *modulus* function is defined by

$$\operatorname{abs} : \mathbb{C} \longrightarrow \mathbb{R}_0^+, \quad z = x + iy \mapsto |z| := \sqrt{z\bar{z}} = \sqrt{x^2 + y^2}, \tag{5.10}$$

where the term *absolute value* is often preferred for real numbers $z \in \mathbb{R}$ and the term *modulus* is often preferred if one also considers complex numbers $z \notin \mathbb{R}$.

Lemma 5.10. *For each $x \in \mathbb{R}$, one has*

$$|x| = x \cdot \operatorname{sgn}(x) = \begin{cases} x & \text{for } x \geq 0, \\ -x & \text{for } x < 0. \end{cases} \tag{5.11}$$

Proof. One has

$$|x| = \sqrt{x^2} = \begin{cases} x & \text{for } x \geq 0, \\ -x & \text{for } x < 0, \end{cases} \tag{5.12}$$

as claimed. ■

Theorem 5.11. *The following rules hold for each $z, w \in \mathbb{C}$:*

(a) $z \neq 0 \;\Rightarrow\; |z| > 0$.

(b) $||z|| = |z|$.

(c) $|z| = |\bar{z}|$.

(d) $\max\{|\operatorname{Re} z|, |\operatorname{Im} z|\} \leq |z| \leq |\operatorname{Re} z| + |\operatorname{Im} z|$.

(e) $|zw| = |z||w|$.

(f) *For $w \neq 0$, one has* $|\frac{z}{w}| = \frac{|z|}{|w|}$.

(g) Triangle Inequality:

$$|z + w| \leq |z| + |w|. \tag{5.13}$$

(h) Inverse Triangle Inequality:

$$\big||z| - |w|\big| \leq |z - w|. \tag{5.14}$$

Proof. We carry out the proofs for $z, w \in \mathbb{C}$. However, for $z, w \in \mathbb{R}$, everything can easily be shown directly from (5.11), without making use of square roots.

Let $z = x + iy$ with $x, y \in \mathbb{R}$.

(a): If $z \neq 0$, then $x \neq 0$ or $y \neq 0$, i.e. $x^2 > 0$ or $y^2 > 0$ by Th. 4.7(c), implying $x^2 + y^2 > 0$ by Th. 4.7(f), i.e. $|z| = \sqrt{x^2 + y^2} > 0$.

(b): Since $a := |z| \in \mathbb{R}_0^+$, we have $|a| = \sqrt{a^2} = a = |z|$.

(c): Since $\bar{z} = x - iy$, we have $|\bar{z}| = \sqrt{x^2 + (-y)^2} = \sqrt{x^2 + y^2} = |z|$.

(d): It is $x = \operatorname{Re} z$, $y = \operatorname{Im} z$. Let $a := \max\{|x|, |y|\}$. As remarked in Def. and Rem. 5.8, the square root function is increasing and, thus, taking square roots in the chain of inequalities $a^2 \leq x^2 + y^2 \leq (|x| + |y|)^2$ implies $a \leq |z| \leq |x| + |y|$ as claimed.

(e): As remarked in Def. and Rem. 5.8, the square root function is injective, and, thus, (e) follows from

$$|zw|^2 = zw\,\overline{zw} \overset{\text{Def. and Rem. 5.5(a)}}{=} zw\bar{z}\bar{w} = z\bar{z}\,w\bar{w} = |z|^2\,|w|^2.$$

(f): Let $w = u + iv$ with $u, v \in \mathbb{R}$. We first consider the special case $z = 1$. Applying the formula (5.4b) for the inverse to w, one obtains

$$|w^{-1}|^2 = \frac{u^2}{(u^2 + v^2)^2} + \frac{v^2}{(u^2 + v^2)^2} = \frac{1}{u^2 + v^2} = \big(|w|^{-1}\big)^2,$$

i.e. $|w^{-1}| = |w|^{-1}$. Now (f) follows from (e): $|\frac{z}{w}| = |zw^{-1}| = |z||w^{-1}| = |z||w|^{-1} = \frac{|z|}{|w|}$.

