INTRODUCTION TO MATHEMATICS

UNIVERSITY OF TWENTE.

With contributions from:
Harry Aarts, Ed Brinksma, Jasper de Jong, Stefano Piceghello, Jan Willem Polderman, Gerhard Post, Marc Uetz, Marjan van der Velde

Version 2 — July 2023

CONTENTS

INTRODUCTION

This reader is meant as a support to an introductory course on elementary mathematical and logical tools for the bachelor degree programmes in science and engineering. It presents basic concepts and considerations regarding sets, logical statements and combinatorial reasoning. As such, it provides the basis for the treatment of more advanced mathematical topics that are relevant for science and engineering, such as calculus, linear algebra and probability.

Being the introductory course to mathematics, it is natural that this course should also play an important role as an exercise in logical and mathematical construction and reasoning, or, in even broader terms, an exercise in precise and disciplined thinking. It is clear that the latter is of great importance to the working scientist and engineer, and should also be part of any science related academic programme.

In this context it is worthwhile to spend some words on the general role of mathematics in science and engineering. Mathematics is an important language for the precise statements of scientific facts, especially those involving ordering, quantities, probabilities, geometric properties, etc. Consider the following probabilistic statement: *the probability that out of 23 random persons, 2 have the same birthday is larger than 50%*. Yet, if you happen to enter regularly a doctor's waiting room with every time 22 other patients waiting, you will find that the chance that someone of them shares *your* birthday is only around 6%. To understand this difference, you will need the tools to see that there are many more ways to pick 2 persons out of 23, than to pick 1 person out of 22, and you will need to understand how the difference affects the probabilities involved.

Mathematics is not only a language for making statements precise; it is also an important modelling tool. Scientific theories are often formulated as mathematical theories, so that we can use mathematical tools to study their properties, e.g. by proving things about them, or by simulating them in a computer program. A very important property of mathematical theories is that they guarantee *logical consistency*, i.e. that the theory is contradiction free. To get a feeling for this consider the case of the *Barber's paradox*: in a particular village there lives a barber who shaves only all men living in the village who do not shave themselves. It follows that if the barber shaves himself, he must be someone who does not shave himself. If, on the other hand, the barber does not shave himself, he is someone not shaving himself, and must therefore be shaved by the barber, i.e. by himself! It is clear that such a barber cannot exist, and he had better not be an essential element in some scientific theory.

Another important feature of mathematics is its abstract formulation, which only takes into consideration those aspects of a problem that are mathematically relevant. We will try to prove the following statement: *Among all people with a Facebook profile, there are at least two with the same number of friends*.

We formalize and prove this as follows: enumerate (in any order) the Facebook profiles from 1 to n, where n is the total number of Facebook profiles. Let $f(i)$ be the number of friends of profile i. For example, if the profile number 100 has 524 friends, we will write $f(100) = 524$. Note that, for any profile i, it must necessarily be that $0 \leq f(i) \leq n-1$, because any profile can have any number of friends from 0 to the total number of Facebook profiles, excluding itself. Now suppose there exists a particular profile, say j, with no friends, i.e. $f(j) = 0$. Because j will not appear in anyone's profile, the maximal number of friends one can have is $n - 2$ (any of the n profiles, excluding oneself and the j-th profile). Therefore, we have $0 \leq f(i) \leq n - 2$ for all i. So, if we pick n numbers $f(i)$ from $n - 1$ different values $0, \ldots, n - 2$, we get that two of these numbers must be the same (this is known as the "pigeonhole principle"). If, on the other hand, there is no j with $f(j) = 0$, again we must pick n numbers $f(i)$ from $n - 1$ values, this time ranging from 1 to $n - 1$ (since having 0 friends is no longer an option). Therefore, again, two of these numbers must be the same.

An interesting thing about the mathematical proof above is that it reasons in terms of properties of a *function* f, which itself has nothing to do with Facebook profiles. In fact, we only use that $0 \leq f(i) \leq n - 1$ where $1 \leq i \leq n$, and that if for some j we have that $f(j) = 0$ then the maximal value of $f(i)$ for any i must be $n-2$. If we look more closely at the concrete problem, we see that this is because it is a property of friendship that you can only be a friend of somebody, if they in turn are your friend (this is called a *symmetric* property). From these observations, it follows that we can apply our proof to many similar other situations to get interesting results. For example, that at any party there are two people that shake hands with the same number of people. Or, that at the University of Twente there are always two students who have the same number of fellow students living in their house. This example shows that the abstraction of mathematics can lead to a greater generality of the results that are obtained. Solutions to particular problems can often be transferred to a whole class of similar situations, which lends wider applicability and effectiveness to mathematical theories, and the science that builds on them.

Summarizing, one can say that mathematics is a language and tool for science and engineering that enables precise and consistent formulations of scientific statements, and offers powerful tools for modeling analysis, whose effectiveness is closely related to its abstract nature and the generality of its applications. As all languages, it is best learned by trying to speak it a lot. This course offers the first exercises for learning to speak mathematics at an academic level and become acquainted with its grammar, its culture and its mysteries.

1 BASIC SET THEORY AND LOGIC

1.1 Basic set theory

No one shall expel us from the Paradise that Cantor has created.
David Hilbert

1.1.1 Definitions and notations of sets

Sets are one of the building blocks of mathematics. The reason we study them is that this concept provides the underlying structure for a concise formulation of the mathematical theory formulated.

Definition 1.1.1 (Set)**.** A *set* is a well-defined, unordered collection of distinct elements.

In Definition 1.1.1, "*well-defined*" means that the conditions that an element has to satisfy in order to be a member of a set are unambiguous. For example, Ireland is part of the set of European countries, but Canada is not. However, we cannot construct a set of good soccer players since people disagree whether Harry Maguire should be an element of that set. Another example is the set of dark colours: does green belong to it, or not?
One way to describe a set is to write down its elements, separated by commas, and enclose this sequence with curly brackets. For example: the set with elements 1, 3 and 4 is written as

$$\{1, 3, 4\}.$$

A set is *unordered*, which means that we can display the elements in any order we like. Two sets are equal if they have the same elements; we denote equality between sets with the well-known symbol $=$, and inequality with $\neq$. For example, $\{1, 3, 4\} = \{4, 1, 3\}$ because the two sets have the same elements, but $\{1, 3, 4\} \neq \{1, 3\}$.
We use the equality symbol also when we want to give a set a name, for which we often use capital letters: we will write, for example,

$$A = \{1, 3, 4\}, \qquad B = \{1, 4, 3\}, \qquad C = \{1, 3\} \qquad A = B, \qquad A \neq C.$$

If an object x is an element of a set A, we write:

$$x \in A.$$

If it is not, then $x \notin A$. Thus, in the example before, $3 \in A$ and $5 \notin A$.
When defining a set, we may come across duplicates. For example, we can write down the ages of our family members and end up with the list 72, 75, 40, 45, 5, 5, 7. The corresponding set of ages will then include the age 5 only once; a set consists of *distinct* elements. Since we can order the elements of the set in any way we like, we can write it down increasingly and write the set of ages as

$$A = \{5, 7, 40, 45, 72, 75\}.$$

In the examples above, all elements are specified individually. If a set is very large, specifying all its elements may get impractical – or even impossible, if we consider sets with infinitely many elements. Consider for example the set of all positive even numbers: since there are infinitely many positive even numbers, we should come up with another notation. One possibility is to write down the first elements and assume the reader will know what is meant, like in

$$C = \{2, 4, 6, 8, \ldots\}.$$

A better way is to specify explicitly which numbers are elements of the set, for example

$$C = \{x \mid x \text{ is a positive, even integer}\}.$$

The vertical bar means 'such that', thus this notation in words is 'the set C consists of all numbers x such that x is a positive, even integer'.
For example, if we are interested in the numbers for which a function $f(x)$ is positive, we can write

$$D = \{x \mid f(x) > 0\}.$$

Example 1.1.2. Let the set A be given by $A = \left\{x \in \mathbb{R} \mid x^2 + x - 5 \geq 0\right\}$. Is it the case that $2 \in A$? Since $2^2 + 2 - 5 \geq 0$, we have that $2 \in A$. In contrast, $1 \notin A$ since $1^2 + 1 - 5 = -3 < 0$. ($\mathbb{R}$, the set of real numbers, is defined in Section 1.1.2.)

An element of a set need not be a number. Elements of sets can represent any kind of objects. An element of a set can also be a set itself:

$$A = \{\{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}.$$

Be careful when reasoning about sets in sets: the number 1 is not an element of A, but the set containing the element 1 is an element of A. Thus $1 \notin A$, but $\{1\} \in A$.

We can also consider a set that contains no objects at all. This is called the *empty set*.

Definition 1.1.3 (Empty Set)**.** The Empty Set, denoted by $\emptyset$ or $\{\}$, is a set without elements. That is, for every x, $x \notin \emptyset$

One should be quite precise when reasoning about the empty set, as it really contains no elements at all. Therefore, $\emptyset \neq \{\emptyset\}$, as $\emptyset \notin \emptyset$, but $\emptyset \in \{\emptyset\}$. Similarly, $\emptyset \neq \{0\}$ as $0 \notin \emptyset$, but $0 \in \{0\}$.

Example 1.1.4. To visualize the difference between $\emptyset$ and $\{\emptyset\}$, imagine the empty set as an empty, blue box. If you place this box (and just that) inside a red box, the red box will contain the blue empty box, so it won't be empty.

As mentioned before, sets can also contain infinitely many elements.

Definition 1.1.5 (Finite Set, Cardinality)**.** Let A be a set. A is said to be a *finite set* if it has a finite number n of elements (possibly, none). If this is the case, then n is called the *cardinality* of A; this is denoted by $|A| = n$. Otherwise, the set is said to be *infinite*.

Example 1.1.6. Let $A = \{1, 2, 3\}$. Then $|A| = 3$. The set $B = \{\{1, 2\}, 3, 4\}$ has cardinality 3, since the set $\{1, 2\}$ is one element in B. Furthermore, $|\emptyset| = 0$ since the empty set has no elements.

1.1.2 Sets of numbers

As we mentioned, sets need not contain just numbers. However, in mathematics, sets of numbers are often used. Some specific sets of numbers have conventional names; while we won't go much into detail on how the *numbers* themselves are formally defined, we list below a few important sets.

Definition 1.1.7 (Natural numbers, Integers, Rational numbers, Real numbers)**.**

- $\mathbb{N} = \{x \mid x \text{ is a natural number}\} = \{1, 2, 3, \ldots\}$.

  Note that some books include 0 in the set of natural numbers.
- $\mathbb{Z} = \{x \mid x \text{ is an integer}\} = \{0, 1, -1, 2, -2, 3, -3, \ldots\}$.
- $\mathbb{Q} = \{x \mid x \text{ is a rational number}\} = \left\{x \mid x = \frac{a}{b}, \text{ with } a \in \mathbb{Z}, b \in \mathbb{Z} \text{ and } b \neq 0\right\}$.

  Thus $\frac{4}{17} \in \mathbb{Q}$ and $-\frac{1}{5} \in \mathbb{Q}$.
- $\mathbb{R} = \{x \mid x \text{ is a real number}\}$.

  A *real number* can be represented by an integer a followed by a dot and a (possibly infinite) sequence of decimal digits.

  Examples are: 2 $(= 2.0000\ldots)$, $\frac{4}{3}$ $(= 1.333333\ldots)$ and π $(= 3.141592653\ldots)$.

Definition 1.1.8 (Positive, Nonnegative, Negative, Nonpositive Numbers)**.** A number x is called *positive* if $x > 0$, *nonnegative* if $x \geq 0$, *negative* if $x < 0$ and *nonpositive* if $x \leq 0$.

As the natural numbers start at 1 while the integers also have zero and negatives, we have that if $x \in \mathbb{N}$, then also $x \in \mathbb{Z}$ (in Section 1.1.6 we denote this by $\mathbb{N} \subset \mathbb{Z}$). For example, $-4 \in \mathbb{Z}$, but $-4 \notin \mathbb{N}$. Furthermore, if $x \in \mathbb{Z}$ then also $x \in \mathbb{Q}$: each $x \in \mathbb{Z}$ can be written as $\frac{x}{1}$ and thus $x \in \mathbb{Q}$. On the other hand, not all elements of $\mathbb{Q}$ are in $\mathbb{Z}$: consider for example $\frac{1}{2}$.

A relation that is somewhat more difficult to see is that for each $x \in \mathbb{Q}$ also $x \in \mathbb{R}$. The explanation is that any fraction has a decimal representation. The decimal representation of a rational number has a repetitive structure (like $\frac{1}{6} = 0.1666666666\ldots$ and $\frac{13}{7} = 1.857142857142857142\ldots$). Real numbers which are not rational are called *irrational*. So, an irrational number is a number $x \in \mathbb{R}$ with $x \notin \mathbb{Q}$. Examples of irrational numbers are π and $\sqrt{2}$. In Chapter 2 we formally prove that $\sqrt{2} \notin \mathbb{Q}$.

1.1.3 Intervals

Definition 1.1.9 (Interval)**.** An *interval* is a set of real numbers with the property that if two numbers are in the set, then all other numbers in between those two are also in the set.

So, if a certain interval contains the numbers 2 and 4, then the numbers 2.5, $\sqrt{5}$, 3.67208954 and $\frac{11}{3}$ are also in the interval. A *bounded* interval has two endpoints, which indicate what numbers are in the interval. The endpoint can be included in the interval, but it can also be excluded. If an endpoint is included, this is denoted by brackets $[$ or $]$. If it is excluded, this is denoted by brackets $($ or $)$. This leads to the following four kinds of bounded intervals (here $a \leq b$).

$$\begin{aligned}
(a, b) &= \{x \in \mathbb{R} \mid a < x < b\}, \\
[a, b) &= \{x \in \mathbb{R} \mid a \leq x < b\}, \\
(a, b] &= \{x \in \mathbb{R} \mid a < x \leq b\}, \\
[a, b] &= \{x \in \mathbb{R} \mid a \leq x \leq b\}.
\end{aligned}$$

Example 1.1.10. The set $\{x \mid 0 \leq x \leq 4\} = [0, 4]$ is an interval.

The set $\{x \mid 0 \leq x \leq 4,\ x \neq 3\}$ is not an interval.

Example 1.1.11. The set $\{x \mid 0 < x < 5\} = (0, 5)$ is an interval.

The set $\{x \mid 0 < x < 2 \text{ or } 3 < x < 5\}$ is not an interval.

Similarly, we have the following types of *unbounded* intervals (which are not bounded).

$$\begin{aligned}
[a, \infty) &= \{x \in \mathbb{R} \mid x \geq a\}, \\
(a, \infty) &= \{x \in \mathbb{R} \mid x > a\}, \\
(-\infty, b] &= \{x \in \mathbb{R} \mid x \leq b\}, \\
(-\infty, b) &= \{x \in \mathbb{R} \mid x < b\}, \\
(-\infty, \infty) &= \mathbb{R}.
\end{aligned}$$

1.1.4 Extreme values of sets of numbers

Sets of numbers – not just intervals – can also be bounded or unbounded. If there is a number u that is greater than all the elements in a set X of numbers, then we say that X is *bounded above*. Similarly, if there is a number l that is lower than all the elements in X, we say that X is *bounded below*. A set of numbers can then be bounded above, below, or on both sides, or on neither. We are often concerned with the numbers "at the edge" of a set of numbers, i.e., where the "boundary" lies. This motivates the following definition.

Definition 1.1.12 (Upper Bound, Supremum, Lower Bound, Infimum)**.** Let X be a non-empty set of numbers.

- An *upper bound* of X is any number $u \in \mathbb{R}$ such that $u \geq x$ for every $x \in X$.

  If X has upper bounds, its *smallest* upper bound is called the *supremum* of X and denoted by sup(X). "Smallest" means that sup$(X) \leq u$ for any upper bound u of X.
- A *lower bound* of X is any number $l \in \mathbb{R}$ such that $l \leq x$ for every $x \in X$.

  If X has lower bounds, its *greatest* lower bound is called the *infimum* of X and denoted by inf(X). "Greatest" means that inf$(X) \geq l$ for any lower bound l of X.

Example 1.1.13. The set $X = \{4, 5, 6\}$ has many upper bounds: some examples are 10, 8 and $\sqrt{37}$. The number 6 is also an upper bound, because it is greater than or equal to any element of X. Any number lower than 6 cannot be an upper bound of X, because it wouldn't be greater than nor equal to 6 (and $6 \in X$). Hence sup$(X) = 6$. Similarly, inf$(X) = 4$.

Example 1.1.14. The set $\mathbb{N}$ of natural numbers is bounded below; we have inf$(\mathbb{N}) = 1$. However, $\mathbb{N}$ is not bounded above, because for every $x \in \mathbb{R}$ we can find a natural number $n > x$.

Example 1.1.15. The interval $I = [3, 4)$ is bounded (above and below). We have inf$(I) = 3$ and sup$(I) = 4$.

Note that in this last example, we have inf$(I) = 3 \in I$, but sup$(I) = 4 \notin I$. Indeed, the supremum and infimum of a set, if they exist, need not be elements of the set itself. If they are, we award them specific names:

Definition 1.1.16 (Maximum, Minimum)**.** Let X be a non-empty set of numbers.

- If X is bounded above and $\sup(X) \in X$, we call this element the *maximum* of X, and denote it by $\max(X)$. If $\sup(X) \notin X$, the set has no maximum.
- If X is bounded below and $\inf(X) \in X$, we call this element the *minimum* of X, and denote it by $\min(X)$. If $\inf(X) \notin X$, the set has no minimum.

Note then that a set X may have a supremum and a maximum (if $\sup(X) \in X$), or a supremum and no maximum (if $\sup(X) \notin X$), or neither (if the set is not bounded above). Mind the definition: if a set has both a supremum and a maximum, they must coincide. So, if a set does not have a supremum, then it cannot have a maximum either. The same applies to infimum and minimum.

Example 1.1.17. Consider the set $V = \left\{\frac{1}{n} \mid n \in \mathbb{N}\right\}$. This set is bounded above, because no element in V is greater than 1; indeed $\sup(V) = 1$. Since $\sup(V) = 1 = \frac{1}{1} \in V$, we also have that V has a maximum $\max(V) = \sup(V) = 1$. The set V is also bounded below, for example, by -5, -2 and 0. One can show that $\inf(V) = 0$, since 0 is lower than any element in V, and any number greater than 0 is also greater than some number in V. However, $0 \notin V$, so V has no minimum.

Example 1.1.18. Let a and $b \in \mathbb{R}$, with $a < b$. Then the intervals

$$(a, b)\,, \quad [a, b)\,, \quad (a, b]\,, \quad [a, b]\,, \quad (a, \infty) \quad \text{and} \quad [a, \infty)$$

all share the same infimum a. Of these, the intervals $[a, b)$, $[a, b]$ and $[a, \infty)$ have a minimum (which is still a), while the other ones have no minimum.

1.1.5 Summation of the elements in a set

A *summation* is the addition of a set of numbers. For example if $A = \{1, 2, 5, 7\}$, then the summation of the elements of A is $1 + 2 + 5 + 7 = 15$. To denote this summation, we use the symbol $\sum$ and write

$$\sum_{a \in A} a.$$

In this last notation, we specify the objects to add (the values of a) on the right of the summation sign and specify which of these objects we take into account under the summation sign (the numbers a that are in the set A). In this way, we can also manipulate what we want to add. For example, if we want to double the value of each element, we write

$$\sum_{a \in A} 2a \qquad (= 2 + 4 + 10 + 14 = 30).$$

Another common way to define a summation is by making use of an index. Thus if we want to add the numbers a_1, a_2, a_3, a_4, a_5 we can write $\sum_{i=1}^{5} a_i$.

This notation should be read as follows. Start with the first value of the index which is indicated *under* the summation sign: here the index is i and its first value is 1. Substituting this value in the expression indicated *after* the summation sign gives the first number of the summation: here a_1. Now raise the index i by 1 to get the next number in the summation: here i becomes 2 and the second number in the summation is a_2. Continue this process of raising the index up to and including the value that is indicated *above* the summation sign: here the last value of the index i is 5. So

$$\sum_{i=0}^{5} a_i = a_1 + a_2 + a_3 + a_4 + a_5.$$

This last notation is very useful if the numbers we want to add satisfy a certain order.