(g) follows from

$$\begin{aligned} |z+w|^2 &= (z+w)(\bar{z}+\bar{w}) = z\bar{z}+w\bar{z}+z\bar{w}+w\bar{w} \\ &\overset{\text{Def. and Rem. 5.5(b)}}{=} |z|^2 + 2\,\mathrm{Re}(z\bar{w}) + |w|^2 \\ &\overset{\text{(d)}}{\leq} |z|^2 + 2|z\bar{w}| + |w|^2 = \big(|z|+|w|\big)^2, \end{aligned}$$

once again using that the square root function is increasing.

(h): Using (g), we obtain

$$\begin{aligned} |z| = |z-w+w| \leq |z-w|+|w| \quad &\Rightarrow \quad |z|-|w| \leq |z-w|, \\ |w| = |w-z+z| \leq |z-w|+|z| \quad &\Rightarrow \; -(|z|-|w|) \leq |z-w|, \end{aligned}$$

implying $\big||z|-|w|\big| \leq |z-w|$ by (5.11) (notice $|z|-|w| \in \mathbb{R}$). ■

Remark 5.12. Each complex number $(x,y) = x+iy$ can be visualized as a point in the so-called *complex plane*, where the horizontal x-axis represents real numbers and the veritcal y-axis represents purely imaginary numbers. Then the addition of complex numbers is precisely the vector addition of 2-dimensional vectors in the complex plane, and conjugation is represented by reflection through the x-axis. Moreover, the modulus $|z|$ of a complex number is precisely its distance from the origin $(0,0)$, and $|z-w|$ is the distance between the points $z=(x,y)$ and $w=(u,v)$ in the plane. Complex multiplication can also be interpreted geometrically in the plane: If ϕ denotes the angle that the vector representing $z=(x,y)$ forms with the x-axis, and, likewise, ψ denotes the angle that the vector representing $w=(u,v)$ forms with the x-axis, then zw is the vector of length $|zw|$ that forms the angle $\phi+\psi$ with the x-axis (we will better understand this geometrical interpretation of complex multiplication later (see Def. and Rem. 8.29), when writing complex numbers in the polar form $z = x+iy = |z|\exp(i\phi)$, making use of the exponential function exp).

5.3 Sums and Products

Here we compile some important rules involving sums and products of complex numbers (the exceptions are the estimates in Th. 5.13(d),(e) below, which actually require real numbers):

Theorem 5.13. (a) *For each $n \in \mathbb{N}$ and each $\lambda, \mu, z_j, w_j \in \mathbb{C}$, $j \in \{1,\ldots,n\}$:*

$$\sum_{j=1}^{n} (\lambda\, z_j + \mu\, w_j) = \lambda \sum_{j=1}^{n} z_j + \mu \sum_{j=1}^{n} w_j.$$

(b) *For each $n \in \mathbb{N}_0$ and each $z \in \mathbb{C}$:*

$$(1-z)(1+z+z^2+\cdots+z^n) = (1-z)\sum_{j=0}^{n} z^j = 1-z^{n+1}.$$

(c) *For each $n \in \mathbb{N}_0$ and each $z, w \in \mathbb{C}$:*

$$w^{n+1} - z^{n+1} = (w - z) \sum_{j=0}^{n} z^j \, w^{n-j} = (w - z)(w^n + zw^{n-1} + \cdots + z^{n-1}w + z^n).$$

(d) *For each $n \in \mathbb{N}$ and each $x_j, y_j \in \mathbb{R}$, $j \in \{1, \ldots, n\}$:*

$$\left(\forall_{j \in \{1,\ldots,n\}} \, x_j \leq y_j \right) \quad \Rightarrow \quad \sum_{j=1}^{n} x_j \leq \sum_{j=1}^{n} y_j,$$

where equality can only hold if $x_j = y_j$ for each $j \in \{1, \ldots, n\}$.

(e) *For each $n \in \mathbb{N}$ and each $x_j, y_j \in \mathbb{R}$, $j \in \{1, \ldots, n\}$:*

$$\left(\forall_{j \in \{1,\ldots,n\}} \, 0 < x_j \leq y_j \right) \quad \Rightarrow \quad \prod_{j=1}^{n} x_j \leq \prod_{j=1}^{n} y_j,$$

where equality can only hold if $x_j = y_j$ for each $j \in \{1, \ldots, n\}$.

(f) Triangle Inequality: *For each $n \in \mathbb{N}$ and each $z_j \in \mathbb{C}$, $j \in \{1, \ldots, n\}$:*

$$\left| \sum_{j=1}^{n} z_j \right| \leq \sum_{j=1}^{n} |z_j|.$$

Proof. In each case, the proof can be conducted by an easy induction. We carry out (c) and leave the other cases as exercises. For (c), the base case ($n = 0$) is provided by the true statement $w^{0+1} - z^{0+1} = w - z = (w - z)z^0 \, w^{0-0}$. For the induction step, one computes

$$\begin{aligned}
(w - z) \sum_{j=0}^{n+1} z^j \, w^{n+1-j} &= (w - z) \left(z^{n+1} w^0 + \sum_{j=0}^{n} z^j \, w^{n+1-j} \right) \\
&= (w - z) z^{n+1} + (w - z) \, w \sum_{j=0}^{n} z^j \, w^{n-j} \\
&\overset{\text{ind. hyp.}}{=} (w - z) \, z^{n+1} + w(w^{n+1} - z^{n+1}) = w^{n+2} - z^{n+2},
\end{aligned}$$

completing the induction. ∎

5.4 Binomial Coefficients and Binomial Theorem

The goal in this section is to expand $(z+w)^n$ into a sum. This sum involves the so-called *binomial coefficients* $\binom{n}{k}$, which are also useful in other contexts. To obtain an idea for what to expect, let us compute the cases $n = 0, 1, 2, 3$: $(z + w)^0 = 1$, $(z + w)^1 = z + w$,

$(z+w)^2 = z^2 + 2zw + w^2$, $(z+w)^3 = z^3 + 3z^2w + 3zw^2 + w^3$. One finds that the coefficients form what is known as *Pascal's triangle*, which we write for $n = 0, \ldots, 5$:

$$\begin{array}{lccccccccccc} n=0: & & & & & & 1 & & & & & \\ n=1: & & & & & 1 & & 1 & & & & \\ n=2: & & & & 1 & & 2 & & 1 & & & \\ n=3: & & & 1 & & 3 & & 3 & & 1 & & \\ n=4: & & 1 & & 4 & & 6 & & 4 & & 1 & \\ n=5: & 1 & & 5 & & 10 & & 10 & & 5 & & 1 \end{array} \tag{5.15}$$

The entries of the nth row of Pascal's triangle are denoted by $\binom{n}{0}, \ldots, \binom{n}{n}$. One also observes that one obtains each entry of the $(n+1)$st row, except the first and last entry, by adding the corresponding entries in row n to the left and to the right of the considered entry in row $n+1$. The first and last entry of each row are always set to 1. This can be summarized as

$$\underset{n\in\mathbb{N}_0}{\forall} \left(\binom{n}{0} = \binom{n}{n} = 1, \quad \binom{n+1}{k} = \binom{n}{k-1} + \binom{n}{k} \text{ for } k \in \{1, \ldots, n\} \right). \tag{5.16}$$

The following Def. 5.14 provides a different and more general definition of binomial coefficients. We will then prove in Prop. 5.15 that the binomial coefficients as defined in Def. 5.14 do, indeed, satisfy (5.16).

Definition 5.14. For each $\alpha \in \mathbb{C}$ and each $k \in \mathbb{N}_0$, we define the *binomial coefficient*

$$\binom{\alpha}{0} := 1, \quad \binom{\alpha}{k} := \prod_{j=1}^{k} \frac{\alpha + 1 - j}{j} = \frac{\alpha(\alpha-1)\cdots(\alpha-k+1)}{1 \cdot 2 \cdots k} \text{ for } k \in \mathbb{N}. \tag{5.17}$$

Proposition 5.15. (a) *For each $\alpha \in \mathbb{C}$ and each $k \in \mathbb{N}$:*

$$\binom{\alpha}{0} = 1, \quad \binom{\alpha+1}{k} = \binom{\alpha}{k-1} + \binom{\alpha}{k}. \tag{5.18}$$