Example 1.1.19. Let $B = \{6, 9, 12, 15, 18\}$. Then we have:

$$\sum_{b \in B} b = \sum_{i=2}^{6} 3i = 6 + 9 + 12 + 15 + 18 = 60.$$

Using indices we can manipulate the way we write summations; e.g., verify that

$$\sum_{i=1}^{6} i = \sum_{j=0}^{5} (j+1).$$

This will be a useful tool in Section 2.6.

1.1.6 Subsets

The same object – for example, a number – can be an element of more than one set: for example, $1 \in \{1, 2\}$ and $1 \in \{1, 3\}$. In Example 1.1.2, we considered a set A containing all $x \in \mathbb{R}$ that satisfy a certain condition; in this case, all elements of the set A are selected from the set $\mathbb{R}$, so they obviously belong to $\mathbb{R}$ too. In such a case, we say that A is a *subset* of $\mathbb{R}$. Below we make this definition precise.

Definition 1.1.20 (Subset)**.** Let A and B be sets. If for every $x \in A$ it also holds that $x \in B$, i.e., if every element of A is also an element of B, we say that A is a *subset* of B and denote this relation by $A \subseteq B$. If A is not a subset of B, we write $A \nsubseteq B$.

An illustration of subsets is given in Figures 1.1(a) and 1.1(b).

Example 1.1.21. Let $A = \{1, 2, 3, 4, 5, 6\}$, $B = \{2, 4, 6\}$ and $C = \{1, 2, 3, 4, 5\}$. Then $B \subseteq A$ and $C \subseteq A$. However, $A \nsubseteq B$, $A \nsubseteq C$, $B \nsubseteq C$ and $C \nsubseteq B$.

Remark 1.1.22. Recall from Section 1.1.1 that two sets A and B are *equal* if they have the same elements. This implies that if $A = B$ then $A \subseteq B$ and $B \subseteq A$. The converse also holds: if $A \subseteq B$ and $B \subseteq A$, then $A = B$. This is actually a way to show that two sets are equal.

A visualization of equality of sets is given in Figure 1.1(c).

Example 1.1.23. If $A = \{1, 2, 3\}$ and $B = \{x \mid x$ is a positive integer and $x^2 < 12\}$, then $A = B$.

Definition 1.1.24 (Proper Subset)**.** Consider two sets A and B, where every element of a set A is also an element of a set B, but there is at least one element of B that is not in A. In other words: $A \subseteq B$, and $A \neq B$. In this case we say that A is a *proper subset* of B and denote this relation by $A \subset B$.

An illustration of a proper subset is given in Figure 1.1(a).

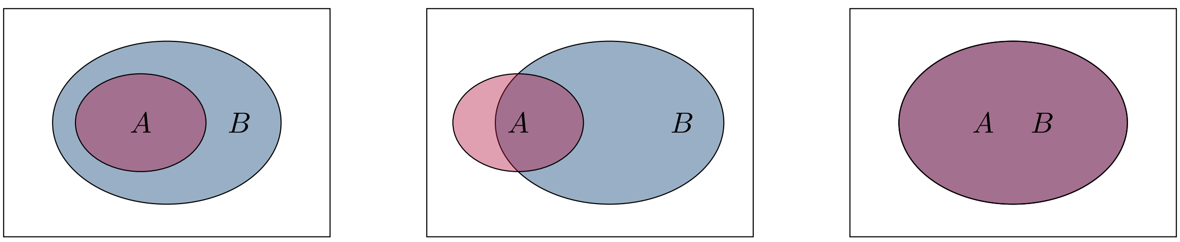
Example 1.1.25. We have that $\{1, 3\} \subset \{1, 3, 5\}$, because $\{1, 3\} \subseteq \{1, 3, 5\}$, but $5 \notin \{1, 3\}$. However, it is not the case that $\{1, 3\}$ is a proper subset of $\{1, 3\}$ itself, because $\{1, 3\}$ is evidently equal to itself.
Moreover, $\mathbb{N} \subset \mathbb{Z}$, $\mathbb{Z} \subset \mathbb{Q}$ and $\mathbb{Q} \subset \mathbb{R}$. See Section 1.1.2 for the definitions of $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ and $\mathbb{R}$.

Especially when dealing with sets that contain other sets, it is important to bear in mind that being an element of a set and being a subset of a set are two different notions. The following example illustrates the difference.

Example 1.1.26.

$$\begin{array}{rcccc}
\{2\} \in \{\{2\}, 3\}, & \text{but} & \{2\} \not\subseteq \{\{2\}, 3\} & \text{and} & \{\{2\}\} \subseteq \{\{2\}, 3\}. \\
\{2, 3\} \subseteq \{1, 2, 3\}, & \text{but} & \{2, 3\} \notin \{1, 2, 3\} & \text{and} & 2, 3 \in \{1, 2, 3\}. \\
\emptyset \subseteq \emptyset, & \text{but} & \emptyset \notin \emptyset & \text{and} & \emptyset \in \{\emptyset\}. \\
\{\emptyset\} \in \{\{\emptyset\}\}, & \text{but} & \{\emptyset\} \not\subseteq \{\{\emptyset\}\} & \text{and} & \emptyset \subseteq \{\{\emptyset\}\}.
\end{array}$$

Take some time to fully understand the examples above. The following real-life example is more concrete.



(a) A is a subset of B: $A \subseteq B$. **(b)** A is not a subset of B: $A \not\subseteq B$. **(c)** A and B are equal: $A = B$.

Figure 1.1: Venn diagrams illustrating subsets and equality of sets.

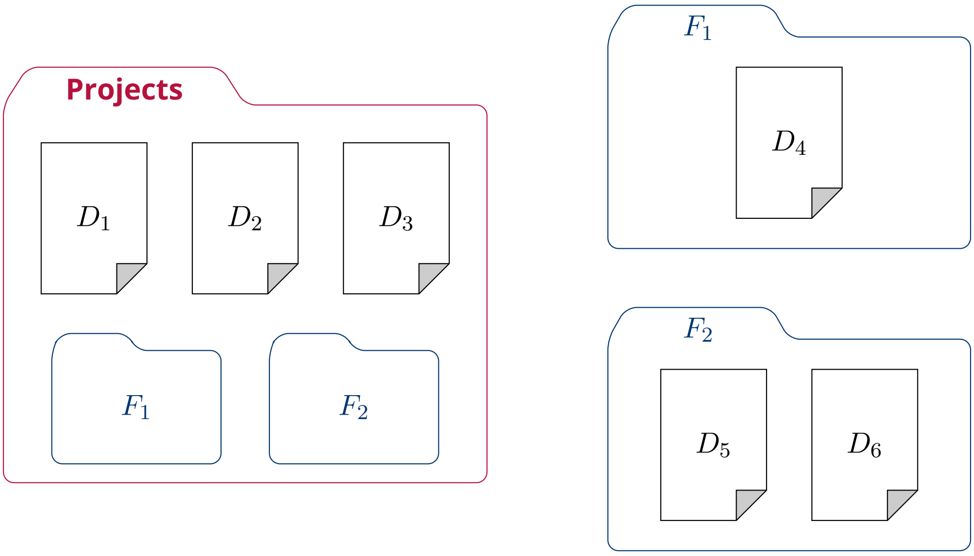


Figure 1.2: Pictures corresponding to Example 1.1.27.

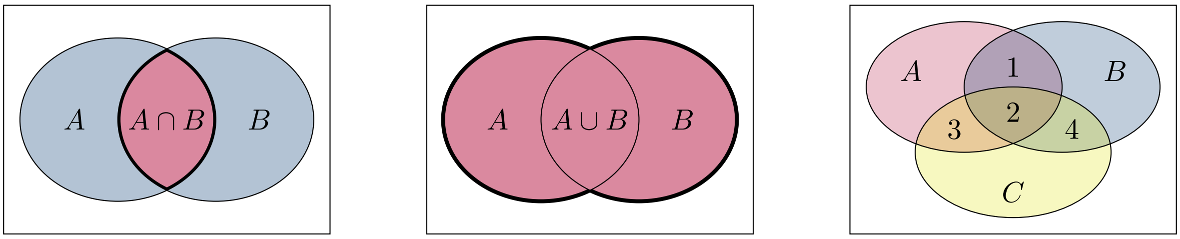
Example 1.1.27. You store your projects for a University course in your computer, in a folder named Projects. This folder contains two other folders F_1, F_2 and three documents D_1, D_2, D_3.
Thus, there is a set Projects $= \{F_1, F_2, D_1, D_2, D_3\}$. The two folders and the three documents are all *elements* of the top folder Projects, thus $F_1 \in$ Projects and $D_2 \in$ Projects.
The folders F_1 and F_2 are sets themselves: they contain other documents. Folder F_1 has only one document, D_4. Thus $F_1 = \{D_4\}$. Folder F_2 has two documents, D_5 and D_6. Therefore, $F_2 = \{D_5, D_6\}$. If we use these expressions for F_1 and F_2 in the large Projects folder, we obtain: Projects $= \{\{D_4\}, \{D_5, D_6\}, D_1, D_2, D_3\}$.
Now note that D_4 is not an element of Projects. If you want to open that document on your computer, you first have to open the folder F_1 and only then can you open the document D_4. Therefore the folder F_1 is an element of Projects and the document D_4 is not! A visualization of this example is given in Figure 1.2.

1.1.7 Union and intersection

Now that we know what a set is, we define operations on sets.

Definition 1.1.28 (Union)**.** Let A and B be sets. The *union* of the sets A and B, denoted by $A \cup B$, is the set that contains those elements that are either in A, in B, or in both A and B.
So: $A \cup B = \{x \mid x \in A \text{ or } x \in B\}$.
Note how this is *different* from $\{A, B\}$.

Definition 1.1.29 (Intersection)**.** Let A and B be sets. The *intersection* of the sets A and B, denoted by $A \cap B$, is the set that contains those elements that are both in A and B.
So: $A \cap B = \{x \mid x \in A \text{ and } x \in B\}$.



(a) The intersection of A and B. **(b)** The union of A and B. **(c)** Three sets.

Figure 1.3: Venn diagrams illustrating the union and intersection of sets.

If A and B have no elements in common, then $A \cap B = \emptyset$. In this case, we say that A and B are *disjoint*.

Example 1.1.30. Consider a mechanic who uses two boxes of tools. Then the union of the two boxes contains all tools that the mechanic can use.

Example 1.1.31. Consider the sets $A = \{1, 2, 3, 4, 5\}$ and $B = \{2, 3, 4, 6\}$.
Then $A \cup B = \{1, 2, 3, 4, 5, 6\}$ and $A \cap B = \{2, 3, 4\}$.

Example 1.1.32. Consider the intervals $A = (0, 3)$ and $B = [2, 5]$.
Then $A \cup B = (0, 5]$ and $A \cap B = [2, 3)$.

The definitions of union and intersection can be extended to more than two sets. Consider Figure 1.3(c). Here $A \cap B$ is given by the areas 1 and 2, $A \cap C$ is given by the areas 2 and 3, and $B \cap C$ is given by the areas 2 and 4. The intersection $A \cap B \cap C$ is given by area 2.

If we need to consider the union of an arbitrary number of sets, for example of the sets A_1, A_2, ..., A_{n-1}, A_n, rather than writing $A_1 \cup A_2 \cup \ldots \cup A_{n-1} \cup A_n$ we can use the notation $\bigcup_{i=1}^{n} A_i$:

$$\bigcup_{i=1}^{n} A_i = A_1 \cup A_2 \cup \ldots \cup A_{n-1} \cup A_n.$$

This can also be done for intersections: $\bigcap_{i=1}^{n} A_i$ denotes the intersection of all sets A_i:

$$\bigcap_{i=1}^{n} A_i = A_1 \cap A_2 \cap \ldots \cap A_{n-1} \cap A_n.$$

Example 1.1.33. For $k \in \{1, 2, 3, 4, 5, 6, 7\}$ the set A_k is given by $A_k = \left(\frac{1}{k}, \frac{2}{k}\right]$. Then:

$$A_5 = \left(\tfrac{1}{5}, \tfrac{2}{5}\right]; \qquad \bigcup_{k=2}^{6} A_k = \left(\tfrac{1}{6}, 1\right]; \qquad \bigcap_{k=4}^{7} A_k = \left(\tfrac{1}{4}, \tfrac{2}{7}\right]; \qquad \bigcap_{k=1}^{7} A_k = \emptyset.$$

See Figures 1.4 and 1.5 for a visualisation of the union or the intersection of more than two intervals.

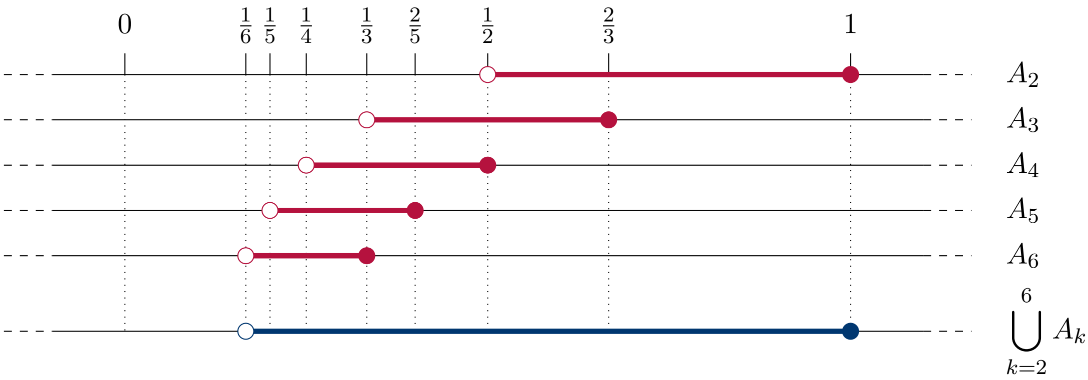


Figure 1.4: The union of more than two intervals in Example 1.1.33. A white dot means that that the point does not belong to the interval; a filled dot means that the point belongs to the interval.

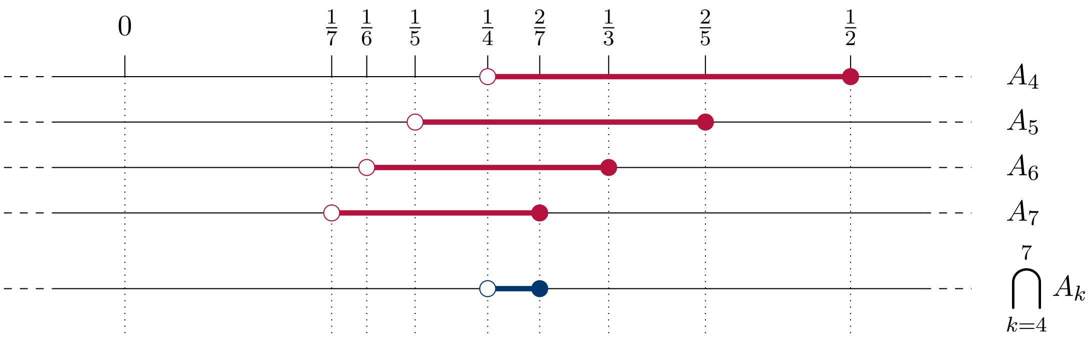
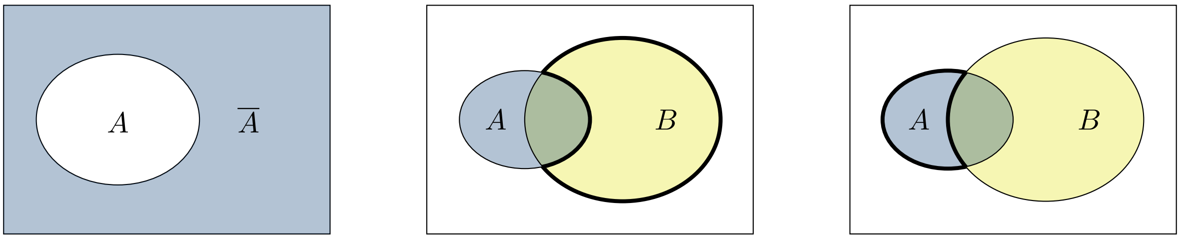


Figure 1.5: The intersection of more than two intervals, see Example 1.1.33.

1.1.8 Set difference, universal sets and complement

In the introduction we already mentioned the village where the barber shaves only those men in the village who do not shave themselves. It follows that if the barber shaves himself, he must be someone who does not shave himself. If, on the other hand, the barber, who lives in the village, does not shave himself, he must shave himself! We can conclude that in the physical world a barber with these properties cannot exist. A similar problem can arise when trying to define sets. Consider the specification $X = \{x \mid x \notin x\}$. We see that if $X \in X$, then X must fulfil the defining property of X, so $X \notin X$. If, on the other hand, $X \notin X$, then X fulfils its defining property, and therefore $X \in X$! Clearly, we have a contradiction. This problem with this definition of sets is known as "Russell's paradox".

It is obvious that, in order to have a consistent theory of sets, we cannot allow the construction of sets such as the "set" X given above. The question now is, of course, how to avoid that. Actually, this turns out to be a deep question, that kept quite some mathematicians busy at the beginning of the twentieth century. The problem is that the collection of all definable sets itself cannot be a set because it becomes, in some sense, too large. However, if for some reason we already know some large enough collection of elements, A, to be a well-behaved set, then all sets of the form $\{x \in A \mid P(x)\}$ are also well-behaved. Here $P(x)$



(a) A and its complement.

(b) The difference $B - A$ is given by the yellow area.

(c) The difference $A - B$ is given by the blue area.

Figure 1.6: Venn diagrams illustrating the complement and difference.

is some condition on the elements of A (such as the one in Example 1.1.2).

Such large enough sets of elements that hopefully will avoid problems like Russell's paradox are known as *universal sets*. In this course, we will not be concerned with how to obtain such safe, and well-behaved universal sets. In the context of this course all natural candidates for universal sets are well-behaved, or such universal sets can be safely assumed to exist.

A universal set is denoted by U. The definition of U depends on the context. In Example 1.1.30 we spoke about a mechanic and a toolbox: in this case, the universal set will denote all possible tools the mechanic could bring. In Example 1.1.31, we could consider all positive integers. Since there are many different sets that could be used as a universal set, the particular universal set being considered must always be described explicitly if the context is ambiguous.

When a universal set is given, we can define the complement of a set.

Definition 1.1.34 (Complement)**.** Let A be a set and let U be a universal set. The *complement* of A consists of all elements that are in U, but not in A. This is denoted by $\overline{A} = \{x \mid x \in U \text{ and } x \notin A\}$.

Furthermore, we define the difference of two sets.

Definition 1.1.35 (Difference)**.** Let A and B be sets. Then the *difference* $A - B$ is given by all elements that are in A, but not in B. Thus $A - B = \{x \mid x \in A, x \notin B\}$, or, equivalently, $A - B = A \cap \overline{B}$. Another notation for $A - B$ is $A \setminus B$.

Note that in particular $\overline{A} = U - A$. The complement and difference of sets are illustrated in Figure 1.6.

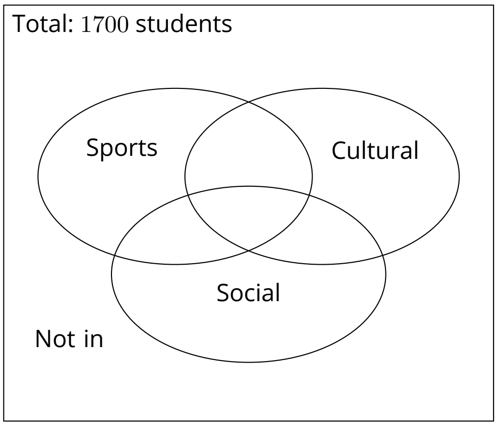
Example 1.1.36. Let $U = \{1, 2, 3, 4, 5\}$, $A = \{1, 2\}$ and $B = \{2, 3, 4\}$. Then $A - B = \{1\}$ and $B - A = \{3, 4\}$. Furthermore we have $\overline{A} = \{3, 4, 5\}$ and $\overline{B} = \{1, 5\}$.