(b) *For each $n \in \mathbb{N}_0$:*

$$\binom{n}{n} = 1. \tag{5.19}$$

The above statements include (5.16) *as a special case.*

Proof. (a): The first identity is part of the definition in (5.17). For the second identity, we first observe, for each $k \in \mathbb{N}$,

$$\binom{\alpha}{k} = \prod_{j=1}^{k} \frac{\alpha+1-j}{j} = \frac{\alpha+1-k}{k} \prod_{j=1}^{k-1} \frac{\alpha+1-j}{j} = \binom{\alpha}{k-1} \frac{\alpha+1-k}{k}, \tag{5.20}$$

which implies

$$\begin{aligned}\binom{\alpha}{k-1}+\binom{\alpha}{k} &= \binom{\alpha}{k-1}\left(1+\frac{\alpha+1-k}{k}\right) = \binom{\alpha}{k-1}\frac{\alpha+1}{k} \\ &= \frac{\alpha+1}{k}\prod_{j=1}^{k-1}\frac{\alpha+1-j}{j} = \prod_{j=1}^{k}\frac{\alpha+2-j}{j} = \binom{\alpha+1}{k}. \end{aligned} \tag{5.21}$$

(b): $\binom{0}{0}=1$ according to (5.17). For $n\in\mathbb{N}$, (5.19) is proved by induction. The base case ($n=1$) is provided by the true statement $\binom{1}{1}=\frac{1+1-1}{1}=1$. For the induction step, one computes

$$\binom{n+1}{n+1} = \prod_{j=1}^{n+1}\frac{n+1+1-j}{j} = \frac{n+1}{n+1}\prod_{j=1}^{n}\frac{n+1-j}{j} = \binom{n}{n} \overset{\text{ind. hyp.}}{=} 1, \tag{5.22}$$

which completes the induction. ■

Theorem 5.16 (Binomial Theorem)**.** *For each $z,w\in\mathbb{C}$ and each $n\in\mathbb{N}_0$, the following formula holds:*

$$(z+w)^n = \sum_{k=0}^{n}\binom{n}{k}z^{n-k}w^k = z^n + \binom{n}{1}z^{n-1}w + \cdots + \binom{n}{n-1}zw^{n-1} + w^n. \tag{5.23}$$

Proof. The proof is conducted via induction on n. The base case ($n=0$) is provided by the correct statement $(z+w)^0 = 1 = \binom{0}{0}z^{0-0}w^0$. For the induction step, we first observe

$$(z+w)^{n+1} = (z+w)\,(z+w)^n = z\,(z+w)^n + w\,(z+w)^n. \tag{5.24}$$

Using the induction hypothesis, we now further manipulate the two terms on the right-hand side of (5.24):

$$\begin{aligned} z\,(z+w)^n &\overset{\text{ind. hyp.}}{=} z\sum_{k=0}^{n}\binom{n}{k}z^{n-k}w^k = \sum_{k=0}^{n}\binom{n}{k}z^{n+1-k}w^k \\ &\overset{\binom{n}{n+1}=0}{=} \sum_{k=0}^{n+1}\binom{n}{k}z^{n+1-k}w^k, \end{aligned} \tag{5.25}$$

$$\begin{aligned} w\,(z+w)^n &\overset{\text{ind. hyp.}}{=} w\sum_{k=0}^{n}\binom{n}{k}z^{n-k}w^k = \sum_{k=0}^{n}\binom{n}{k}z^{n-k}w^{k+1} \\ &= \sum_{k=1}^{n+1}\binom{n}{k-1}z^{n+1-k}w^k. \end{aligned} \tag{5.26}$$

Plugging (5.25) and (5.26) into (5.24) yields

$$\begin{aligned}(z+w)^{n+1} &= \binom{n}{0} z^{n+1} w^0 + \sum_{k=1}^{n+1} \left(\binom{n}{k} + \binom{n}{k-1} \right) z^{n+1-k} w^k \\ &\overset{\text{Prop. 5.15}}{=} \binom{n+1}{0} z^{n+1} w^0 + \sum_{k=1}^{n+1} \binom{n+1}{k} z^{n+1-k} w^k \\ &= \sum_{k=0}^{n+1} \binom{n+1}{k} z^{n+1-k} w^k, \end{aligned} \tag{5.27}$$

completing the induction. ■

The binomial theorem can now be used to infer a few more rules that hold for the binomial coefficients:

Corollary 5.17. *One has the following identities:*

$$\forall_{n \in \mathbb{N}_0} \qquad \sum_{k=0}^{n} \binom{n}{k} = \binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{n} = 2^n, \tag{5.28a}$$

$$\forall_{n \in \mathbb{N}} \qquad \sum_{k=0}^{n} \binom{n}{k} (-1)^k = \binom{n}{0} - \binom{n}{1} + \binom{n}{2} - + \cdots + (-1)^n \binom{n}{n} = 0. \tag{5.28b}$$

Proof. (5.28a) is just (5.23) with $z = w = 1$; (5.28b) is just (5.23) with $z = 1$ and $w = -1$. ■

The formulas provided by the following proposition are also sometimes useful.