1.1.9 Venn diagrams

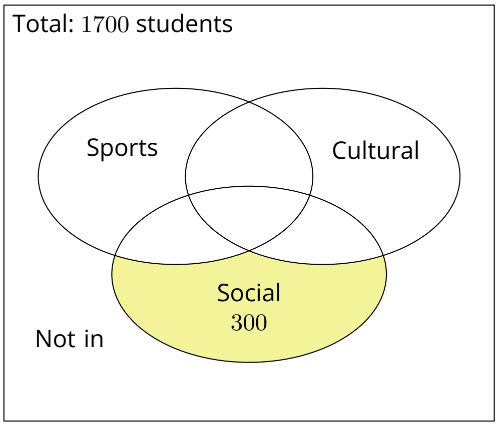
The diagrams that have been used so far to visualize sets are called *Venn diagrams*. They show relations that may exist among sets in a set-equality or a subset statement. The interior of an area represents all elements that are in that intersection of the sets involved. For example, in Figure 1.3(c) the areas 1 and 2 contain the elements of $A \cap B$, and area 3 contains the elements that are in $(A \cap C) - B$. The white area represents all elements in $\overline{A \cup B \cup C}$. Other Venn diagrams are given in Figure 1.1, Figures 1.3(a) and 1.3(b), and Figure 1.6.

These diagrams can be used to make complicated problems easier to solve. Consider the following example.

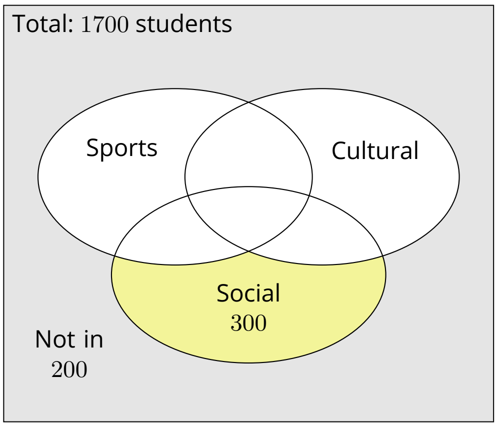
Example 1.1.37. A university has three kinds of students' clubs: sports clubs, cultural activity clubs, and social activity clubs. Of the 1700 first-year students of the university 200 do not belong to any of the university's clubs. 800 of the first-year students are members of a sports club, 300 are members of a social activity club only, 300 are members of both sports and social activity clubs, and 200 are members of both culture and social activity clubs, but not member of any sports club. How many students are members of only cultural activity clubs? We can solve this problem by making a Venn diagram and filling in the given information. This is done stepwise in Figure 1.7. Then from the last diagram we can deduce the number of students that are members only of a cultural club: $1700 - 200 - 500 - 300 - 200 - 300 = 200$ students.



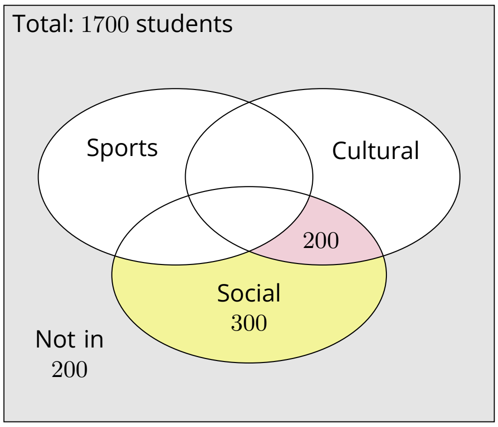
(a) The initial diagram.



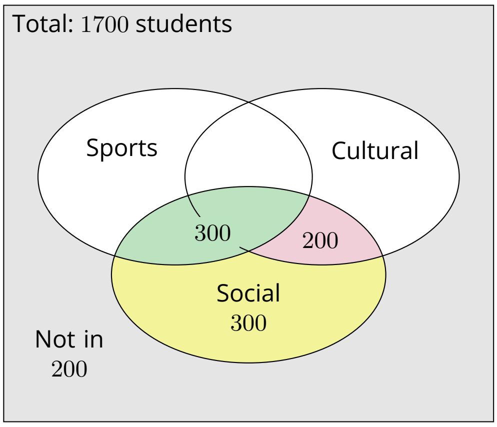
(b) 300 are only members of a social club.



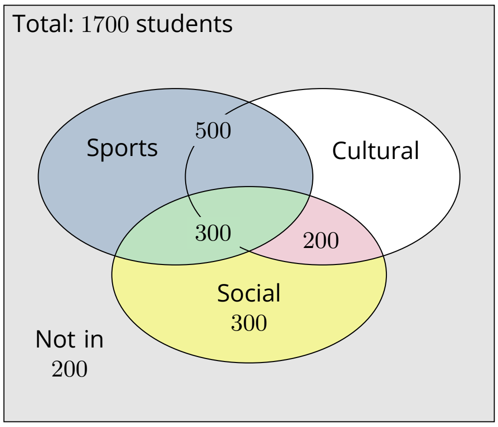
(c) 200 are not member of any club.



(d) 200 are only members of both cultural and social activity clubs.



(e) 300 are members of both sports and social clubs.



(f) $800 - 300 = 500$ are members of a sports club, but not a social club.

Figure 1.7: Venn diagrams solving the problem of Example 1.1.37.

1.2 Basic logic

Logic is the technique by which we add conviction to truth.
Jean de la Bruyère

1.2.1 Propositions and truth values

We will start this section with a definition.

Definition 1.2.1 (Proposition)**.** A *proposition* is a statement whose meaning can be given in terms of the truth values *true* and *false*.

Propositions are typically basic statements of the form "$0 < 5$", "$5 < 1$", "I own a house": an assertion that can be classified as true or false. There are several ways in which we can denote that a proposition is true or false: if it is true, we can denote that by 1 or T. If it is false, we can denote that by 0 or F.

"If the socialists win the elections, then there will be an emphasis on healthcare. If there is an emphasis on healthcare, more government money will be spent on healthcare. Thus, if the socialists win the elections, more government money will be spent on healthcare."
The above is an example of a logical statement. To write it down mathematically, we have to break this sentence up into smaller pieces and give them short names. Consider the following statements:

p : The socialists win the elections.
q : There will be an emphasis on healthcare.
r : More government money will be spent on healthcare.

All of these are propositions; each statement is either true or false, but not both. For example, "enjoy your birthday!" is not a proposition since it cannot be true or false. Furthermore, there are sentences that are propositions and yet we are not able to determine whether they are true or not. For example, "Lucille is blond" is a proposition that can only be evaluated if we know about which Lucille we are talking – since there are many people with that name. Thus in the remainder of this chapter, we will assume that we can determine whether the propositions p, q and r are true or false.

1.2.2 Propositional connectives

Propositions like p, q and r can be combined to make a new proposition. For example, we have stated that if the socialists win the elections, then there will be an emphasis on healthcare. In mathematics this is called an *implication*, and written as $p \to q$.
For the proposition $p \to q$ to be true, it is required that if p is true then q must also be true: if the socialists win the elections and indeed there is an emphasis on healthcare, then the

implication holds true. If p is false (the socialists do not win the elections), then there are no requirements on q in order for $p \to q$ to be true: this means that, if p is false, then $p \to q$ is automatically true.
The proposition $p \to q$ is false if p is true but q is false: in our example, this happens if the socialists win the elections, but there is no emphasis on healthcare.

In the same way we can encode the sentence "If there is an emphasis on healthcare, more government money will be spent on healthcare" as $q \to r$. If we know that $p \to q$ and $q \to r$ are true, we know that if p is true then q is true, and that if q is true then r is true. Thus, if p is true, then r is also true, so we have that $p \to r$ is true.

The following list contains connectives that are frequently used in logical statements.

Definition 1.2.2 (Implication, Double implication, Disjunction, Conjunction, Negation)**.**

Name		Symbol	Interpretation
Implication	("if ... then")	$\to$	$p \to q$ is true whenever it is the case that if p is true then q is true; it is false otherwise.
Double implication	("if and only if")	$\leftrightarrow$	$p \leftrightarrow q$ is true whenever it is the case that p is true if and only if q is true; it is false otherwise.
Disjunction	("or")	$\vee$	$p \vee q$ is true whenever p is true or q is true (or both are true); it is false otherwise.
Conjunction	("and")	$\wedge$	$p \wedge q$ is true whenever both p and q are true; it is false otherwise.
Negation	("not")	$\neg$	$\neg p$ is true whenever p is false; it is false whenever p is true.

Example 1.2.3. Consider the statement "If it rains today, I take my umbrella with me". If we define the propositions

p : It rains today,
q : I take my umbrella with me.

Then the statement above can be expressed by: $p \to q$.

Example 1.2.4. Consider the statement "If you have €1000 available or you are a thief, you can get an expensive TV". To write this in terms of logic, we introduce the following propositions.

p : You can get an expensive TV,
q : You have €1000 available,
r : You are a thief.

Then the statement above can be expressed by $(q \vee r) \to p$.

1.2.3 Truth tables

Propositions are either true or false. With this information, we can determine the truth value of longer expressions. For example, we can examine the expression $p \to q$ from Example 1.2.3. That states that "if it rains today, I take my umbrella with me". Now imagine that it rains, but I forgot to take my umbrella. Thus, p has truth value 1 and q has truth value 0. Then the expression $p \to q$ is false, i.e., it has truth value 0.

These arguments can become long and inconvenient, since we need many words and have to consider all possible cases. To resolve this issue, we can make use of *truth tables*. In Table 1.1, the truth values of the basic compound propositions are given.

p	q	$p \to q$	$p \leftrightarrow q$	$p \vee q$	$p \wedge q$	$\neg p$
0	0	1	1	0	0	1
0	1	1	0	1	0	1
1	0	0	0	1	0	0
1	1	1	1	1	1	0

Table 1.1: Truth table for basic compound propositions. The value 1 means that the statement is true, the value 0 means it is false.

Example 1.2.5. Let's revisit Example 1.2.3 about the rain and the umbrella. For every combination of truth values of p ("it rains today") and q ("I take my umbrella with me"), we can use Table 1.1 to determine the corresponding truth value of $p \to q$ ("if it rains today, I take my umbrella with me").

- The fourth row corresponds to both p and q being true, so it does rain and I do take my umbrella with me. From the table, we can read that $p \to q$ has truth value 1, so the statement is true.
- The third row corresponds to p being true and q being false, so it rains but I do not take my umbrella with me. In this case, $p \to q$ has truth value 0, which means that the statement "if it rains today, I take my umbrella with me" is false.
- Pay attention to the first row: p is false, so it does not rain today. For the implication to be true, we prescribe a condition on me taking my umbrella only if rains today, but since it does not rain, no condition on q is prescribed that we could ever violate. From the truth table, we see that the compound statement $p \to q$ is true.
- Similarly, the second row corresponds to p again being false, so we do not need to check the truth value of q to determine that the implication $p \to q$ is true.

Example 1.2.6. Consider the following statement: "If I win the lottery, I will quit my job". We can express this as an implication $p \to q$, with:

p : I win the lottery,
q : I will quit my job.

Assume that $p \to q$ is true. What can we say about p and q? It might be the case that I do win the lottery (p is true) and that indeed I will quit my job (q is true). If, instead, I do not win the lottery (p is false), it is irrelevant whether or not I quit my job, because the condition does not apply (for example, I could quit because I got a better offer somewhere else, or I could stay because I like my colleagues). All we can say is that if I don't quit my job (q false), then it *cannot* be the case that I've won the lottery (p true), because then my statement $p \to q$ would be false.

Truth tables can be used to determine the truth values of more complex statements (composed by several propositions and connectives). Table 1.2 shows the truth table of the statement $\neg(p \to q) \vee (\neg q \wedge r)$. Note that the table is constructed step by step (column by column), using the definitions of the propositional connectives given in Table 1.1. Be careful with the order of operations on propositions. The first operation to apply to a proposition is the negation $\neg$. After that, apply $\wedge$ and then $\vee$. Finally, the implication $\to$ is applied. Thus, $p \to q \wedge r$ is the same as $p \to (q \wedge r)$ and $\neg p \vee q$ is the same as $(\neg p) \vee q$. Often brackets are used to make sure no confusion arises. Here we make no difference between round brackets "( )" and square brackets "[ ]", but curly brackets "{ }" are not commonly used because they may cause confusion with notations in set theory.

p	q	r	$p \to q$	$\neg(p \to q)$	$\neg q$	$\neg q \wedge r$	$\neg(p \to q) \vee (\neg q \wedge r)$
0	0	0	1	0	1	0	0
0	0	1	1	0	1	1	1
0	1	0	1	0	0	0	0
0	1	1	1	0	0	0	0
1	0	0	0	1	1	0	1
1	0	1	0	1	1	1	1
1	1	0	1	0	0	0	0
1	1	1	1	0	0	0	0

Table 1.2: Truth table for $\neg(p \to q) \vee (\neg q \wedge r)$.

Truth tables can be used to establish how two (compound) statements are related, as shown in the following example.

Example 1.2.7. Suppose that you are working on a project with two fellow students. And suppose that based on experiments on an object, you construct the following hypothesis: "If we increase the oxygen level, then the object emits light". However, your fellow students have constructed the following different hypotheses respectively:

1. If the object does not emit light, then we did not increase the oxygen level.
2. If we do not increase the oxygen level, then the object emits light.

So if p is the statement "We increase the oxygen level" and q is the statement "The object emits light", then your hypothesis corresponds to $p \to q$. The hypotheses of your fellow students respectively correspond to: $\neg q \to \neg p$ and $\neg p \to q$. To be able to have a fruitful discussion on how to proceed with your project, you first need to understand how your hypotheses are related. Are they equivalent, do they contradict each other, or neither? We investigate by constructing Table 1.3.

p	q	$\neg p$	$\neg q$	$p \to q$	$\neg q \to \neg p$	$\neg p \to q$
0	0	1	1	1	1	0
0	1	1	0	1	1	1
1	0	0	1	0	0	1
1	1	0	0	1	1	1

Table 1.3: The statements $p \to q$ and $\neg q \to \neg p$ are logically equivalent.

As it turns out, the statements $p \to q$ and $\neg q \to \neg p$ have the same truth values: their columns are identical.
Moreover, observe that even though $\neg p \to q$ does not have the same truth values as the other statements, it does not contradict them. For example, when the object emits light regardless of oxygen level ($q = 1$), all three hypotheses are true.

This leads to the following definitions.

Definition 1.2.8 (Logically Equivalent)**.** Let s_1, s_2 be two propositions. We say that s_1, s_2 are logically equivalent if s_1 is true if and only if s_2 is true (which is the same as saying that s_1 is false if and only if s_2 is false). This is denoted by $s_1 \Leftrightarrow s_2$. In a truth table, the columns corresponding to logically equivalent propositions are identical.

In example 1.2.7 the statements "If we increase the oxygen level, then the object emits light" and "If the object does not emit light, then we did not increase the oxygen level" are logically equivalent, which can be observed from Table 1.3.
Another important example is the logical equivalence of the two statements $p \leftrightarrow q$ and $(p \to q) \wedge (q \to p)$, to be shown in Exercise 1.17. In words: the statement "p if and only if q" is logically equivalent to the statement "if p then q, and if q then p".

There are two more concepts that are worth a couple of words. First of all, consider a statement that is always true, no matter the values of the propositions that compose it. A trivial example of this is $p \vee \neg p$, see Table 1.4. It is called a *tautology*.

Definition 1.2.9 (Tautology)**.** A *tautology* is a statement that is always true, no matter the values of the propositions that compose it.

In a truth table, the column corresponding to a tautology consists of merely ones.
Note that if two statements s_1 and s_2 are logically equivalent (i.e. $s_1 \Leftrightarrow s_2$), then the statement $s_1 \leftrightarrow s_2$ is a tautology. This also holds the other way around: if $s_1 \leftrightarrow s_2$ is a tautology, then $s_1 \Leftrightarrow s_2$.
In example 1.2.7 the statement "(If we increase the oxygen level, then the object emits light)

is true if and only if (If the object does not emit light, then we did not increase the oxygen level)” is a tautology, as we observed from Table 1.3 that these statements are logically equivalent.

Mind the difference: $s_1 \leftrightarrow s_2$ is a proposition that might be true or false, whereas $s_1 \Leftrightarrow s_2$ indicates that the proposition $s_1 \leftrightarrow s_2$ is always true.
On the opposite, we can have a statement that is always false. This is called a *contradiction*.

Definition 1.2.10 (Contradiction)**.** A *contradiction* is a statement that is always false, no matter the values of the propositions that compose it.

An example of a contradiction is $p \wedge \neg p$. In a truth table, the column corresponding to a contradiction consists of merely zeros. This is shown in Table 1.4.

p	$\neg p$	$p \vee \neg p$	$p \wedge \neg p$
0	1	1	0
1	0	1	0

Table 1.4: The statement $p \vee \neg p$ is a tautology and $p \wedge \neg p$ is a contradiction.

If a statement is not a tautology, a truth table can be used to find values for the propositions that make the statement false: a *counterexample* for the statement.

Definition 1.2.11 (Counterexample)**.** A *counterexample* to a statement is a set of propositions that make the statement false.

For example, from the fourth row of Table 1.2 we deduce that $p = 0$, $q = 1$, $r = 1$ is a counterexample for the statement $\neg(p \to q) \vee (\neg q \wedge r)$ (because the column corresponding to the compound statement $\neg(p \to q) \vee (\neg q \wedge r)$ has a zero in the fourth row). In fact, Table 1.2 shows that there are even five counterexamples for the statement $\neg(p \to q) \vee (\neg q \wedge r)$.
In Table 1.3, we see that there is exactly one counterexample to $p \to q$, namely $p = 1, q = 0$. That is, the only way to disprove the hypothesis “If we increase the oxygen level, then the object emits light”, is to increase the oxygen level without having the object emit light.

The next example once again emphasizes the importance of the order in which the operations on propositions must be applied.

Example 1.2.12. Consider the following statement: $p \to (\neg p \to q)$. This statement means that if p is true, then if p is not true, q must be true. This is an example of a tautology: if p is true, then p cannot be not true and q may be anything because of the right implication. If p is not true, then the left implication has no effect. This is clarified with a truth table in Table 1.5. Furthermore, this example shows that the brackets need to be placed in this case: $(p \to \neg p) \to q$ is *not* a tautology.

Example 1.2.12 gives rise to the following important logical concept.

p	q	$\neg p$	$\neg p \to q$	$p \to (\neg p \to q)$	$p \to \neg p$	$(p \to \neg p) \to q$
0	0	1	0	1	1	0
0	1	1	1	1	1	1
1	0	0	1	1	0	1
1	1	0	1	1	0	1

Table 1.5: Truth table for the compound statements $p \to (\neg p \to q)$ and $(p \to \neg p) \to q$.

Definition 1.2.13. Let s_1 and s_2 be two propositions. We say that s_1 *logically implies* s_2 if the implication $s_1 \to s_2$ is a tautology. This is denoted by $s_1 \Rightarrow s_2$. Other ways to express this are "$s_1 \to s_2$ is a *logical implication*" or "s_2 *is a logical consequence of* s_1".

Again, mind the difference: $s_1 \to s_2$ is a proposition that might be true or false, whereas $s_1 \Rightarrow s_2$ indicates that the proposition $s_1 \to s_2$ is always true.

Example 1.2.14. In Example 1.2.12 and Table 1.5 we have seen that $p \to (\neg p \to q)$ is a tautology. Therefore p logically implies $\neg p \to q$, or $p \Rightarrow \neg p \to q$.

1.2.4 Membership tables

Statements about sets can be examined using truth tables. This idea is based on the strong connection between set theory and logic.

For example, if A and B are sets, the statement $A \cup B = B \cup A$ means that the sets $A \cup B$ and $B \cup A$ have the same elements. In other words: if $x \in A \cup B$ then also $x \in B \cup A$ and if $x \in B \cup A$ then also $x \in A \cup B$. Using logical connectives, we get:

$$[(x \in A \cup B) \to (x \in B \cup A)] \wedge [(x \in B \cup A) \to (x \in A \cup B)]\,,$$

or, $[(x \in A \cup B) \leftrightarrow (x \in B \cup A)]$. Furthermore, $x \in A \cup B$ means $x \in A \vee x \in B$. Therefore, the statement $A \cup B = B \cup A$ is equivalent to the statement $(x \in A \vee x \in B) \leftrightarrow (x \in B \vee x \in A)$. Table 1.6 shows that the latter statement is a tautology, and therefore the equality $A \cup B = B \cup A$ holds for all sets A and B.

$x \in A$	$x \in B$	$x \in A \vee x \in B$	$x \in B \vee x \in A$	$(x \in A \vee x \in B) \leftrightarrow (x \in B \vee x \in A)$
0	0	0	0	1
0	1	1	1	1
1	0	1	1	1
1	1	1	1	1

Table 1.6: Truth table for $(x \in A \vee x \in B) \leftrightarrow (x \in B \vee x \in A)$.

For convenience, mostly the "$x \in$"-part is often omitted in the truth table and the original set theoretic notations are used for the operators (but formally we are considering logical *statements*!). The truth table is then called a *membership table*. The membership table corresponding to the statement $A \cup B = B \cup A$ is shown in Table 1.7.

Membership tables are also used to examine statements about sets that contain other set-theoretical operators. Table 1.8 shows the correspondence between set-theoretical and logical connectives.

A	B	$A \cup B$	$B \cup A$	$A \cup B = B \cup A$
0	0	0	0	1
0	1	1	1	1
1	0	1	1	1
1	1	1	1	1

Table 1.7: Membership table for $A \cup B = B \cup A$.

Set operator	Logical connective
$x \in A \cup B$	$x \in A \vee x \in B$
$x \in A \cap B$	$x \in A \wedge x \in B$
$x \in \overline{A}$	$\neg(x \in A)$
$x \in A - B$	$x \in A \wedge \neg(x \in B)$
$A \subseteq B$	$x \in A \rightarrow x \in B$
$A = B$	$x \in A \leftrightarrow x \in B$

Table 1.8: Relation between set-theoretical operators and logical connectives.

Table 1.9 shows that the equation $\overline{A \cup B} = \overline{A} \cap \overline{B}$ holds. This equation is one of the *De Morgan laws*. Another De Morgan law is: $\overline{A \cap B} = \overline{A} \cup \overline{B}$, see Exercise 1.21(a).

A	B	$A \cup B$	$\overline{A \cup B}$	$\overline{A}$	$\overline{B}$	$\overline{A} \cap \overline{B}$	$\overline{A \cup B} = \overline{A} \cap \overline{B}$
0	0	0	1	1	1	1	1
0	1	1	0	1	0	0	1
1	0	1	0	0	1	0	1
1	1	1	0	0	0	0	1

Table 1.9: Membership table for $\overline{A \cup B} = \overline{A} \cap \overline{B}$.

Membership tables can help to find a counterexample if a statement about sets does not hold in general. Consider for example the statement $(A - C) \cup (B - C) = (A \cup B) - (B \cap C)$. Table 1.10 shows a membership table for this statement (for layout reasons, the last column corresponding to the compound statement $(A - C) \cup (B - C) = (A \cup B) - (B \cap C)$ is omitted). Since the sixth and ninth columns are not identical, the equality does not hold in general. Furthermore, to find a counterexample, we look in the table for a row in which these columns differ. In this case, the columns differ (only) in the sixth row. Looking at the first three columns in this row, we see that a counterexample can be constructed with sets A, B and C, such that there exists an element x with $x \in A$, $x \notin B$ and $x \in C$.
Take $x = 0$ and $A = \{0\}$, $B = \{1\}$ and $C = \{0\}$. Then $(A - C) \cup (B - C) = \{1\}$ and $(A \cup B) - (B \cap C) = \{0, 1\}$. So $(A - C) \cup (B - C) \neq (A \cup B) - (B \cap C)$, which is a counterexample.

A	B	C	$A-C$	$B-C$	$(A-C)\cup(B-C)$	$A\cup B$	$B\cap C$	$(A\cup B)-(B\cap C)$
0	0	0	0	0	0	0	0	0
0	0	1	0	0	0	0	0	0
0	1	0	0	1	1	1	0	1
0	1	1	0	0	0	1	1	0
1	0	0	1	0	1	1	0	1
1	0	1	0	0	0	1	0	1
1	1	0	1	1	1	1	0	1
1	1	1	0	0	0	1	1	0

Table 1.10: Membership table for $(A-C)\cup(B-C)$ and $(A\cup B)-(B\cap C)$.

Also Venn diagrams can be used to examine statements about sets (especially when there are no more than three sets involved). However, these pictures are not considered as formal mathematical proofs.

1.2.5 Predicates and quantifiers

In contrast to a proposition, a *predicate* is a statement whose truth generally cannot be determined directly, as it may contain variables whose actual values influence the truth or falsehood of the statement. Examples of predicates are "$x > 0$", "$x^3 < y$", "Mr. x owns a house", etc. To decide on the truth of predicates we must assign values to the variables, turning the predicates into propositions. E.g., assigning 1 to x and 2 to y turns $x^3 < y$ into the true proposition $1^3 < 2$. Thus, a predicate is more general than a proposition.

With the use of predicates, we can make statements about a group of propositions. For example, we can determine whether a whole group of propositions is true or not.

Example 1.2.15. Consider the set $X = \{1,2,3,4,5,6,7,8,9,10\}$. Define $p(x)$ as the predicate "$x > 5$" and $q(x)$ as "$x > 4$". Then $p(2)$ is false, $p(6)$ is true, $q(4)$ is false. Furthermore, for all $x \in X$ we have that if $p(x)$ is true, then $q(x)$ must be true: if $x > 5$ then also $x > 4$. Thus, for all $x \in X$, we have that $p(x) \to q(x)$ is true.

Each predicate has a domain, the values of x for which the proposition $p(x)$ is considered. Often we want to say something about a group of propositions. For example, we want to know if a function is always positive or not. Thus, we question whether $f(x) > 0$ for all x, or whether there is an x with $f(x) \leq 0$. This is called a *universally quantified statement*, and x is a *quantified variable*.

Definition 1.2.16 (Universal Quantifier)**.** Let $p(x)$ denote a predicate. The statement $\forall x\,(p(x))$ is true when $p(x)$ is true for all x from some specified domain. The symbol that represents "for all x" is $\forall x$.
If the domain D of the quantified variable x is not clear from the context, we can also use the notation $\forall x \in D\ (p(x))$.

Example 1.2.17. Consider, for the domain $\mathbb{R}$, the proposition

$$\forall x \ \left(x^2 \geq 0\right).$$

In words, this means "for all $x \in \mathbb{R}$, we have that $x^2 \geq 0$". This proposition is true: there is no real x such that $x^2 < 0$.
The same statement could also be written as $\forall x \in \mathbb{R} \ \left(x^2 > 0\right)$, making the domain of x explicit.

Example 1.2.18. Consider the predicate "$x^2 \geq 0$". We want to know whether this is true for all $x \in \mathbb{R}$. Thus, we question whether the following proposition is true or false:

$$\forall x \in \mathbb{R} \ \left(x^2 - 1 > 0\right).$$

This proposition is not true, since we can find an $x \in \mathbb{R}$ for which $x^2 - 1 > 0$ is not true; e.g., consider the value $x = 0$. Then the proposition $0^2 - 1 > 0$ is false, so $x^2 - 1 > 0$ is not true for all $x \in \mathbb{R}$.

Note that in this last example we made use of the fact that we needed only one x for which $x^2 - 1 > 0$ was false to conclude that the proposition $\forall x \, (x^2 - 1 > 0)$ was false. This is a counterexample, which is often used in mathematics to show that a theorem is not true in general. Counterexamples are treated in more detail in Section 2.2.

A related notion is the *existentially quantified statement*.

Definition 1.2.19 (Existential Quantifier)**.** Let $p(x)$ denote a predicate. The statement $\exists x \, (p(x))$ is true when $p(x)$ is true for at least one x from some specified domain. The symbol that represents "there exists an x" is $\exists x$.

Example 1.2.20. Consider the following proposition, with the domain $\mathbb{R}$,

$$\exists x \ \left(\tfrac{x}{x^2+1} = \tfrac{2}{5}\right).$$

This proposition is true since we can find at least one real number x for which $\frac{x}{x^2+1} = \frac{2}{5}$ is true. For example, taking $x = 2$, we obtain the true proposition $\frac{x}{x^2+1} = \frac{2}{5}$.
Note that not every value of x makes $\frac{x}{x^2+1} = \frac{2}{5}$ a true proposition. For example, $x = 1$ yields $\frac{1}{2} = \frac{2}{5}$, which is false. However, it suffices to find one x that makes the proposition true. There can be thousands of x which give a true proposition, however we need only one value to make $\exists x \, p(x)$ true.

Example 1.2.21. Consider the following predicates with the domain $\mathbb{R}$.

$p(x): \quad x^3 - 2x^2 + x = 2,$
$q(x): \quad x^2 - 4 = 0.$

Now consider the following proposition: $\exists x\,(p(x) \wedge q(x))$. We want to know whether there exists at least one x for which both $x^3 - 2x^2 + x = 2$ and $x^2 - 4 = 0$ are true. For $x = 2$, both equalities are true. Thus we have found one x, hence $\exists x\,(p(x) \wedge q(x))$ is true.

With the use of quantifiers we can describe statements about sets using logical symbols, called *quantified statements*.

Example 1.2.22. Let A and B be sets.
The statement $A \subseteq B$ can be formulated as: $\forall x\,(x \in A \rightarrow x \in B)$.
The statement $A = B$ can be formulated as: $\forall x\,(x \in A \leftrightarrow x \in B)$.
The statement $A \subset B$ can be formulated as: $\forall x\,(x \in A \rightarrow x \in B) \wedge \exists x\,(x \in B \wedge \neg(x \in A))$.

The connection between the universal quantifier $\forall$ and the existential quantifier $\exists$ is given in the following theorem.

Theorem 1.2.23. If $p(x)$ is a predicate, the propositions in (a) are equivalent (i.e., either both are true or both are false) and the propositions in (b) are equivalent.

(a) $\neg(\forall x\, p(x))$ and $\exists x\,(\neg p(x))$.

(b) $\neg(\exists x\, p(x))$ and $\forall x\,(\neg p(x))$.

Thus if we want to show that $p(x)$ is true for all x, we can also show that there is no value for x for which $p(x)$ is false. Conversely, if we want to show that there is no value for x for which $p(x)$ is false, we can also show that $p(x)$ is true for all x.

1.3 Exercises

Set theory

Exercise 1.1. Which of the following sets are equal?

a) $\{1,2,3\}$ b) $\{1,\{2,3\}\}$ c) $\{1,2,3,2\}$

Exercise 1.2. Determine all the elements in each of the following sets:

a) $A=\{1+(-1)^n \mid n\in\mathbb{N}\}$ b) $A=\left\{n+\frac{1}{n} \mid n\in\{1,2,3,5,7\}\right\}$

c) $A=\left\{n^3+n^2 \mid n\in\{0,1,2,3,4\}\right\}$

Exercise 1.3. Give an example of sets X, Y, and Z such that $X\in Y$, $Y\in Z$, but $X\notin Z$.

Exercise 1.4. Let $A=\{1,\{1\},\{2\}\}$. Which of the following statements are true?

a) $1\in A$ b) $\{1\}\in A$ c) $\{1\}\subseteq A$ d) $\{\{1\}\}\subseteq A$

e) $\{2\}\in A$ f) $\{2\}\subseteq A$ g) $\{\{2\}\}\subseteq A$

Exercise 1.5. Determine for each of the following sets whether they are intervals or not. If they are, give their interval notation. If they are not, explain why.

a) $\{x \mid 0<x<5\}$ b) $\{x \mid 4\leq x<6\}$

c) $\{x \mid 0<x<3\}\cup\{x \mid 4\leq x<6\}$ d) $\{x \mid 0<x<6\}\cap\{x \mid 4\leq x<8\}$

Exercise 1.6. Determine for each of the following sets the minimum, maximum, infimum and supremum, if they exist.

a) $[2,3]$ b) $(2,3]$ c) $\mathbb{Z}$

d) $\left\{\frac{n}{n+1} \mid n\in\mathbb{N}\right\}$ e) $\{1+(-1)^n \mid n\in\mathbb{N}\}$ f) $\left\{\frac{1}{x} \mid x\in(0,\infty)\right\}$

Exercise 1.7. Evaluate the following summations:

a) $\displaystyle\sum_{i=1}^{3} i$ b) $\displaystyle\sum_{i=1}^{3}(2i+3)$ c) $\displaystyle\sum_{k=0}^{1000} 1$ d) $\displaystyle\sum_{k=0}^{1000}(-1)^k$

Exercise 1.8. For $U=\{1,2,3,\ldots,9,10\}$ let $A=\{1,2,3,4,5\}$, $B=\{1,2,4,8\}$, $C=\{1,2,3,5,7\}$, and $D=\{2,4,6,8\}$. Determine each of the following:

a) $(A\cup B)\cap C$ b) $\overline{C}\cup\overline{D}$ c) $A\cup(B\cap C)$

d) $\overline{C\cap D}$ e) $(A\cup B)-C$ f) $A\cup(B-C)$

g) $(B-C)-D$ h) $B-(C-D)$

Exercise 1.9. Let A, B, C, $D \subseteq \mathbb{Z}$ be defined as follows:

$$A = \{2n \mid n \in \mathbb{Z}\}, \quad B = \{3n \mid n \in \mathbb{Z}\}, \quad C = \{4n \mid n \in \mathbb{Z}\}, \quad \text{and} \quad D = \{6n \mid n \in \mathbb{Z}\}.$$

Which of the following statements are true?

a) $C \subseteq A$ b) $A \subseteq C$ c) $B \subseteq D$ d) $D \subseteq B$
e) $D \subseteq A$ f) $\overline{D} \subseteq \overline{A}$

Exercise 1.10. For the sets in Exercise 1.9, determine the following sets.

a) $B \cup D$ b) $A \cap B$ c) $B \cap C$ d) $A \cup B$

Exercise 1.11. Let A, B, C, D, E, $F \subseteq \mathbb{Z}$ be defined as follows:

$$A = \{2m - 1 \mid m \in \mathbb{Z}\}, \qquad B = \{2n + 3 \mid n \in \mathbb{Z}\}, \qquad C = \{2p - 3 \mid p \in \mathbb{Z}\},$$
$$D = \{3r + 1 \mid r \in \mathbb{Z}\}, \qquad E = \{3s + 2 \mid s \in \mathbb{Z}\}, \qquad F = \{3t - 2 \mid t \in \mathbb{Z}\}.$$

Which of the following statements are true?

a) $A = B$ b) $A = C$ c) $B = C$ d) $D = E$
e) $D = F$ f) $E = F$

Exercise 1.12. Let, for $i \in \{1, 2, 3, \ldots, 10\}$, the intervals A_i be given by $A_i = [i, 10i)$. Determine the following sets:

a) A_7 b) $\bigcup_{i=3}^{7} A_i$ c) $\bigcap_{i=3}^{7} A_i$ d) $\bigcup_{i=1}^{10} A_i$ e) $\bigcap_{i=1}^{10} A_i$

Exercise 1.13. Consider a group of 100 students. There are three courses they can take: history, English and mathematics. 20 students like books so take all three courses. 10 however prefer to drink beer all day so do no course at all. 10 students find mathematics interesting though difficult, so take it as their only course. 25 students take English, but not history. On the opposite, 15 students take history, but not English. Use a Venn diagram to determine how many students take both the history and English courses, but not mathematics.

Logic

Exercise 1.14. Let p, q, r and s denote the following statements:

p : I finish my assignment before lunch.
q : I play tennis in the afternoon.
r : The sun is shining.
s : The humidity is low.

Write the following compound statements in symbolic form:

a) If the sun is shining, I play tennis in the afternoon.
b) Finishing my assignment before lunch is necessary for me playing tennis this afternoon.
c) I play tennis in the afternoon if and only if the humidity is low.
d) If the sun is not shining, the humidity is low.
e) If the sun is shining and the humidity is low, I will finish my assignment before lunch and play tennis in the afternoon.

Exercise 1.15. For $x \in \mathbb{R}$, define $\lfloor x \rfloor$ as the floor function: x is rounded down to the closest integer. So $\lfloor 3 \rfloor = 3$, $\lfloor 4.2 \rfloor = 4$, $\lfloor 6.9 \rfloor = 6$ and $\lfloor -1.1 \rfloor = -2$. Start with the integers $m = 3$ and $n = 8$ and evaluate the following code. The values of m and n are kept throughout the assignment: the output of a) is the input for b), etc. The notion `n:=n+2` means that the new value of n is the old value plus two. Determine the final values for m and n.

a) `if n-m=5 then n:=n-2`
b) `if ((2*m=n) and (⌊n/4⌋=1)) then n:=4*m-3`
c) `if ((n<8) or (⌊m/2⌋=2)) then n:=2*m else m:=2*n`
d) `if ((m<20) and (⌊n/6⌋=1)) then m:=m-n-5`
e) `if ((n=2*m) or (⌊n/2⌋=5)) then m:=m+2`

Exercise 1.16. Let p and q be the following statements concerning integers k and l:

p: k is even;
q: l is even.

Write the following two statements in symbolic form:

a) k is even and l is odd, or k is odd and l is even.
b) k and l are not both even and not both odd.

Use a truth table to show that the statements in a) and b) are equivalent.

Exercise 1.17. Use truth tables to show that the following statements are logically equivalent.

a) $p \to q$ and $\neg p \vee q$
b) $p \leftrightarrow q$ and $(p \to q) \wedge (q \to p)$
c) $p \wedge (q \vee r)$ and $(p \wedge q) \vee (p \wedge r)$

Exercise 1.18. Use truth tables to show that the following statements are logical implications.

a) $[(p \vee q) \wedge \neg q] \to p$

b) $[(p \to q) \wedge (q \to r)] \to (p \to r)$

Exercise 1.19. Use truth tables to examine if the following statements are tautologies. If not, give a counterexample by assigning truth values to the propositions that make the statement false.

a) $(p \wedge (p \to q)) \to q$

b) $(p \to q) \to (q \to p)$

c) $(\neg p \vee r) \to (q \to r)$

d) $[(p \to r) \wedge (q \to r)] \to [(p \vee q) \to r]$

Exercise 1.20. Let A, B, C be sets. Give a counterexample for the statement:
If $A \subseteq B$ and $B \not\subseteq C$, then $A \not\subseteq C$. (Hint: use a Venn diagram).

Exercise 1.21. Use membership tables to examine the following statements concerning sets A, B, C and D. If a statement is not true in general, provide a counterexample.

a) $\overline{A \cap B} = \overline{A} \cup \overline{B}$ (De Morgan law)

b) $(A \cap B) \cup (C - B) = (A \cup \overline{B}) \cap C$

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

d) $(A \cup \overline{B}) \subseteq (A \cap B) \cup \overline{(B \cap C)}$

e) $(A \cap B \cap \overline{C}) \cup (A \cap \overline{D}) = A - [(A \cup B) \cap C \cap D]$

Exercise 1.22. Let $p(x)$ be the statement "$x^2 > 10$".
Determine the truth value of $p(x)$ for the following values of x:

a) $x = 3$

b) $x = -2$

c) $x = 5$

Determine the truth value of $\forall x\, p(x)$ for each of the following domains:

d) $\mathbb{R}$

e) $\{1, 2, 3, 4\}$

f) The interval $[10, 56.7]$

Determine the truth value of $\exists x\, p(x)$ for each of the following domains:

g) $\mathbb{R}$

h) $\{1, 2, 3, 4\}$

i) The interval $[10, 56.7]$

Exercise 1.23. Let $p(x)$ be the statement $\frac{x^2+2}{x} > 2$ and $q(x)$ be the statement $\frac{x^2+2}{x} \leq 2$. Consider the domain of the positive real numbers: $(0, \infty)$.

a) Determine the truth value of $\forall x\, p(x)$.

b) Determine the truth value of $\exists x\, q(x)$.

c) How are a) and b) related?