Proposition 5.18. (a) *For each $\alpha \in \mathbb{C}$ and each $k \in \mathbb{N}_0$:*

$$\sum_{j=0}^{k} \binom{\alpha + j}{j} = \binom{\alpha}{0} + \binom{\alpha+1}{1} + \cdots + \binom{\alpha+k}{k} = \binom{\alpha+k+1}{k}. \tag{5.29}$$

(b) *For each $n, k \in \mathbb{N}_0$ with $k \leq n$:*

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}. \tag{5.30}$$

Moreover, for $n \geq 1$, one has $\binom{n}{k} = \#\mathcal{P}_k(\{1, \ldots, n\})$, where

$$\mathcal{P}_k(A) := \big\{ B \in \mathcal{P}(A) : \#B = k \big\} \tag{5.31}$$

denotes the set of all subsets of a set A that have precisely k elements.

(c) *For each $n, k \in \mathbb{N}_0$:*

$$\sum_{j=0}^{k} \binom{n + j}{n} = \binom{n}{n} + \binom{n+1}{n} + \cdots + \binom{n+k}{n} = \binom{n+k+1}{n+1}. \tag{5.32}$$

Proof. The induction proofs of (a) and (b) are left as exercises. For (c), one computes

$$\sum_{j=0}^{k}\binom{n+j}{n} \overset{(5.30)}{=} \sum_{j=0}^{k}\frac{(n+j)!}{n!(n+j-n)!} \overset{(5.30)}{=} \sum_{j=0}^{k}\binom{n+j}{j}$$
$$\overset{(5.29)}{=} \binom{n+k+1}{k} \overset{(5.30)}{=} \frac{(n+k+1)!}{k!(n+1)!} = \binom{n+k+1}{n+1},$$

thereby establishing the case. ■

6 Polynomials

6.1 Arithmetic of $\mathbb{K}$-Valued Functions

Notation 6.1. We will write $\mathbb{K}$ in situations, where we allow $\mathbb{K}$ to be $\mathbb{R}$ or $\mathbb{C}$.

Notation 6.2. If A is any nonempty set, then one can add and multiply arbitrary functions $f, g : A \longrightarrow \mathbb{K}$, and one can define several further operations to create new functions from f and g:

$$(f+g) : A \longrightarrow \mathbb{K}, \qquad (f+g)(x) := f(x) + g(x), \tag{6.1a}$$
$$(\lambda f) : A \longrightarrow \mathbb{K}, \qquad (\lambda f)(x) := \lambda f(x) \quad \text{for each } \lambda \in \mathbb{K}, \tag{6.1b}$$
$$(fg) : A \longrightarrow \mathbb{K}, \qquad (fg)(x) := f(x)g(x), \tag{6.1c}$$
$$(f/g) : A \longrightarrow \mathbb{K}, \qquad (f/g)(x) := f(x)/g(x) \quad (\text{assuming } g(x) \neq 0), \tag{6.1d}$$
$$\operatorname{Re} f : A \longrightarrow \mathbb{R}, \qquad (\operatorname{Re} f)(x) := \operatorname{Re}(f(x)), \tag{6.1e}$$
$$\operatorname{Im} f : A \longrightarrow \mathbb{R}, \qquad (\operatorname{Im} f)(x) := \operatorname{Im}(f(x)). \tag{6.1f}$$

For $\mathbb{K} = \mathbb{R}$, we further define

$$\max(f,g) : A \longrightarrow \mathbb{R}, \qquad \max(f,g)(x) := \max\big\{f(x), g(x)\big\}, \tag{6.1g}$$
$$\min(f,g) : A \longrightarrow \mathbb{R}, \qquad \min(f,g)(x) := \min\big\{f(x), g(x)\big\}, \tag{6.1h}$$
$$f^+ : A \longrightarrow \mathbb{R}, \qquad f^+ := \max(f, 0), \tag{6.1i}$$
$$f^- : A \longrightarrow \mathbb{R}, \qquad f^- := \max(-f, 0). \tag{6.1j}$$

Finally, once again also allowing $\mathbb{K} = \mathbb{C}$,

$$|f| : A \longrightarrow \mathbb{R}, \qquad |f|(x) := |f(x)|. \tag{6.1k}$$

One calls f^+ and f^- the *positive part* and the *negative part* of f, respectively. For $\mathbb{R}$-valued functions f, we have

$$|f| = f^+ + f^-. \tag{6.1l}$$

6.2 Polynomials

Definition 6.3. Let $n \in \mathbb{N}$. Each function from $\mathbb{K}$ into $\mathbb{K}$, $x \mapsto x^n$, is called a *monomial*. A function P from $\mathbb{K}$ into $\mathbb{K}$ is called a *polynomial* if, and only if, it is a linear combination of monomials, i.e. if, and only if P has the form

$$P : \mathbb{K} \longrightarrow \mathbb{K}, \quad P(x) = \sum_{j=0}^{n} a_j x^j = a_0 + a_1 x + \cdots + a_n x^n, \quad a_j \in \mathbb{K}. \tag{6.2}$$

The a_j are called the *coefficients* of P. The largest number $d \leq n$ such that $a_d \neq 0$ is called the *degree* of P, denoted $\deg(P)$. If all coefficients are 0, then P is called the *zero polynomial*; the degree of the zero polynomial is defined as -1 (in Th. 6.6(b) below, we will see that each polynomial of degree $n \in \mathbb{N}_0$ is uniquely determined by its coefficients $a_0, \ldots, a_n$ and vice versa).

Polynomials of degree ≤ 0 are *constant*. Polynomials of degree ≤ 1 have the form $P(x) = a + bx$ and are called *affine* functions (often they are also called *linear* functions, even though this is not really correct for $a \neq 0$, since every function P that is linear (in the sense of linear algebra) must satisfy $P(0) = 0$). Polynomials of degree ≤ 2 have the form $P(x) = a + bx + cx^2$ and are called *quadratic* functions.

Each $\xi \in \mathbb{K}$ such that $P(\xi) = 0$ is called a *zero* or a *root* of P.

A *rational function* is a quotient P/Q of two polynomials P and Q.

Remark 6.4. Let $\lambda \in \mathbb{K}$ and let P, Q be polynomials. Then λP, $P+Q$, and PQ defined according to Not. 6.2 are polynomials as well. More precisely, if $\lambda = 0$ or $P \equiv 0$, then $\lambda P = 0$; if $P \equiv 0$, then $P + Q = Q$; if $Q \equiv 0$, then $P + Q = P$; if $P \equiv 0$ or $Q \equiv 0$, then $PQ = 0$. If $\lambda \neq 0$ and

$$\begin{gathered} P(x) = \sum_{j=0}^{n} a_j x^j, \quad Q(x) = \sum_{j=0}^{m} b_j x^j, \\ \text{with } \deg(P) = n \geq 0, \quad \deg(Q) = m \geq 0, \quad n \geq m \geq 0, \end{gathered} \tag{6.3}$$

then, defining $b_j := 0$ for each $j \in \{m+1, \ldots, n\}$ in case $n > m$,

$$(\lambda P)(x) = \sum_{j=0}^{n} (\lambda\, a_j)\, x^j, \qquad \deg(\lambda P) = n, \tag{6.4a}$$

$$(P+Q)(x) = \sum_{j=0}^{n} (a_j + b_j)\, x^j, \qquad \deg(P+Q) \leq n = \max\{m, n\}, \tag{6.4b}$$

$$(PQ)(x) = \sum_{j=0}^{m+n} c_j\, x^j, \qquad \deg(PQ) = m + n, \tag{6.4c}$$

where, setting $a_k := 0$ for each $k \in \{n+1, \ldots, m+n\}$ and $b_k := 0$ for each $k \in \{m+1, \ldots, m+n\}$,

$$\underset{j \in \{0,\ldots,n+m\}}{\forall} c_j = \sum_{k=0}^{j} a_k b_{j-k}. \tag{6.4d}$$