Exercise 1.24. (Cf. Example 1.2.22) Let A and B be sets. Give quantified statements for:

a) $A \subset B$

b) $A \not\subseteq B$

c) $A \not\subset B$

d) $A \cap B = \emptyset$

Exercise 1.25. Consider the domain $\mathbb{Q} - \{0\}$. Determine the truth value of the following statements:

a) $\exists x\ [\exists y\ (xy = 1)]$ b) $\exists x\ [\forall y\ (xy = 1)]$ c) $\forall y\ [\exists x\ (xy = 1)]$

Exercise 1.26. Negation of quantified statements.
Use Theorem 1.2.23 to determine statements that are equivalent to the following statements and do not use the operator "¬".

a) $\neg\,[\forall d \in D\ (d > -1)]$
b) $\neg\left[\forall \varepsilon > 0\ \left[\exists \delta > 0\ \left[\forall x \in \mathbb{R}\ \big((|x| < \delta) \to \big(x^2 < \varepsilon\big)\big)\right]\right]\right]$

2 PROOFS

Formulating a proof of a statement is not easy and requires a lot of practice. In this chapter we discuss how to formalize a statement, what kind of proof techniques there are and how to start formulating a proof. One could wonder why we care so much about writing arguments so precisely as done in the previous chapter. Often, a picture or short argument will give the feeling that the statement is true – why bother about constructing formal proofs?

The answer to this question lies in generalization. If you have a specific problem, it might not need a formal proof to solve it. If someone else has another problem that is slightly related, this problem might be solved in the same way – or this might turn out to be not the case. Analyzing a problem to see under which conditions the solution is true makes it so that other people can benefit from this knowledge and find solutions to other problems, starting from results that have been reached already, without having to reinvent the wheel. For example, one may ask whether or how the solution to a problem changes under different conditions.

For this, it is necessary that these problems are formulated mathematically and in the same language, so that other people are able to independently verify the validity of the solution. Thus, even if it easy to see that a statement is true, we still need to prove it: what at first looks like unnecessary extra work, will save time in the long run.

To see why this indeed works, consider the following example. Remember the chemistry lessons in high school where a chemical equation was given and you had to determine the right coefficients. Now if this equation included only a few atoms it would be easy to solve, but as soon as the number of atoms got larger the puzzling got heavier. Mathematicians came up with a more structured approach to solve this problem systematically instead of using some trial and error method: linear algebra. It turns out that many other problems can be solved with this theory as well: economic models, social studies use it to represent who knows who in a group of people, physicists use it to calculate how heat flows through objects, engineers use it to calculate the forces an object can handle, and there are many more applications. The mathematical theory is the same, regardless of the application at hand.

Finally, learning how to formulate and to prove a statement helps you to structure your thoughts and make an argument solid. When statements get complicated and proofs get long, the skill you obtain is how to keep the overview and cut down a problem into several smaller, easier problems. This is a skill that is very useful in everyday life – it is no coincidence that many mathematicians end up in high, influential positions in society where you would not have expected them if you recall they studied theoretical concepts for at least five years. So although the theory in this course might be quite difficult at first sight, think of it as a long-term investment.

2.1 How to prove a statement?

An idea which can be used once is a trick. If it can be used more than once it becomes a method.
György Pólya and Gábor Szegö

Most mathematics you have learned so far usually had a recipe: there is a certain procedure you have to follow, and as soon as you have learned that procedure you are able to do all of the exercises. It might take some time to learn the procedure, but once you know how it works it gets easy.

A *proof* of a statement is something else than just giving some examples for which the statement is valid (hoping that these examples convince the reader that the statement is also valid in all other situations that can be considered). E.g., if we want to prove that for any sets A, B and C, the equality $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ holds, it is not enough to show that this equality holds for some specific chosen sets A, B and C (e.g., $A = \{1, 2, 3\}$, $B = \{2, 4, 5\}$ and $C = \{1, 2, 4\}$), since this does not imply in any way that the equation also holds for other choices of A, B and C.
A *proof* of a statement is a watertight argument that guarantees that the statement holds in all possible situations that can be considered.
There is no standard procedure that will enable you to prove all statements. There are however some guidelines that can help.

1. Determine what is given and what you can assume about the problem. Determine what you must show or find.
2. Write down the mathematical definitions of what you have to show, and the definitions of concepts you may use. These first two steps require some reading skills: what exactly is asked? What exactly is given already?
3. Before starting the formal proof, look at the problem and see if the statement is reasonable. Things that might help here are making a picture, trying an example, or discussing the problem with others. Do not give up quickly on this part, as the other steps will be easier as soon as you have the feeling the statement must be true. Conversely, if you think the statement is not true, you can try to find a counterexample. If you find it you are done, and if you cannot find it then think about why it is not possible to find one.

4. If it is not clear why the statement is true, browse through related theorems and examples to see if they have something to do with what you are given or what you need to show. This might give you an idea for a proof.
5. As soon as you have the feeling the statement is true, analyze why that is the case. A proof often exists of several steps which lead from the givens to the desired result. Write down these consecutive steps. It should be like a construction work: orderly, systematic and with a reasonable pace. This is the step in which you actually write the proof. It is of the utmost importance that you carefully explain all steps you take. Someone else (with the same mathematical knowledge as you) must be able to follow your arguments without you sitting next to them elucidating each part they do not understand. A proof that is only clear to yourself is useless.
6. Now that you have written down everything there is, take some distance and see if it is a good argument. Are all steps justified? Is there something missing? Is the conclusion what was asked for?

Concerning the formulation of the arguments in a mathematical proof, one often avoids the logical notations treated in Chapter 1. To improve the readability of a proof, logical symbols like $\forall$, $\exists$, $\to$, $\leftrightarrow$, $\wedge$, $\vee$ are mostly replaced by their literal equivalents: "for all", "there exists", "if... then", "if and only if", "and", "or". It is however important to realize that the logical framework that we built in Chapter 1 can always be used as a fallback whenever one doubts whether a proof is actually valid. If necessary, this somewhat mechanical, though strictly objective system will help us decide in these situations.

Before we start with examples of mathematical proofs, we once more want to emphasize the important difference between an "if... then" statement and an "if and only if" statement. Consider, for example, the following statements concerning integers a and b: "if a and b are odd, then ab is odd" and "a and b are odd if and only if ab is odd". The second statement is stronger than the first one. So proving the first statement is not enough to guarantee that the second one is true. To prove that the second statement is true one must prove the first statement as well as the statement "if ab is odd then a and b are odd".
In *definitions* however, often "if... then" is used when "if and only if" is meant. Consider for example Definition 1.1.20. Formally this definition should be stated as: A is a subset of B *if and only if* every element of A is an element of B. Also Definition 2.1.2, concering even and odd integers, is stated in the "if... then" form, where "if and only if" is meant.

Now let's consider examples of mathematical proofs. We start with a proof of a statement in set theory.

Example 2.1.1. (De Morgan's law.)

$$\overline{A \cup B} = \overline{A} \cap \overline{B} \text{ for all sets } A \text{ and } B.$$

Considering the statement which has to be proved, we see that this statement concerns the equality of the set $\overline{A \cup B}$ *and the set* $\overline{A} \cap \overline{B}$*. In Chapter 1 we learned that two sets are equal if each element of the first set is also in the second set and each element of the second set is also in the first set. In other words: the first set is a subset of the second set and the second set is a subset of the first set. This gives rise to the idea to split the proof into two parts.*
In the first part we show that each element of $\overline{A \cup B}$ *is also in the set* $\overline{A} \cap \overline{B}$*. This can be formulated as: for each* x *we have: if* $x \in \overline{A \cup B}$ *then also* $x \in \overline{A} \cap \overline{B}$*. And in the second part we show that for each* x *we have: if* $x \in \overline{A} \cap \overline{B}$ *then also* $x \in \overline{A \cup B}$*.*
Now that we have an idea of the structure of the proof, we start writing. The arguments in the proof are based on the definitions of the complement, the union and the intersection of sets, given in Chapter 1.

Proof.

Part 1. Take an arbitrary element $x \in \overline{A \cup B}$. We will show that $x \in \overline{A} \cap \overline{B}$.
Well, if $x \in \overline{A \cup B}$, then, by the definition of complement of a set: $x \notin A \cup B$. By the definition of union of two sets, this means that x is neither in A, nor in B, so $x \notin A$ and $x \notin B$. Again, by the definition of complement, this means that $x \in \overline{A}$ and $x \in \overline{B}$. Finally, by the definition of intersection of two sets, this last statement is equivalent to $x \in \overline{A} \cap \overline{B}$. Since this argument is true for $x \in \overline{A \cup B}$, we have $\overline{A \cup B} \subseteq \overline{A} \cap \overline{B}$.

Part 2. Take an arbitrary element $x \in \overline{A} \cap \overline{B}$. We will show that $x \in \overline{A \cup B}$.
This part of the proof is Exercise 2.1. □

Note the square "□". This symbol indicates the end of a proof.

The next example shows the proof that the product of two odd numbers is odd. In order to construct a formal proof for this statement, we first give a precise definition of *even* and *odd* integers.

Definition 2.1.2 (Even, Odd). Let n be an integer, i.e., $n \in \mathbb{Z}$. We say that

- n is *even* if there exists an integer $k \in \mathbb{Z}$ such that $n = 2k$.
- n is *odd* if there exists an integer $k \in \mathbb{Z}$ such that $n = 2k + 1$.

Note that an integer is either even or odd.

Example 2.1.3.

If m and n are two odd integers, then mn is also an odd integer.

To analyse this statement we first use the definition of an odd *integer to formalize what is given and what we need to prove. The condition that* m *is an odd integer means that there exists an integer* $k \in \mathbb{Z}$ *such that* $m = 2k+1$*. The condition that* n *is an odd integer means that there also* *exists such an integer for n. Of course this need not be the same integer k that we introduced for m (otherwise we would get $m = 2k + 1$ and also $n = 2k + 1$, and therefore $m = n$, which is of course not necessarily the case). So, let's take the letter l: there exists an integer $l \in \mathbb{Z}$ such that $n = 2l + 1$. We must show that the integer mn is odd, in other words, we must show that there exists an integer $p \in \mathbb{Z}$ such that $mn = 2p + 1$. Note that again we chose another letter to indicate that mn is odd: p is not necessarily equal to k or equal to l. Now we have formalized mathematically what is given and what we want to prove and can start writing down the proof.*

Proof. Since m and n are odd, there exist $k, l \in \mathbb{Z}$ such that $m = 2k + 1$ and $n = 2l + 1$. We now must show that there exists a $p \in \mathbb{Z}$ such that $mn = 2p + 1$.
Well, from the fact that m and n are odd, we get

$$mn = (2k + 1)(2l + 1) = 4kl + 2k + 2l + 1.$$

Is this an odd integer? If so, what is p?
Factorizing the terms in the calculation above, we get

$$4kl + 2k + 2l + 1 = 2(2kl + k + l) + 1.$$

So we can take $p = 2kl+k+l$, which is an integer. Now the proof is complete, since we have shown that we can always find an integer p as described above, regardless of the values of the odd integers m and n. □

Note that the expression for p we described in the proof ($p = 2kl + k + l$) depends on the values of k and l, and therefore on the values of m and n. This is not surprising: if we took other integers for m and n, the product mn would probably also be different, and therefore also the value for p would change.

When studying a proof, be careful not to accept all that is said without verifying the steps. At first sight the following proof might be reasonable, but the result is not true at all.

Example 2.1.4.

$$4 = 3.$$

Proof. Let a, b and c be three numbers such that

$$a + b = c.$$

This can also be written as

$$(4a - 3a) + (4b - 3b) = 4c - 3c.$$

After reorganizing:

$$4a + 4b - 4c = 3a + 3b - 3c.$$

Factorization yields

$$4(a + b - c) = 3(a + b - c).$$

Finally cancel the same term left and right:

$$4 = 3. \qquad \square$$

What went wrong?

If we do not check conditions or theorems before we apply them, awkward things like Example 2.1.4 can happen. In case you have not noticed the mistake there yet: the last step is only valid if $a + b - c \neq 0$. However, we assumed $a + b = c$, so $a + b - c = 0$.

In the following sections, some frequently used proof techniques are discussed.

2.2 Counterexample

If only I had the theorems! Then I should find the proofs easily enough.
Bernhard Riemann

As we already have seen in Chapter 1, a counterexample can be used to show that a theorem is not true. It is an example that satisfies the conditions stated in the theorem, but does not satisfy the theorem's conclusion. In that case, we have shown that the theorem is not true in general. This saves all the work of formulating a proof, therefore it is often wise to start searching for a counterexample if you are not yet convinced that the theorem is valid. The following examples are about prime numbers. A *prime number* (or *prime*) is a positive integer which has two different divisors, namely 1 and itself. So, the ten smallest prime numbers are: 2, 3, 5, 7, 11, 13, 17, 19, 23 and 29.

Statement 2.2.1.

All prime numbers are odd.

This statement is true for all prime numbers, except for 2 which is an even number. Thus, we have found a counterexample by taking the number 2: this number 2 is a prime, but it is not odd. The statement is false.

Statement 2.2.2.

For all $n \in \mathbb{N}$, the number $n^2 + n + 41$ is prime.

One can verify that this statement is true for all $n \leq 39$. However it is easy to see that it is false for $n = 41$ (and also for $n = 40$). Therefore the statement is not true: we constructed a counterexample by taking $n = 41$: 41 satisfies the condition of the statement ($41 \in \mathbb{N}$), but not the conclusion ($41^2 + 41 + 41 = 41 \cdot 43$ is not prime). The statement is false.

A counterexample can also be used to verify the necessity of the conditions of a theorem. If there are many conditions needed for a theorem, the result might not be so useful. Conversely, if there are just a few conditions needed, the theorem is much more widely applicable: it is much stronger. Therefore, it is useful to check if all conditions are really necessary for the theorem to be true. This can be done using counterexamples. To show that a certain condition is necessary for the theorem, skip that condition and construct a counterexample to show that the remaining conditions cannot guarantee the validity of the conclusion.

Statement 2.2.3.

If $x \geq 0$, $y \geq 0$ and $\sqrt{x^2} = \sqrt{y^2}$, then $x = y$.

This statement has three conditions: $x \geq 0$, $y \geq 0$ and $\sqrt{x^2} = \sqrt{y^2}$. Each of these conditions is necessary to make it a true statement. If, for example, the first condition "$x \geq 0$" is skipped, then a counterexample for the statement can be constructed by taking $x = -1$ and $y = 1$. The remaining conditions are satisfied ($y \geq 0$ and $\sqrt{x^2} = \sqrt{y^2}$), but not the conclusion: $x \neq y$.

2.3 Contradiction

The proof [of the existence of an infinity of prime numbers] is by reductio ad absurdum, and reductio ad absurdum, which Euclid loved so much, is one of a mathematician's favourite weapons. It is a far finer gambit than any chess gambit: a chess player may offer the sacrifice of a pawn or even a piece, but a mathematician offers the game.

Godfrey Harold Hardy

The idea behind this proof technique is that we do not try to prove directly that the given theorem is true. Instead, we assume the theorem is false. Then we show that this has unacceptable consequences. Thus, it cannot be that the theorem is false. Therefore, it must be true. An example of a theorem that is proved by contradiction is the Pigeonhole Principle.

Theorem 2.3.1 (Pigeonhole Principle)**.** If m pigeons occupy n pigeonholes and $m > n$, then at least one pigeonhole is occupied by two or more pigeons.

Proof. Consider m pigeons and n pigeonholes, with $m > n$ and suppose the theorem is not true.
Then there are no pigeonholes occupied by more than one pigeon. So each pigeonhole is occupied by at most one pigeon. Since there are n pigeonholes, this means that at most n pigeons occupy a pigeonhole. Thus, there are at least $m - n > 0$ pigeons that are not in a pigeonhole. This is a contradiction with the given that all m pigeons occupy a pigeonhole. So the assumption that the theorem is false contradicts the givens. Therefore the theorem must be true. □

Another example concerning the Pigeonhole Principle is the example about the number of Facebook profiles in the Introduction of these lecture notes. We end this section with a bit more advanced example of a proof by contradiction.

Example 2.3.2.

$$\sqrt{2} \notin \mathbb{Q}.$$

Proof. Assume that the statement is false, i.e., assume that $\sqrt{2} \in \mathbb{Q}$.
Then, by the definition of the set $\mathbb{Q}$ (see Section 1.1.2), there exist integers $\tilde{a}$, $\tilde{b} \in \mathbb{Z}$, $\tilde{b} \neq 0$, such that $\sqrt{2} = \frac{\tilde{a}}{\tilde{b}}$.
First, if necessary, we simplify this fraction (by repeatedly dividing numerator and denominator by 2) to get a fraction $\frac{a}{b} = \frac{\tilde{a}}{\tilde{b}}$ such that not both a and b are even.
Squaring the equation $\sqrt{2} = \frac{a}{b}$, we get: $2 = \frac{a^2}{b^2}$ and therefore $a^2 = 2b^2$. So a^2 is even, since it is twice the value of an integer (cf. Definition 2.1.2). Since the square of an odd number is odd (take $m = n$ in Example 2.1.3), a must be even. Therefore (again by Definition 2.1.2), there exists an integer k such that $a = 2k$. Substituting this expression for a in the equation $a^2 = 2b^2$, we get $(2k)^2 = 2b^2$, so $4k^2 = 2b^2$. Dividing this equation by 2 yields $2k^2 = b^2$, which implies that b^2 is even and therefore also b is even. This contradicts the assertion above that not both a and b are even. Therefore, there cannot exist integers $\tilde{a}$ and $\tilde{b}$ such that $\sqrt{2} = \frac{\tilde{a}}{\tilde{b}}$.
This completes our proof of $\sqrt{2} \notin \mathbb{Q}$. □

2.4 Direct proof

This is a one-line proof... if we start sufficiently far to the left.

The previous methods proved that a theorem was not true, or showed that the theorem could not be false. A more elegant way to prove a theorem is to make use of a direct proof. A direct proof is a sequence of logical arguments that deduce the conclusion from the givens of the theorem. Often, other theorems and results are used as arguments. The following example can be proved using a direct proof.

Example 2.4.1.

If a and b are even integers, then the sum $a + b$ is an even integer as well.

Proof. Suppose a and b are even integers. By Definition 2.1.2, there exist $k \in \mathbb{Z}$ and $l \in \mathbb{Z}$ such that $a = 2k$ and $b = 2l$. In order to prove that $a + b$ is even, we must show that there exists an integer $p \in \mathbb{Z}$ such that $a + b = 2p$. Well, $a + b = 2k + 2l = 2(k + l)$, so we can take $p = k + l$. This proves that $a + b$ is an even integer. □

The next example of a direct proof is an application of Theorem 2.3.1.

Example 2.4.2.

Let $A \subseteq \{1,2,3,4,5,6,7,8,9\}$ with $|A| = 6$.
Then A contains two different elements i and j such that $i + j = 10$.

Proof. Let $A \subseteq \{1,2,3,4,5,6,7,8,9\}$ with $|A| = 6$.
Consider the 6 elements of A as 6 pigeons and consider the sets $\{1,9\}$, $\{2,8\}$, $\{3,7\}$, $\{4,6\}$, $\{5\}$, as 5 pigeonholes. Now put each pigeon in the pigeonhole that contains the number of the pigeon (e.g. if $7 \in A$ then put pigeon 7 in pigeonhole $\{3,7\}$). Now apply Theorem 2.3.1 with $m = 6$ and $n = 5$. Then we obtain that (at least) one fo the sets $\{1,9\}$, $\{2,8\}$, $\{3,7\}$, $\{4,6\}$ and $\{5\}$ contains two elements of A. Obviously this set must be one of the sets $\{1,9\}$, $\{2,8\}$, $\{3,7\}$ or $\{4,6\}$, because the set $\{5\}$ cannot contain more than one element of A. Therefore A must have at least one of the sets $\{1,9\}$, $\{2,8\}$, $\{3,7\}$ or $\{4,6\}$ as a subset. And so, A must contain two different elements i and j such that $i + j = 10$. □

Also the proofs of Examples 2.1.1 and 2.1.3 are direct proofs.