Formula (6.4c) can be proved by induction on $m = \deg(Q) \in \mathbb{N}_0$ as follows: For $m = 0$, we compute

$$(PQ)(x) = b_0 \sum_{j=0}^{n} a_j\, x^j = \sum_{j=0}^{n+0} b_0 a_j\, x^j,$$

i.e. $c_j = b_0 a_j = \sum_{k=0}^{j} a_k b_{j-k}$, which establishes the base case, remembering $b_{j-k} = 0$ for $j > k$. For the induction step, we compute, for $\deg(Q) = m + 1$,

$$\begin{aligned}
(PQ)(x) &= \sum_{j=0}^{n} a_j\, x^j \sum_{\alpha=0}^{m+1} b_\alpha\, x^\alpha = \sum_{j=0}^{n} a_j\, x^j \left(b_{m+1} x^{m+1} + \sum_{\alpha=0}^{m} b_\alpha\, x^\alpha \right) \\
&\overset{\text{ind. hyp.}}{=} \sum_{j=0}^{n} a_j b_{m+1}\, x^{m+1+j} + \sum_{j=0}^{m+n} \left(\sum_{k=0}^{j} a_k b_{j-k} \right) x^j \\
&= \sum_{j=m+1}^{m+n+1} a_{j-m-1} b_{m+1}\, x^j + \sum_{j=0}^{m+n} \left(\sum_{k=0}^{j} a_k b_{j-k} \right) x^j \\
&= \sum_{j=0}^{m+n+1} \left(\sum_{k=0}^{j} a_k b_{j-k} \right) x^j,
\end{aligned}$$

which completes the induction step. There is a notational issue in the second and third line in of the above computation, since, in both lines, the b_{m+1} in the first sum is the actual b_{m+1} from Q, but $b_{m+1} = 0$ in the second sum in both lines, which is due to the induction hypothesis being applied for $m < m+1$. This is actually used when combining both sums in the last step, computing, for $m+1 \le j \le m+n$: $a_{j-m-1} b_{m+1}\, x^j + a_{j-m-1} \cdot 0 \cdot x^j = a_{j-m-1} b_{m+1}\, x^j$. For $j = m+n+1$, one has $\sum_{k=0}^{m+n+1} a_k b_{m+n+1-k} = a_n b_{m+1}$, since $b_{m+n+1-k} = 0$ for $n > k$ and $a_k = 0$ for $k > n$.

Finally, $\deg(PQ) = m + n$ follows from $c_{m+n} = a_m b_n \neq 0$.

Theorem 6.5. (a) *For each polynomial P given in the form of* (6.3) *and each $\xi \in \mathbb{K}$, we have the identity*

$$P(x) = \sum_{j=0}^{n} b_j\, (x - \xi)^j, \tag{6.5}$$

where

$$\underset{j \in \{0,\dots,n\}}{\forall} b_j = \sum_{k=j}^{n} a_k \binom{k}{j} \xi^{k-j}, \quad \textit{in particular} \quad b_0 = P(\xi), \quad b_n = a_n. \tag{6.6}$$

(b) *If P is a polynomial with $n := \deg(P) \ge 1$, then, for each $\xi \in \mathbb{K}$, there exists a polynomial Q with $\deg(Q) = n - 1$ such that*

$$P(x) = P(\xi) + (x - \xi)\, Q(x). \tag{6.7}$$

In particular, if ξ is a zero of P, then $P(x) = (x - \xi)\, Q(x)$.

Proof. (a): For $\xi = 0$, there is nothing to prove. For $\xi \neq 0$, defining the auxiliary variable $\eta := x - \xi$, we obtain $x = \xi + \eta$ and

$$P(x) = \sum_{k=0}^{n} a_k(\xi+\eta)^k \overset{(5.23)}{=} \sum_{k=0}^{n}\sum_{j=0}^{k} a_k \binom{k}{j} \xi^{k-j}\eta^j = \sum_{k=0}^{n}\sum_{j=0}^{n} a_k \binom{k}{j} \xi^{k-j}\eta^j$$
$$= \sum_{j=0}^{n}\sum_{k=0}^{n} a_k \binom{k}{j} \xi^{k-j}\eta^j = \sum_{j=0}^{n}\sum_{k=j}^{n} a_k \binom{k}{j} \xi^{k-j}\eta^j, \tag{6.8}$$

which is (6.5).