2.5 Proof by cases

If there is a problem you can't solve, then there is an easier problem you can solve: find it.
György Pólya

Sometimes it is hard to construct a proof directly, as there are several cases to distinguish. Then a proof can be constructed by proving these cases separately. This leads to a so-called proof by cases. Consider the following example.
Remember that the *absolute value* of a number x is denoted by $|x|$. It is defined as

$$|x| = \begin{cases} x & \text{if } x \geq 0, \\ -x & \text{if } x < 0. \end{cases}$$

So, if $x = -5$ then $|x| = 5$, if $x = 4$ then $|x| = 4$ and if $x = 0$ then $|x| = 0$.

Example 2.5.1.

For all $x \in \mathbb{R}: \quad x \leq |x|$.

Proof. Let $x \in \mathbb{R}$. We will distinguish two cases.
Case one. If $x \geq 0$, then $|x| = x$ and therefore $x \leq |x|$.
Case two. If $x < 0$, then $|x| = -x$ and, since $|x| \geq 0$. this implies $x = -|x| \leq 0 \leq |x|$.
So $x \leq |x|$.
In both cases we proved that $x \leq |x|$. Since for each $x \in \mathbb{R}$ we have either $x \geq 0$ or $x < 0$ we proved that the inequality $x \leq |x|$ holds for all $x \in \mathbb{R}$. □

Another example of a proof by cases is the proof concerning the number of Facebook profiles, in the introduction of these lecture notes. There we distinguished the two cases “there exists a profile with no friends” and “there does not exist a profile with no friends”.

2.6 Mathematical induction

*We **define** the ‘natural numbers’ as those to which proofs by mathematical induction can be applied, i.e. as those that possess all inductive properties.*
Bertrand Russell

Imagine a long table where you stand on the head end. On the table is a long, long, possibly infinite row of blocks. Some of them are marked with a dot. Suppose that you know two things:

(a) The first block is marked with a dot.

(b) For each integer $k \geq 1$: if the block with number k is marked with a dot, then also the block with number $k + 1$ is marked with a dot.

What do these two statements imply? We know because of (a) that the first block is marked. Because the first block is marked, (b) applied to $k = 1$ implies that the second block must be marked as well. Now we know that the second block is marked, we apply (b) again, now taking $k = 2$, and deduce that the third block is marked. When this argument is repeated, we can derive that also block 402 and block 385492 are marked with a dot. Thus, all blocks are marked with a dot.

A similar example uses domino blocks. If one block falls, the next block will fall as well. So if you push the first block, all of the blocks (if you placed them correctly) will fall. This illustrates the principle of mathematical induction. Mathematical induction is a proof technique that is often used to prove that statements $S(n)$ are true for all positive integer values of n (in the example above the statement $S(n)$ would be: “the ”n-th block is marked with a dot”).

The next theorem formalizes the validity of this proof technique.

Theorem 2.6.1 (Principle of Mathematical Induction)**.** Let, for each $n \in \mathbb{N}$, $S(n)$ be a statement. Suppose that:

(a) $S(1)$ is true;

(b) For each $k \in \mathbb{N}$, if $S(k)$ is true, then also $S(k + 1)$ is true.

Then $S(n)$ is true for every positive integer n.

Theorem 2.6.1 can be proved using the precise definition of the set $\mathbb{N}$, but this proof is beyond the scope of this course. We will however use the proof technique of mathematical induction itself.

Step (a) is called the *basis step*, step (b) is the *induction step*. The numbering of the statements do not necessarily need to start with 1. E.g. the principle of mathematical induction can also be applied if a sequence of consecutive numbered statements $S(n)$, with $n \geq 13$: $S(13)$, $S(14)$, $S(15)$, etc. are given such that the first statement $S(13)$ is true, and for each $k \geq 13$, if $S(k)$ is true, then also $S(k+1)$ is true.
The principle of mathematical induction is very useful when statements concerning integers are involved. All the blocks mentioned above had an integer number, and the corresponding statement $S(n)$ would be that "block number n is marked with a dot". In the domino example, $S(n)$ would be the statement "block number n will fall".

The following example concerns a well-known formula for the sum of the first n natural numbers (cf. Section 1.1.5). In order to explicate clearly the principles of a proof with mathematical induction, we first show an extended version of the proof (including comments concerning the structure of the proof). Then we state the formal proof (which you will understand as soon as you are familiar with the ideas of mathematical induction). This second proof is the usual way induction proofs are formulated.

Example 2.6.2.

$$\text{For all } n \in \mathbb{N}: \quad \sum_{i=1}^{n} i = \frac{n(n+1)}{2}.$$

Proof (extended version). We define, for each $n \in \mathbb{N}$, the statement $S(n)$ by:

$$S(n): \quad \sum_{i=1}^{n} i = \frac{n(n+1)}{2}. \tag{2.1}$$

We will prove, using mathematical induction, that $S(n)$ is true for all $n \in \mathbb{N}$. In order to do so, we must prove the basis step (a) and the induction step (b).

<u>Basis step</u> for $n = 1$.
To prove $S(1)$, we calculate the left-hand side and right-hand side of (2.1) for $n = 1$:

$$\sum_{i=1}^{1} i = 1 \qquad \text{and} \qquad \frac{1(1+1)}{2} = 1.$$

Because these are equal, $S(1)$ is true.

<u>Induction step</u>.
Now we prove the induction step. So we *assume* that $S(k)$ is true for some $k \in \mathbb{N}$:

$$\sum_{i=1}^{k} i = \frac{k(k+1)}{2}. \tag{2.2}$$

(2.2) is called *induction hypothesis*. Using this induction hypothesis, we will try to prove that also the statement $S(k+1)$ must be true, in other words, assuming that (2.2) is true we will try to prove that:

$$\sum_{i=1}^{k+1} i = \frac{(k+1)(k+2)}{2}. \tag{2.3}$$

In order to use the induction hypothesis, we must rewrite the left-hand side of (2.3) in such a way that the expression $\sum_{i=1}^{k} i$ appears. Then we can apply the induction hypothesis (2.2) and replace this expression by $\frac{k(k+1)}{2}$. After that it remains to show that this new expression is equal to the right-hand side of (2.3).

So we start rewriting the left-hand side of (2.3) in such a way that (2.2) can be used. This can be done by "splitting off the $(k+1)$-st term of the sum":

$$\sum_{i=1}^{k+1} i \quad = \quad 1+2+\cdots+k+(k+1) \quad = \quad \left(\sum_{i=1}^{k} i\right) + (k+1). \tag{2.4}$$

Note that now the induction hypothesis (2.2) can be applied to the right-hand side of (2.4):

$$\left(\sum_{i=1}^{k} i\right) + (k+1) = \frac{k(k+1)}{2} + (k+1). \tag{2.5}$$

Now it remains to show that the right-hand side of (2.5) is equal to the right-hand side of (2.3). This can be done with straightforward calculations:

$$\frac{k(k+1)}{2} + (k+1) = \frac{k(k+1)}{2} + \frac{2(k+1)}{2} = \frac{k(k+1)+2(k+1)}{2} = \frac{(k+1)(k+2)}{2}. \tag{2.6}$$

Now, from (2.4)–(2.6) we obtain (2.3), which we what we wanted to prove in the induction step

Thus, combining the basis step, the induction step, and the principle of mathematical induction, we have proved that (2.1) is true for all $n \in \mathbb{N}$. □

Remarks 2.6.3.

1. It is important to realize that in the proof *we do not know* if the statement $S(k)$ in the induction hypothesis is true or false. The only thing we need to show, for an arbitrary k, is that *if* $S(k)$ is true then also $S(k+1)$ must be true.
2. The last equality (2.6) of the proof can also be proved by working out the left-hand side and right-hand side separately and then show that those expressions are equal.

Now we state the common version of the proof (without the remarks concerning the structure of the proof).

Proof (formal version). Proof by mathematical induction.

Basis for $n = 1$.

$$\sum_{i=1}^{1} i = 1 \qquad \text{and} \qquad \frac{1(1+1)}{2} = 1.$$

Induction step.
Let $k \in \mathbb{N}$ and assume that

$$\sum_{i=1}^{k} i = \frac{k(k+1)}{2}. \tag{2.7}$$

We will show that (2.7) implies:

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

Well:

$$\sum_{i=1}^{k+1} i = \left(\sum_{i=1}^{k} i\right) + (k+1) = \frac{k(k+1)}{2} + (k+1) = \frac{k(k+1)+2(k+1)}{2} = \frac{(k+1)(k+2)}{2},$$

where the second equality follows from the induction hypothesis (2.7). □

You might have known the result in Example 2.6.2 already, or have been able to reason why statement (2.1) would be true. Now we will show an example with a somewhat more involved proof. First we formally induce the notion of "divisible by".

Definition 2.6.4 (Divisibility)**.** Let m and d be integers, i.e., $m, d \in \mathbb{Z}$. We say that m is *divisible by* d if there exists an integer $l \in \mathbb{Z}$ such that $m = dl$.

Note that in case $d = 2$, Definition 2.6.4 corresponds to the definition of *even* in Definition 2.1.2.

Example 2.6.5.

For all $n \in \mathbb{N}$, the number $5^n - 1$ is divisible by 4.

As with Example 2.6.2 we will first give an extended proof (to help you understand the principle of mathematical induction) and then the formal version.

Proof (extended version). For each $n \in \mathbb{N}$, define the statement $S(n)$ by:

$$S(n): \quad 5^n - 1 \text{ is divisible by } 4. \tag{2.8}$$

We will prove, using mathematical induction, that $S(n)$ is true for all $n \in \mathbb{N}$.

Basis step for $n = 1$.
$S(1)$ is true because

$$5^1 - 1 = 4 = 4 \cdot 1 \quad \text{(take } l = 1 \text{ in definition 2.6.4).}$$

Induction step.
Assume that $S(k)$ is true for *some* integer $k \geq 1$. So our induction hypothesis is

$$5^k - 1 \text{ is divisible by } 4, \qquad \text{i.e.,} \quad 5^k - 1 = 4l \text{ for some integer } l. \tag{2.9}$$

Using this induction hypothesis, we will try to prove that also the statement $S(k+1)$ is true, so we will try to prove that

$$5^{k+1} - 1 \text{ is divisible by } 4. \tag{2.10}$$

In order to use the induction hypothesis (2.9), we must rewrite the expression $5^{k+1} - 1$ in (2.10) in such a way that the term 5^k appears. Then we can apply the induction hypothesis (2.9) and replace 5^k by $4l + 1$. After that it remains to show that the expression that appears after this substitution is also divisible by 4.
So we start rewriting (2.10) so that (2.9) can be used. This can be done by splitting off one factor 5;

$$5^{k+1} - 1 = 5 \cdot 5^k - 1. \tag{2.11}$$

Now the induction hypothesis (2.9) can be applied to the right-hand side of (2.11): the factor 5^k can be replaced by $4l + 1$:

$$5 \cdot 5^k - 1 = 5(4l + 1) - 1. \tag{2.12}$$

Now it remains to show that the right-hand side of (2.12) is also divisible by 4. This is easy:

$$5(4l + 1) - 1 = 5 \cdot 4l + 5 - 1 = 4 \cdot 5l + 4 = 4(5l + 1). \tag{2.13}$$

The right-hand side of (2.13) is clearly divisible by 4, because it equals 4 times an integer.
Now, from (2.11)–(2.13) we obtain (2.10), which is what we wanted to prove in the induction step.

Thus, combining the basis step, the induction step, and the principle of mathematical induction, we have proved that (2.8) is true for all integers $n \geq 1$. $\square$

Proof (formal version). Proof by mathematical induction.
Basis for $n = 1$.

$$5^1 - 1 = 4 = 4 \cdot 1.$$

Induction step.
Let $k \in \mathbb{N}$ and assume that

$$5^k - 1 = 4l \quad \text{for some } l \in \mathbb{Z}. \tag{2.14}$$

We will show that (2.14) implies:

$$5^{k+1} - 1 = 4m \quad \text{for some } m \in \mathbb{Z}.$$

Well:

$$5^{k+1} - 1 = 5 \cdot 5^k - 1 = 5(4l + 1) - 1 = 4(5l + 1),$$

where the second equality follows from the induction hypothesis (2.14).
So we can take $m = 5l + 1$. $\square$

2.7 Exercises

Exercise 2.1.

a) Complete the second part of the proof of Example 2.1.1.
b) Prove that for any sets A, B and C: $A - (B \cup C) = (A - B) \cap (A - C)$.

Exercise 2.2. Find the errors in the following "proofs":

a) Statement: $-3 = 3$.
Proof. If $x = -3$, then $x^2 = 9$. So $x = \sqrt{9} = 3$. Hence, $-3 = 3$. □
b) Statement: $-8 = 8$.
Proof. If $x = -8$, then $x^{\frac{2}{3}} = \sqrt[3]{(-8)^2} = \sqrt[3]{64} = \sqrt[3]{8^2}$. So $x = 8$. Hence, $-8 = 8$. □

Exercise 2.3. Give a proof or a counterexample for each of the following statements:

a) If a, $b \in \mathbb{R}$ and $a^2 > b^2$, then $a > b$.
b) If $x \in \mathbb{R}$ and $x^3 = x$, then $x^2 = 1$.

Exercise 2.4. Give a proof or a counterexample for each of the following statements concerning arbitrary integers m, $n \in \mathbb{Z}$:

a) If both m and n are odd, then $m + n$ is even.
b) There exist m, $n \in \mathbb{Z}$ such that $m^2 + n^2 = 11$.
c) If n is even, then $(-1)^n = 1$.
d) If n^3 is even, then also n must be even.
e) $n(n + 1)$ is even.
f) If mn is odd, then both m and n are odd.

Exercise 2.5. For each of the following statements, prove that it is true or prove that it is false.

a) The sum of two primes is *not* a prime.
b) There exists a *unique* prime of the form $n^2 - 1$ for $n \in \mathbb{N}$.
c) There exists a number $n \in \mathbb{N}$, $n \geq 4$, such that n, $n + 2$ and $n + 4$ are all prime.

Exercise 2.6. A *perfect square* is the square of an integer. E.g.: 0, 1, 4, 9, 16, etc.
Give a proof for each of the following statements:

a) Each perfect square can be written as $4k$ or $4k + 1$, for some $k \in \mathbb{Z}$.
b) No perfect square ends with the digit 2.
c) The square of an odd integer has the form $8k + 1$, for some $k \in \mathbb{Z}$.
d) Let a, b, $c \in \mathbb{N}$ be such that $a^2 + b^2 = c^2$ (such a triple (a, b, c) is called a *Pythagorean triple*). Prove that if c is even then also a and b must be even.

Exercise 2.7. Give a proof or a counterexample for each of the following statements concerning the set of rational numbers $\mathbb{Q}$:

a) The average of two rational numbers is a rational number.
b) The average of two irrational numbers is an irrational number.
c) The difference between a rational number and an irrational number is an irrational number.

Exercise 2.8.

a) Prove that $\sqrt{3}$ is an irrational number. Hint: follow the proof of Example 2.3.2.
You may use (without proving it) the property that: for an integer a, if its square a^2 is divisible by 3, then also a itself is divisible by 3.
b) Let $a, b \in \mathbb{R}$ with $a < b$. Prove that there exists an $x \in \mathbb{R}$ such that $a < x < b$.
c) Prove that $x = 1.288888\ldots$ is a rational number. Hint: consider $100x - 10x$.

Exercise 2.9. Let $A \subseteq \{1, 3, 7, 8, 15, 16, 17, 20, 21, 22, 24\}$ with $|A| = 7$.

a) Prove that A contains two different elements i and j such that $i + j$ is divisible by 11.
Hint: see Example 2.4.2.
b) Show with a counterexample that the statement in a) is not necessarily true if $|A| = 6$.

Exercise 2.10. Prove the following statements with mathematical induction.

a) For all $n \in \mathbb{N}$: $\displaystyle\sum_{i=0}^{n}(2i + 1) = n^2$.
(The sum of the first n positive odd numbers is equal to n^2.)
b) For all $n \in \mathbb{N}$: $\displaystyle\sum_{i=1}^{n} i^2 = \frac{n(n+1)(2n+1)}{6}$.
(A formula for the sum of the first n squares.)
c) For all $n \in \mathbb{N}$: $\displaystyle\sum_{i=1}^{n}(i \cdot 2^i) = 2 + (n-1)2^{n+1}$.
d) For all $r \in \mathbb{R}$, $r \neq 1$, and all non-negative integers $n \geq 0$: $\displaystyle\sum_{i=0}^{n} r^i = \frac{1 - r^{n+1}}{1 - r}$.
Note in case $r = 0$: $0^0 = 1$ by definition.

Exercise 2.11. This exercise concerns the well-known Fibonacci numbers (which played an important role in Dan Brown's bestseller "The Da Vinci Code").
For each integer $n \geq 0$, the *Fibonacci number* F_n is recursively defined by:

(1) $F_0 = 0$, $F_1 = 1$,

(2) for each $n \geq 2$: $F_n = F_{n-1} + F_{n-2}$.

a) Show that $F_2 = 1$, $F_3 = 2$, $F_4 = 3$ and $F_5 = 5$. Determine F_6 and F_7.

Prove the following statements with mathematical induction:

b) For all non-negative integers $n \geq 0$: $\displaystyle\sum_{i=0}^{n} F_i = F_{n+2} - 1$.

c) For all non-negative integers $n \geq 0$: $\displaystyle\sum_{i=0}^{n} F_i^2 = F_n F_{n+1}$.

d) For all $n \in \mathbb{N}$: $F_{n+1}F_{n+1} - F_n^2 = (-1)^n$.

Exercise 2.12. Prove the following statements with mathematical induction (cf. Example 2.6.5).

a) For all non-negative integers $n \geq 0$: the number $2^{2n+1} + 1$ is divisible by 3.

b) For all non-negative integers $n \geq 0$: the number $7^{n+2} + 8^{2n+1}$ is divisible by 57.

Exercise 2.13. Let, for $n \in \mathbb{N}$, the numbers $a_n \in \mathbb{R}$ be recursively defined by:

(1) $a_1 = 1$,

(2) for all $n \geq 1$: $a_{n+1} = \sqrt{a_n\sqrt{3}}$.

a) Prove with mathematical induction that for all $n \in \mathbb{N}$: $0 < a_n < \sqrt{3}$.

b) Prove that for all $n \in \mathbb{N}$: $a_{n+1} > a_n$.

Exercise 2.14.

a) Prove that for each $x \in \mathbb{R}$: $|x|^2 = x^2$.

b) Prove that for all x_1, $x_2 \in \mathbb{R}$: $|x_1x_2| = |x_1|\,|x_2|$.

c) Prove that for all x_1, $x_2 \in \mathbb{R}$: $|x_1 + x_2| \leq |x_1| + |x_2|$.
Hint: first prove $|x_1 + x_2|^2 \leq (|x_1| + |x_2|)^2$ using a) and b) and the result of Example 2.5.1.

d) Prove with mathematical induction that for all $n \geq 2$ and all real numbers x_1, x_2, $\ldots$, x_n:

$$\left|\sum_{i=1}^{n} x_i\right| \leq \sum_{i=1}^{n} |x_i|.$$

Exercise 2.15. Find the error in the following “proof” that all people are identical.

Proof. We define, for each integer $n \geq 1$, the statement $S(n)$ by:

$$S(n): \quad \text{in each group of } n \text{ people, all people are identical.} \tag{2.15}$$

We will prove, using mathematical induction, that $S(n)$ is true for all integers $n \geq 1$.

Basis step for $n = 1$.

$S(1)$ is true because in any group of 1 person, this person is of course identical to himself or herself.

Induction step.
Now assume that $S(k)$ is true for *some* integer $k \geq 1$. So our induction hypothesis is:

In each group of k people, all people are identical.

Using this induction hypothesis, we will prove that also the statement $S(k+1)$ is true, i.e., we will prove that

In each group of $k+1$ people, all people are identical.

Well, consider any group of $k+1$ people. Leaving one person x out, we get a group of k people, which are all identical because of our induction hypothesis. Letting person x back in and leaving another person out we get again a group of k people, which are also identical because of the induction hypothesis. Therefore person x is identical to the others, and so all $k+1$ people must be identical. This proves the induction step.

Thus, combining the basis step, the induction step, and the principle of mathematical induction, we have proved that (2.15) is true for all integers $n \geq 1$, and therefore all people are identical. $\square$

3 COUNTING

Everything that can be counted does not necessarily count;
everything that counts cannot necessarily be counted.
Albert Einstein (attributed)

In how many ways can you arrange seven books on a shelf? How many different soccer teams can be formed if there are fourteen players? How many 5-card poker hands are there? The question 'In how many ways can we do something?' is often asked. In many applications, the answer to that question is a huge number. There are lots of possibilities for train schedules, for hospital schedules, in steps to be taken in a computer program.

Warning: For exposition purposes, the theorems presented in this chapter are mainly explained using informal arguments, rather than using the rigorous language introduced in the previous chapters.

3.1 Inclusion-Exclusion Principle

There are two rules in counting that might seem obvious results, but are essential building blocks of more complicated theorems. The first is the product rule.

Product rule. Suppose that a procedure can be broken down into a sequence of two tasks. If there are n_1 ways to do the first task and, for each of these ways of doing the first task, there are n_2 ways to do the second task, then there are $n_1 n_2$ ways to do the procedure.

Example 3.1.1. How many different license plates for cars are available if each plate consists of two digits, two letters and again two digits if all (26) letters and digits are allowed? Here we can use the product rule: $10 \times 10 \times 26 \times 26 \times 10 \times 10 = 6,760,000$ different plates.

The second counting rule is the sum rule.

Sum rule. If a task can be done either in one of n_1 ways or in one of n_2 ways, where no element of the set of n_1 ways is the same as any of the set of n_2 ways, then there are $n_1 + n_2$ ways to do the task.

Example 3.1.2. Suppose you want to join one student club. If there are 18 cultural clubs and 35 sports clubs, then there are $18 + 35 = 53$ clubs that you can join.

Note that it is essential in Example 3.1.2 that the set of 18 cultural clubs and the set of 35 sports clubs are *disjoint*, i.e., their intersection is empty. If, for example, 4 of the 18 cultural clubs also belong to the 35 sports clubs, then these four clubs would be counted twice in the sum $18+35$. So in order to count the number of distinct clubs, we must in that case subtract 4 from the sum of the number of cultural clubs and sports clubs: $18+35-4=49$. This idea is called the *principle of inclusion-exclusion*. We state this principle in the next theorem, for two and three sets. An illustration is given in Figure 1.3 on page 16. The principle can be extended to more than three sets, but this is beyond the scope of this course.

Theorem 3.1.3. If A, B and C are finite sets, then:

(i) $|A \cup B| = |A| + |B| - |A \cap B|$.

(ii) $|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|$.

Proof. (i) We must count the elements that are in $A \cup B$. In $A \cup B$ an element can be in A, in B or in both. Thus, if we count the elements in A and those in B and add them ($|A|+|B|$), we have double counted the elements that are in both sets. So, in order to count the elements in $A \cup B$, we have to subtract the number of elements in $A \cap B$ from $|A| + |B|$. This proves the result of part (i).

(ii) We must count the elements that are in $A \cup B \cup C$. If we count the elements in A in B and in C and add them ($|A|+|B|+|C|$), we have double counted the elements that are both in A and B, and those that are both in A and C, and also those that are both in B and C. If we subtract these three quantities from $|A| + |B| + |C|$, we get

$$|A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| \,. \tag{3.1}$$

Now the elements that are in the intersection of A, B and C are counted three times in $|A|+|B|+|C|$, but subtracted three times in $-|A \cap B| - |A \cap C| - |B \cap C|$. So, these elements are not counted in (3.1). Hence, in order to determine $|A \cup B \cup C|$, the number of elements in $A \cap B \cap C$ must be added to (3.1). This completes the proof of part Item (ii). □

Venn diagrams can be very helpful when using the inclusion-exclusion principle (cf. Example 1.1.37 on page 19 and Exercise 1.13).

3.2 Permutations

Suppose there are three vacancies in a company and three people running for those jobs. The product rule can be used to determine in how many ways the jobs can be divided over the applicants. For the first job, we can select one of the three applicants. Then, for the second job, there are two applicants left, and the last candidate will take the last job. Thus, there are $3 \times 2 \times 1 = 6$ ways in which the vacancies and applicants can be matched.

In the previous example, the number of orderings of the three candidates is calculated. We introduce a notation which turns out to be very convenient when counting the number of orderings. For all positive integers, $n!$ is defined as $n! = n \cdot (n-1) \cdots 2 \cdot 1$; $n!$ is pronounced as "n factorial". In several expressions it is convenient to define $0! = 1$.

Definition 3.2.1 (permutation)**.** A *permutation* of n distinct objects x_1, x_2, ..., x_n is an ordering of these n objects.

Thus, in the example above, there are 6 permutations of the three applicants. The following theorem generalizes this idea.

Theorem 3.2.2. The number of permutations of n distinct objects is equal to $n!$.

Proof. By convention, the theorem holds in case $n = 0$, since $0! = 1$, and 0 elements can be ordered in 1 way: the empty sequence.
If $n \geq 1$, there are n ways to select the first object. For each of these selections, there are $n-1$ possible choices for the second object. So, by the product rule, there are $n(n-1)$ ways to select the first two objects. For each choice of the first two objects, there are $n-2$ possibilities to take the third object, which yields (again by the product rule) $n(n-1)(n-2)$ ways to select the first three objects. Continuing this argument up to the last object, we obtain that there are $n(n-1)(n-2)\cdots 1$ ways to order all n objects. By definition, this number is equal to $n!$. □

Note that the given proof of Theorem 3.2.2 can be formalized into a proof by induction.

Now consider the case that we have more elements available than needed. For example, there are more applicants than jobs.

Example 3.2.3. Assume there are 4 jobs and 7 applicants. Suppose we first choose a candidate for the first job. This can be done in 7 ways. Now, for the second job, there are 6 applicants left. Thus, there are 6 ways in which we can choose the candidate for the second job. We therefore have $7 \cdot 6 = 42$ ways to select the first two job candidates. For the third job there are 5 applicants left, and for the fourth job 4. So we have $7 \cdot 6 \cdot 5 \cdot 4 = 840$ ways to select four people from the group of seven and match them to different jobs.

The following theorem generalizes the idea of Example 3.2.3. First we give the definition of an r-permutation.

Definition 3.2.4 (r-permutation)**.** Let S be a set with n elements and $0 \leq r \leq n$. An r-permutation (of elements of S) is a permutation of r distinct elements of S.
The number of r-permutations of a set of n elements is denoted by $P(n, r)$.

In Example 3.2.3 we determined the number of 4-permutations of the set of 7 applicants. So $P(7,4)=840$. The following theorem provides a general expression for $P(n,r)$.

Theorem 3.2.5. let S be a set with n elements and $0 \leq r \leq n$. Then $P(n,r)=\dfrac{n!}{(n-r)!}$.

Proof. Let S be a set with n elements and $0 \leq r \leq n$. By convention, the theorem holds in case $r=0$, since $\frac{n!}{(n-0)!}=1$, and 0 elements can be ordered in 1 way: the empty sequence. If $r \geq 1$, there are n ways to select the first element of S. For each of these selections, there are $n-1$ possible choices for the second element. So, by the product rule, there are $n(n-1)$ ways to select the first two elements. For each choice of the first two elements of S, there are $n-2$ possibilities to take the third element, which yields (again by the product rule) $n(n-1)(n-2)$ ways to select the first three elements. Continuing this argument up to r elements, we obtain that there are

$$P(n,r)=n(n-1)(n-2)\cdots(n-r+1) \tag{3.2}$$

ways to order r arbitrarily chosen elements of S. Note that the expression on the right-hand side contains exactly r factors.
Now it remains to show that the right-hand side in (3.2) is equal to $\frac{n!}{(n-r)!}$. This can be done by a straightforward calculation. First we multiply the right-hand side in (3.2) by the fraction $\frac{(n-r)!}{(n-r)!}$, which is equal to 1, and obtain

$$P(n,r)=n(n-1)(n-2)\cdots(n-r+1)\cdot\frac{(n-r)(n-r-1)\cdots 2\cdot 1}{(n-r)(n-r-1)\cdots 2\cdot 1}. \tag{3.3}$$

Note that the numerator of this product equals $n!$ and the denominator equals $(n-r)!$. Hence, $P(n,r)=\dfrac{n!}{(n-r)!}$. □

Example 3.2.6. Ten senior teams and thirteen junior teams participate in a volleyball tournament. At the end of the tournament, three different prizes will be given to the best senior teams and five different prizes to the best junior teams. In how many ways can the eight prizes be allocated?
Well, the senior prizes can be allocated in $P(10,3)$ ways. For each of these allocations, the junior prizes can be divided in $P(13,5)$ ways. Therefore, by the product rule, the eight different prizes can be allocated in $P(10,3)\cdot P(13,5)$ ways. By Theorem 3.2.5, this number is equal to $\frac{10!}{7!}\cdot\frac{13!}{8!}=111,196,800$.

3.3 Combinations

Up to now, we have considered orderings of elements where the ordering (x_1,x_2) differs from (x_2,x_1). Often, the order in which these objects are chosen is not important. Consider for example a class that chooses two representatives, or someone who wants to select five snacks for a party. Then the order in which they are chosen does not matter. In these situations, a selection of objects is called a combination.

Definition 3.3.1. Let S be a set with n elements and $0 \leq r \leq n$. An r-combination is a selection of r elements from S.
The number of r-combinations of a set of n elements is denoted by $\binom{n}{r}$.
The expression $\binom{n}{r}$ is called a *binomial coefficient* and is pronounced as "n choose r".

Note that if S is a set with n elements, then a selection of r elements from S corresponds to a subset with r elements. Hence we have the following result.

Theorem 3.3.2. Let S be a set with n elements and $0 \leq r \leq n$. Then there are $\displaystyle\binom{n}{r}$ subsets with r elements.

The next theorem provides an expression for $\binom{n}{r}$.

Theorem 3.3.3. Let S be a set with n elements and $0 \leq r \leq n$. Then $\displaystyle\binom{n}{r} = \frac{n!}{r!(n-r)!}$.

Proof. Let S be a set with n elements and $0 \leq r \leq n$.
By convention, the theorem holds in case $r = 0$, since $\frac{n!}{0!(n-0)!} = 1$, and 0 elements can be selected in 1 way: the empty selection.
If $r \geq 1$, then we obtain from Theorem 3.2.5 that there are $P(n,r) = \frac{n!}{(n-r)!}$ *ordered* selections (r-permutations) of r elements. By Theorem 3.2.2, each r-combination corresponds to $r!$ r-permutations, since the r selected elements of an r-combination can be ordered in $r!$ ways. Therefore, the number of r-combinations is $\frac{P(n,r)}{r!}$. This proves the theorem. □

Example 3.3.4. Consider a sports event where 48 athletes battle for the win. After an individual qualification race, three of them will race together to determine who wins which prize. There are $\binom{48}{3} = \frac{48!}{3!45!} = 17,296$ ways in which the athletes for the final race can be selected. In the final, there are $P(3,3) = \frac{3!}{0!} = 6$ ways in which the three finalists can be ordered first, second and third. So, by the product rule, there are $17,296 \cdot 6 = 103,776$ ways in which a first, second and third best can be chosen from the 48 athletes. This last number can also be calculated directly by evaluating $P(48,3) = \frac{48!}{45!} = 103,776$: simply select a first, second and third prize winner from the 48 participating athletes.

Example 3.3.5. Consider a standard deck of 52 cards, consisting of 13 hearts, 13 spades, 13 clubs and 13 diamonds, each color containing the values $2, \ldots, 10$, jack, queen, king and ace. A *full house* is a selection of 5 cards, three of them having the same value and the other two also having the same value. For example three sevens and a pair of jacks. We calculate the number of different full houses, if also the "colors" count, e.g., a triple sevens of spades, hearts and clubs is considered different from a triple sevens of spades, hearts and diamonds.

Well, we can first choose the value of the triple card in a full house. This can be done in $\binom{13}{1}$ ways (choose one value out of the 13 possible values). For each choice of the value of the triple card, we can choose the colors of the triple card in $\binom{4}{3}$ ways (choose 3 colors out of 4). So, by the product rule, there are $\binom{13}{1}\binom{4}{3}$ ways to choose the triple card. For each choice of a triple card, there are $\binom{12}{1}$ choices for the value of the pair (choose one value out of the remaining 12 values), and for each choice of this value, there are $\binom{4}{2}$ possibilities to choose the colors of the pair. Therefore, the number of full houses is equal to $\binom{13}{1}\binom{4}{3}\binom{12}{1}\binom{4}{2} = 3,744$.

The following relations lead to Pascal's triangle.

Theorem 3.3.6. Let S be a set with n elements and $1 \leq r \leq n$. Then

(i) $\displaystyle\binom{n}{0} = 1$ and $\displaystyle\binom{n}{n} = 1$.

(ii) $\displaystyle\binom{n}{r} = \binom{n}{n-r}$.

(iii) $\displaystyle\binom{n+1}{r} = \binom{n}{r-1} + \binom{n}{r}$.

Proof. The statements (i) and (ii) are easy to prove using Theorem 3.3.3. Also (iii) can be proved using this theorem, see Exercise 3.7. $\square$

We can arrange the binomial coefficients in a well-known scheme, called Pascal's triangle. The $(n+1)$-st line in Pascal's triangle contains the binomial coefficients $\binom{n}{r}$, for $r = 0, 1, \ldots, n$. In Figure 3.1 the first 5 rows are given. The triangle on the right of this figure contains the values of the corresponding binomial coefficients on the left. Note how the relations in Theorem 3.3.6 determine the structure of this scheme.

$$\begin{array}{ccccccccc}
 & & & & \binom{0}{0} & & & & \\
 & & & \binom{1}{0} & & \binom{1}{1} & & & \\
 & & \binom{2}{0} & & \binom{2}{1} & & \binom{2}{2} & & \\
 & \binom{3}{0} & & \binom{3}{1} & & \binom{3}{2} & & \binom{3}{3} & \\
\binom{4}{0} & & \binom{4}{1} & & \binom{4}{2} & & \binom{4}{3} & & \binom{4}{4}
\end{array}
\qquad
\begin{array}{ccccccccc}
 & & & & 1 & & & & \\
 & & & 1 & & 1 & & & \\
 & & 1 & & 2 & & 1 & & \\
 & 1 & & 3 & & 3 & & 1 & \\
1 & & 4 & & 6 & & 4 & & 1
\end{array}$$

Figure 3.1: The top five rows of Pascal's triangle.

Pascal's triangle has many beautiful structures. For example the sum of the binomial coefficients in the n-th line of the triangle is equal to 2^n, as we will see in Example 3.3.9.

Example 3.3.7. Consider a path in Pascal's triangle from the top $\binom{0}{0}$ to the coefficient $\binom{n}{k}$ consisting of n steps, each of which is either of the type "down left" or "down right". For example, a path from $\binom{0}{0}$ to $\binom{4}{3}$ of type "down right, down right, down left, down right" passes the coefficients $\binom{1}{1}$, $\binom{2}{2}$, $\binom{3}{2}$ and $\binom{4}{3}$ respectively. The number of such paths from $\binom{0}{0}$

to $\binom{n}{k}$ turns out to be exactly $\binom{n}{k}$. This is because such a path consists of exactly k "down right" steps and $n-k$ "down left" steps. The order in which these steps are taken determines which path from $\binom{0}{0}$ to $\binom{n}{k}$ is considered. There are $\binom{n}{k}$ possibilities to choose which of the n steps will be k "down right" steps (the other $n-k$ steps will then be "down left"). So there are exactly $\binom{n}{k}$ paths from $\binom{0}{0}$ to $\binom{n}{k}$.

Binomial coefficients are also useful if one wants to expand the expression $(x+y)^n$ for some $n \in \mathbb{N}$. For example, if we want to expand $(x+y)^3$ without using binomial coefficients we would get:

$$\begin{aligned}
(x+y)^3 &= (x+y)(x+y)^2 \\
&= (x+y)(x^2+xy+xy+y^2) \\
&= (x+y)(x^2+2xy+y^2) \\
&= x^3+2x^2y+xy^2+x^2y+2xy^2+y^3 \\
&= x^3+3x^2y+3xy^2+y^3.
\end{aligned}$$

Note however that the coefficients of x^3, x^2y, xy^2 and y^3 (namely 1, 3, 3 and 1) are precisely the binomial coefficients $\binom{3}{k}$, for $k = 0$, 1, 2, 3 respectively (cf. fourth row in Figure 3.1). So, we have

$$(x+y)^3 = x^3+3x^2y+3xy^2+y^3 = \sum_{k=0}^{3} \binom{3}{k} x^{3-k}y^k.$$

The following theorem generalizes this idea.

Theorem 3.3.8 (Newton's binomial theorem)**.** Let x, $y \in \mathbb{R}$ and $n \in \mathbb{N} \cup \{0\}$. Then

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^{n-k}y^k.$$

Proof. If $n = 0$, the theorem holds since, by convention, the left- and right-hand side are both equal to 1.
If $n \geq 1$, we write $(x+y)^n = (x+y)(x+y)\cdots(x+y)$. If we expand this product of n factors, we obtain a sum of $n+1$ terms of the form $x^{n-k}y^k$, where $k = 0, 1, \ldots, n-1, n$. So it remains to show that the coefficient of each term $x^{n-k}y^k$ is equal to $\binom{n}{k}$.
Well, to obtain a term $x^{n-k}y^k$ we must, when expanding the product, choose k times the y from the n factors $(x+y)$ (and from the remaining $n-k$ factors $(x+y)$ we must choose the x). So there are $\binom{n}{k}$ ways in the expansion to create a term $x^{n-k}y^k$: choose k from n factors to determine the factors from which the y is selected. Thus, the coefficient of $x^{n-k}y^k$ is equal to $\binom{n}{k}$. □

For example, the coefficient of x^3y^9 in the expansion of $(x+y)^{12}$ is $\binom{12}{9} = 220$.

The binomial theorem can also be used to compute certain sums of similar binomial coefficients, as can be seen in the following examples.

Example 3.3.9. Applying the binomial theorem for $x = 1$ and $y = 1$ yields

$$(1+1)^n = \sum_{k=0}^{n} \binom{n}{k} 1^{n-k} \cdot 1^k = \sum_{k=0}^{n} \binom{n}{k}.$$

So, $\displaystyle\sum_{k=0}^{n} \binom{n}{k} = 2^n$.

In expanded form:

$$\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \ldots + \binom{n}{n} = 2^n.$$

Applying the binomial theorem for $x = 1$ and $y = -1$ yields

$$(1-1)^n = \sum_{k=0}^{n} \binom{n}{k} 1^{n-k} \cdot (-1)^k = \sum_{k=0}^{n} (-1)^k \binom{n}{k}.$$

So: $\displaystyle\sum_{k=0}^{n} (-1)^k \binom{n}{k} = 0^n$. In case $n > 0$, we get $\displaystyle\sum_{k=0}^{n} (-1)^k \binom{n}{k} = 0$.

In expanded form:

$$\binom{n}{0} - \binom{n}{1} + \binom{n}{2} - \ldots + (-1)^n \binom{n}{n} = 0.$$

Note that $\displaystyle\sum_{k=0}^{n} (-1)^k \binom{n}{k} = 0^n$ also holds for $n = 0$, since 0^0 is defined as 1.

3.4 Exercises

Exercise 3.1. How many strings of 10 letters of the alphabet $\{A, B, \ldots, Z\}$ can be made if:

a) letters may appear more than once?
b) letters may appear more than once, but at least one of the first two letters in the string must be selected from the set $\{A, B, C, D\}$?

Exercise 3.2. Determine $|A \cup B \cup C|$ when $|A| = 50$, $|B| = 500$, and $|C| = 5000$, and

a) $A \subseteq B \subseteq C$.
b) $A \cap B = A \cap C = B \cap C = \emptyset$.
c) $|A \cap B| = |A \cap C| = |B \cap C| = 3$ and $|A \cap B \cap C|$ = 1.

Exercise 3.3. Let $A = \{1, 2, 3, \ldots, n\}$ and $0 \leq r \leq n$.
In how many ways can we select r elements of A if

a) repetition is allowed (elements can be selected more than once) and the order in which the elements are selected matters?
b) repetition is not allowed (elements can be selected at most once) and the order in which the elements are selected matters?
c) repetition is not allowed and the order does not matter?
d) Prove that the number of subsets of A is equal to 2^n.