(b): According to (a), we have

$$P(x) = P(\xi) + (x-\xi)\, Q(x), \quad \text{with} \quad Q(x) = \sum_{j=1}^{n} b_j\,(x-\xi)^{j-1} = \sum_{j=0}^{n-1} b_{j+1}\,(x-\xi)^j, \tag{6.9}$$

proving (b). ■

Theorem 6.6. (a) *If P is a polynomial with $n := \deg(P) \geq 0$, then P has at most n zeros.*

(b) *Let P, Q be polynomials as in (6.3) with $n = m$, $\deg(P) \leq n$, and $\deg(Q) \leq n$. If $P(x_j) = Q(x_j)$ at $n+1$ distinct points $x_0, x_1, \ldots, x_n \in \mathbb{K}$, then $a_j = b_j$ for each $j \in \{0, \ldots, n\}$.*

Consequence 1: If P, Q with degree $\leq n$ agree at $n+1$ distinct points, then $P = Q$.

Consequence 2: If we know $P = Q$, then they agree everywhere, in particular at $\max\{\deg(P), \deg(Q)\} + 1$ distinct points, which implies they have the same coefficients.

Proof. (a): For $n = 0$, P is constant, but not the zero polynomial, i.e. $P \equiv a_0 \neq 0$ with no zeros as claimed. For $n \in \mathbb{N}$, the proof is conducted by induction. The base case ($n = 1$) is provided by the observation that $\deg(P) = 1$ implies P is the affine function with $P(x) = a_0 + a_1 x$, $a_1 \neq 0$, i.e. P has precisely one zero at $\xi = -a_0/a_1$. For the induction step, assume $\deg(P) = n + 1$. If P has no zeros, then the assertion of (a) holds true. Otherwise, P has at least one zero $\xi \in \mathbb{K}$, and, according to Th. 6.5(b), there exists a polynomial Q such that $\deg(Q) = n$ and

$$P(x) = (x - \xi)\, Q(x). \tag{6.10}$$

From the induction hypothesis, we gather that Q has at most n zeros, i.e. (6.10) implies P has at most $n + 1$ zeros, which completes the induction.

(b): If $P(x_j) = Q(x_j)$ at $n+1$ distinct points x_j, then each of these points is a zero of $P - Q$. Thus $P - Q$ is a polynomial of degree $\leq n$ with at least $n + 1$ zeros. Then (a) implies $\deg(P - Q) = -1$, i.e. $P - Q$ is the zero polynomial, i.e. $a_j - b_j = 0$ for each $j \in \{0, \ldots, n\}$. ■

Remark 6.7. Let P be a polynomial with $n := \deg(P) \geq 0$. According to Th. 6.6(a), P has at most n zeros. Using Th. 6.5(b) for an induction shows there exists $k \in \{0, \dots, n\}$ and a polynomial Q of degree $n - k$ such that

$$P(x) = Q(x) \prod_{j=1}^{k} (x - \xi_j) = (x - \xi_1)(x - \xi_2) \cdots (x - \xi_k) Q(x), \tag{6.11a}$$

where Q does not have any zeros in $\mathbb{K}$ and $\{\xi_1, \dots, \xi_k\} = \{\xi \in \mathbb{K} : P(\xi) = 0\}$ is the set of zeros of P. It can of course happen that P does not have any zeros and $P = Q$ (no ξ_j exist). It can also occur that some of the ξ_j in (6.11a) are identical. Thus, we can rewrite (6.11a) as

$$P(x) = Q(x) \prod_{j=1}^{l} (x - \lambda_j)^{m_j} = (x - \lambda_1)^{m_1} (x - \lambda_2)^{m_2} \cdots (x - \lambda_l)^{m_l} Q(x), \tag{6.11b}$$

where $\lambda_1, \dots, \lambda_l$, $l \in \{0, \dots, k\}$, are the *distinct* zeros of P, and $m_j \in \mathbb{N}$ with $\sum_{j=1}^{l} m_j = k$. Then m_j is called the *multiplicity* of the zero λ_j of P.

References

[EFT07] H.-D. Ebbinghaus, J. Flum, and W. Thomas. *Einführung in die mathematische Logik*, 5th ed. Spektrum Akademischer Verlag, Heidelberg, 2007 (German).

[Kun12] Kenneth Kunen. *The Foundations of Mathematics*. Studies in Logic, Vol. 19, College Publications, London, 2012.

[Phi16] P. Philip. *Analysis I: Calculus of One Real Variable*. Lecture Notes, Ludwig-Maximilians-Universität, Germany, 2015/2016, available in PDF format at `http://www.math.lmu.de/~philip/publications/lectureNotes/philipPeter_Analysis1.pdf`.

[Wal02] Wolfgang Walter. *Analysis 2*, 5th ed. Springer-Verlag, Berlin, 2002 (German).