Exercise 3.4. Let $S = \{1, 2, 3, \ldots, 28, 29, 30\}$. How many subsets A of S satisfy

a) $|A| = 5$?
b) $|A| = 5$ and the smallest element in A is 5?
c) $|A| = 5$ and the smallest element in A is less than 5?

Suppose someone solves c) as follows:
Take any element in S less than 5; this can be done in $\binom{4}{1}$ ways.
Now, for each choice of this element, the other 4 elements of A can be chosen arbitrarily from the remaining 29 elements of S, which can be done in $\binom{29}{4}$ ways.
Therefore, by the product rule, the answer is: $\binom{4}{1}\binom{29}{4}$.

d) Explain why the reasoning above is wrong.

Exercise 3.5. Consider 12 different books of three different authors: 3 books of the first author, 4 of the second author and 5 of the third author. In how many ways can these books be ordered on a shelf if

a) there are no restrictions?
b) books of the third author must be placed on the right-hand side of the shelf, and the authors of the first seven books on the shelf must alternate?

c) books of the same author must be placed together?

d) In how many ways can these 12 books be divided among 4 children, such that they get 3 books each?

Exercise 3.6. Suppose there have been elections and a new government has to be formed. There are twelve different positions, the candidates are 10 men and 8 women. Determine the number of ways in which the government can be formed in each of the following cases.

a) There are no restrictions.

b) There must be 6 men and 6 women in the government.

c) There must be an even number of women in the government.

Exercise 3.7. Prove Theorem 3.3.6.

Exercise 3.8.

a) Determine the coefficient of x^5y^3 in $(x+y)^8$.

b) Determine the coefficient of x^5y^3 in $(2x+3y)^8$.

c) Prove that $\binom{n}{0} + 2\binom{n}{1} + 2^2\binom{n}{2} + \cdots + 2^n\binom{n}{n} = 3^n$.

d) Prove that $2^n\binom{n}{0} - 2^{n-1}\binom{n}{1} + 2^{n-2}\binom{n}{2} - \cdots + (-1)^n\binom{n}{n} = 1$.

TERMINOLOGY AND TRANSLATIONS

Terminology

In mathematics terminology is not as consistent as one could hope. The table below gives notions we introduced with possible variants.

Notion	Explanation / Variant
$\mathbb{N}$	often $\mathbb{N}$ contains 0 as well
size of a (finite) set	cardinality
$[a, b)$ and $[a, \infty)$	$[a, b[$ and $[a, \rightarrow\rangle$
supremum	least upper bound (lub)
infimum	greatest lower bound
$\subseteq$	$\subset$ (as in $A \subset A$)
$A - B$	$A \setminus B$ or $A \cap \overline{B}$
$\neg p$	not p or $\sim p$
$\forall$	official term: universal quantifier
$\exists$	official term: existential quantifier
$\binom{n}{r}$	$C(n, r)$

Translations English-Dutch

English	Dutch
Binomial coefficient	Binomiaalcoëfficient
Binomial Theorem	Binomiaalstelling
Bounded interval	Begrensd interval
Cardinality	Cardinaliteit
Combination	Combinatie
Connective	Connectief
Contradiction	Tegenspraak

English	Dutch
Counterexample	Tegenvoorbeeld
Difference	Verschil
Disjoint	Disjunct
Empty set	Lege verzameling
Existential quantifier	Existentiële kwantor
Factorial	Faculteit
False	Onwaar
Finite set	Eindige verzameling
Inclusion-exclusion principle	Principe van inclusie en exclusie
Induction hypothesis	Inductieveronderstelling
Infimum	Infimum
Infinite set	Oneindige verzameling
Integer	Integer; geheel getal
Intersection	Doorsnede
Irrational	Irrationaal
Logical implication	Logische implicatie; geldig gevolg
Lower bound	Ondergrens
Mathematical induction	Volledige inductie
n choose k	n boven k
Natural number	Natuurlijk getal
Nonnegative	Niet-negatief
Nonpositive	Niet-positief
Odd	Oneven
Perfect square	Kwadraat
Permutation	Permutatie
Predicate	Predikaat
Prime	Priemgetal
Proof by contradiction	Bewijs uit het ongerijmde
Proper subset	Echte (stricte) deelverzameling
Proposition	Propositie; bewering
Quantifier	Kwantor
Quantified statement	Bewering met kwantoren
Rational number	Rationaal getal
Real number	Reëel getal

English	Dutch
Set	Verzameling
Subset	Deelverzameling
Summation	Sommatie
Supremum	Supremum
Tautology	Tautologie
Truth table	Waarheidstabel
Unbounded interval	Onbegrensd interval
Union	Vereniging
Universal quantifier	Universele kwantor
Universal set	Universum
Upper bound	Bovengrens
Venn diagram	Venn diagram

Translations Dutch-English

Dutch	English
Begrensd interval	Bounded interval
Bewering met kwantoren	Quantified statement
Bewijs uit het ongerijmde	Proof by contradiction
Binomiaalcoëfficient	Binomial coefficient
Binomiaalstelling	Binomial Theorem
Bovengrens	Upper bound
Cardinaliteit	Cardinality
Combinatie	Combination
Connectief	Connective
Deelverzameling	Subset
Disjunct	Disjoint
Doorsnede	Intersection
Echte (stricte) deelverzameling	Proper subset
Eindige verzameling	Finite set
Existentiële kwantor	Existential quantifier
Faculteit	Factorial
Inductieveronderstelling	Induction hypothesis

Dutch	**English**
Infimum	Infimum
Integer; geheel getal	Integer
Irrationaal	Irrational
Kwadraat	Perfect square
Kwantor	Quantifier
Lege verzameling	Empty set
Logische implicatie; geldig gevolg	Logical implication
n boven k	n choose k
Natuurlijk getal	Natural number
Niet-negatief	Nonnegative
Niet-positief	Nonpositive
Onbegrensd interval	Unbounded interval
Ondergrens	Lower bound
Oneindige verzameling	Infinite set
Oneven	Odd
Onwaar	False
Permutatie	Permutation
Predikaat	Predicate
Priemgetal	Prime
Principe van inclusie en exclusie	Inclusion-exclusion principle
Propositie; bewering	Proposition
Rationaal getal	Rational number
Reëel getal	Real number
Sommatie	Summation
Supremum	Supremum
Tautologie	Tautology
Tegenspraak	Contradiction
Tegenvoorbeeld	Counterexample
Universele kwantor	Universal quantifier
Universum	Universal set
Venn diagram	Venn diagram
Vereniging	Union
Verschil	Difference
Verzameling	Set

Dutch	English
Volledige inductie	Mathematical induction
Waarheidstabel	Truth table

ANSWERS AND HINTS

Chapter 1

1.1 Only the sets in a) and c) are equal.

1.2 a) $A = \{0, 2\}$. b) $A = \{2, 2\frac{1}{2}, 3\frac{1}{3}, 5\frac{1}{5}, 7\frac{1}{7}\}$.
c) $A = \{0, 2, 12, 36, 80\}$.

1.3 E.g. $X = \emptyset$, $Y = \{\emptyset\}$, $Z = \{\{\emptyset\}\}$, or $X = \{1\}$, $Y = \{\{1\}\}$, $Z = \{\{\{1\}\}\}$.

1.4 All except f) are true.

1.5 a) $(0, 5)$.
b) $[4, 6)$.
c) Not an interval: the set contains the elements 1 and 5, but not 3.
d) $[4, 6)$.

1.6 a) min$(A) = 2$, max$(A) = 3$, inf$(A) = 2$, sup$(A) = 3$.
b) min(A) does not exist, max$(A) = 3$, inf$(A) = 2$, sup$(A) = 3$.
c) None of the minimum maximum, infimum and supremum exist.
d) min$(A) = \frac{1}{2}$, max(A) does not exist, inf$(A) = \frac{1}{2}$, sup$(A) = 1$.
e) min$(A) = 0$, max$(A) = 2$, inf$(A) = 0$, sup$(A) = 2$.
f) min(A) and max(A) do not exist, inf$(A) = 0$, sup(A) does not exist.

1.7 a) 6. b) 21. c) 1001. d) 1.

1.8 a) $\{1, 2, 3, 5\}$. b) $\{1, 3, 4, 5, 6, 7, 8, 9, 10\}$. c) A.
d) $\{1, 3, 4, 5, 6, 7, 8, 9, 10\}$. e) $\{4, 8\}$. f) $\{1, 2, 3, 4, 5, 8\}$.
g) $\emptyset$. h) $\{2, 4, 8\}$.

1.9 a) True. b) False. c) False. d) True. e) True. f) False.

1.10 a) B. b) D. c) $\{12n \mid n \in \mathbb{Z}\}$.
d) $\{0, 2, -2, 3, -3, 4, -4, 6, -6, 8, -8, 9, -9 \ldots\}$.

1.11 Only d) and f) are false.

1.12 a) $[7, 70)$. b) $[3, 70)$. c) $[7, 30)$. d) $[1, 100)$. e) $\emptyset$.

1.13 20 students.

1.14 a) $r \to q$. b) $q \to p$. c) $q \leftrightarrow s$. d) $\neg r \to s$. e) $(r \wedge s) \to (p \wedge q)$.

1.15 a) $m = 3$, $n = 6$. b) $m = 3$, $n = 9$. c) $m = 18$, $n = 9$. d) $m = 4$, $n = 9$. e) $m = 4$, $n = 9$.

1.16 a) $(p \wedge \neg q) \vee (\neg p \wedge q)$. b) $\neg(p \wedge q) \wedge \neg(\neg p \wedge \neg q)$.

1.17 See Definition 1.2.8 and Table 1.3.

1.18 See Definition 1.2.13 and Example 1.2.14.

1.19 a) Tautology. b) Counterexample: $p = 0$, $q = 1$. c) Counterexample: $p = 0$, $q = 1$, $r = 0$. d) Tautology.

1.20 For example $A = \{1\}$, $B = \{1, 2\}$ and $C = \{1, 3\}$.

1.21 a) True.
b) False. Counterexample: $A = \{1\}$, $B = \{1\}$, $C = \emptyset$.
c) True.
d) True.
e) False. Counterexample: $A = \{1\}$, $B = \emptyset$, $C = \emptyset$, $D = \{1\}$.

1.22 The cases c), f), g), h) and i) are true.

1.23 a) True. b) False.
c) They are negations of each other.

1.24 a) $\forall x\ (x \in A \to x \in B) \wedge \exists y\ (y \in B \wedge y \notin A)$.
b) $\exists x\ (x \in A \wedge x \notin B)$.
c) $\exists x\ (x \in A \wedge x \notin B) \vee \forall x\ (x \in A \leftrightarrow x \in B)$.
d) $\neg \exists x\ (x \in A \wedge x \in B)$.

1.25 a) True. b) False. c) True.

1.26 a) $\exists (d \in D)\ (d \leq -1)$.
b) $\exists \varepsilon > 0\ \big(\forall \delta > 0\ \big(\exists x \in R\ \big(|x| < \delta \wedge x^2 \geq \varepsilon\big)\big)\big)$.

Chapter 2

2.1 Use the proof technique of Example 2.1.1.

2.2 a) Hint: $\sqrt{x^2} = |x|$. b) Hint: $x^{\frac{2}{3}} = |x|^{\frac{2}{3}}$.

2.3 a) $a = -1$ and $b = 0$. b) $x = 0$.

2.4 a) True. Give a direct proof using Definition 2.1.2.
b) False. Give a proof by verifying that all possible combinations of m and n fail.
c) True. Give a direct proof (write $n = 2k$).
d) True. Give a proof by contradiction (suppose that n^3 is even and n is odd).
e) True. Give a direct proof, distinguishing the cases n even and n odd.
f) True. Give a proof by contradiction, distinguishing the cases m even and n even.

2.5 a) False. Counterexample: 2 and 3 are prime, as well as $2 + 3 = 5$.
b) True, only for $n = 2$.
Prove for $n > 2$ that $n^2 - 1$ is not a prime (write $n^2 - 1 = (n-1)(n+1)$).
c) False. Prove that n or $n+2$ or $n+4$ is divisible by 3 (distinguish the three cases where the remainder of n upon division by 3 is 0, 1 or 2).

2.6 a) Give a direct proof, distinguishing the cases n even and n odd.
b) Hint: write any number $n \in \mathbb{N}$ as $n = 10k + l$, and distinguish 10 cases.
c) Use Exercise 2.4 e):
$(2n+1)^2 = 4n^2 + 4n + 1 = 4n(n+1) + 1 = 4 \cdot 2k + 1 = 8k + 1.$
d) Give a proof by contradiction; distinguish the cases (a even, b odd), (a odd, b even) and (a odd, b odd).

2.7 a) True. Give a direct proof (the average of p and q is $\frac{p+q}{2}$).
b) False. Counterexample: $\sqrt{2}$ and $-\sqrt{2}$.
c) True. Give a proof by contradiction.

2.8 a) Follow Example 2.3.2. $a^2 = 3b^2$ implies that a is divisible by 3 (see hint in exercise). Now substitute $a = 3k$ in the equation $a^2 = 3b^2$ and deduce that also b must be divisible by 3. Finally, derive a contradiction.
b) Take $x = \frac{a+b}{2}$ (the average of a and b). Prove that $a < x < b$.
c) $x = \frac{116}{90} \in \mathbb{Q}$.

2.9 a) See Example 2.4.2; consider the 6 pigeonholes $\{1, 21\}$, $\{3, 8\}$, $\{7, 15\}$, $\{16, 17\}$, $\{20, 24\}$ and $\{22\}$.
b) Take, for example, $A = \{1, 3, 7, 16, 20, 22\}$.

2.10 a) Follow the proof of Example 2.6.2.
((2.6) becomes: $k^2 + (2(k+1) - 1) = k^2 + 2k + 1 = (k+1)^2$).
b) Follow the proof of Example 2.6.2. In (2.6) show that $\frac{k(k+1)(2k+1)}{6} + (k+1)^2 = \frac{(k+1)(k+2)(2k+3)}{6}$. Note Remarks 2.6.3 (2).
c) Follow the proof of Example 2.6.2.
In (2.6) show that $2 + (k-1)2^{k+1} + (k+1)2^{k+1} = 2 + k \cdot 2^{k+2}$ by subtracting 2 from both sides and then dividing by 2^{k+1}.

d) Follow the proof of Example 2.6.2. In (2.6) show that $\frac{1-r^{k+1}}{1-r}+r^{k+1}=\frac{1-r^{k+2}}{1-r}$ by multiplying both sides by $1-r$.

2.11 a) $F_6=8$, $F_7=13$.

b) Follow the proof of Example 2.6.2.
In (2.6) show that $F_{k+2}-1+F_{k+1}=F_{k+3}-1$ by applying (2) to $n=k+3$.

c) Follow the proof of Example 2.6.2.
In (2.6) show that $F_kF_{k+1}+F_{k+1}^2=F_{k+1}F_{k+2}$ (divide both sides by F_{k+1} and apply (2) to $n=k+2$).

d) In the induction step show that $F_{k+2}F_k-F_{k+1}^2=(-1)^{k+1}$
(write $(-1)^{k+1}=-(-1)^k=-\left(F_{k+1}F_{k-1}-F_k^2\right)$ and apply (2) to $n=k+2$).

2.12 a) Follow the proof of Example 2.6.5. In the induction step show that $2^{2k+3}+1$ is divisible by 3 (write $2^{2k+3}+1=2^2\cdot 2^{2k+1}+1=4(3l-1)+1=3(4l-1)$).

b) Follow the proof of Example 2.6.5. In the induction step show that $7^{k+3}+8^{2k+3}$ is divisible by 57 (write $7^{k+3}+8^{2k+3}=7\cdot 7^{k+2}+64\cdot 8^{2k+1}=7\cdot 7^{k+2}+64(57l-7^{k+2})=57(64l-7^{k+2})$).

2.13 a) In the induction step show that $a_{n+1}>0$ and $a_{n+1}<\sqrt{3}$
(write $a_{n+1}=\sqrt{a_n\sqrt{3}}>\sqrt{0\sqrt{3}}=0$ and $a_{n+1}=\sqrt{a_n\sqrt{3}}<\sqrt{\sqrt{3}\sqrt{3}}=\sqrt{3}$).

b) Use part a): $a_{n+1}=\sqrt{a_n\sqrt{3}}>\sqrt{a_na_n}=a_n$.

2.14 a) Distinguish the cases $x\ge 0$ and $x<0$ (use $|x|=x$ if $x\ge 0$ and $|x|=-x$ if $x<0$).

b) Distinguish the cases (x_1, $x_2\ge 0$), ($x_1\ge 0$, $x_2<0$), ($x_1<0$, $x_2\ge 0$) and (x_1, $x_2<0$).

c)
$$\begin{aligned}|x_1+x_2|^2=(x_1+x_2)^2&=x_1^2+x_2^2+2x_1x_2=|x_1|^2+|x_2|^2+2x_1x_2\\&\le|x_1|^2+|x_2|^2+2\,|x_1x_2|=|x_1|^2+|x_2|^2+2\,|x_2|\,|x_2|\\&=(|x_1|+|x_2|)^2.\end{aligned}$$
Since both $|x_1+x_2|$ and $|x_1|+|x_2|$ are nonnegative, it follows that $|x_1+x_2|\le|x_1|+|x_2|$.

d) The basis step follows from c). In the induction step, apply c) and the induction hypothesis:
$$\left|\sum_{i=1}^{k+1}x_i\right|=\left|\left(\sum_{i=1}^{k}x_i\right)+x_{k+1}\right|\le\left|\sum_{i=1}^{k}x_i\right|+|x_{k+1}|\le\left(\sum_{i=1}^{k}|x_i|\right)+|x_{k+1}|=\sum_{i=1}^{k+1}|x_i|.$$

2.15 The induction step does not hold for $k=1$.

Chapter 3

3.1 a) 26^{10}.

b) $4\cdot 26^9+4\cdot 26^9-4\cdot 4\cdot 26^8$ ($=192\cdot 26^8$).

3.2 a) 5000. b) 5550. c) 5542.

3.3 a) n^r. b) $P(n,r) = \frac{n!}{(n-r)!}$. c) $\binom{n}{r}$.

d) Each $B \subseteq A$ can be constructed by deciding for each $x \in A$ whether $x \in B$ or $x \notin B$. So there are 2 choices for each element, which yield 2^n possibilities to construct a subset. Another way to compute this is making use of part c) and $\sum_{r=0}^{n} \binom{n}{r} = 2^n$ (cf. Example 3.3.9).

3.4 a) $\binom{30}{5}$. b) $\binom{25}{4}$. c) $\binom{29}{4} + \binom{28}{4} + \binom{27}{4} + \binom{26}{4}$ (or $\binom{30}{5} - \binom{26}{5}$).

d) With this reasoning, the subsets containing more than one element less than 5 are counted more than once. For example, the set $A = \{3, 4, 7, 13, 25\}$ is counted twice: once by first choosing 3 and then 4, 7, 13 and 25; and once by first choosing 4 and then 3, 7, 13 and 25.

3.5 a) $12!$. b) $4 \cdot 3 \cdot 3 \cdot 2 \cdot 2 \cdot 1 \cdot 1 \cdot 5! = 3! \cdot 4! \cdot 5!$.

c) $3! \cdot 3! \cdot 4! \cdot 5!$. d) $\binom{12}{3} \cdot \binom{9}{3} \cdot \binom{6}{3} \cdot \binom{3}{3}$.

3.6 a) $\frac{18!}{6!}$. b) $\binom{10}{6} \cdot \binom{8}{6} \cdot 12!$.

3.6 c) $\left(\binom{10}{10} \cdot \binom{8}{2} + \binom{10}{8} \cdot \binom{8}{4} + \binom{10}{6} \cdot \binom{8}{6} + \binom{10}{4} \cdot \binom{8}{8}\right) \cdot 12!$.

3.7 (i) $\binom{n}{0} = \frac{n!}{0!(n-0)!} = \frac{n!}{n!} = 1$; $\binom{n}{n} = \frac{n!}{n!(n-n)!} = \frac{n!}{n!} = 1$.

(ii) $\binom{n}{n-r} = \frac{n!}{(n-r)!(n-(n-r))!} = \frac{n!}{(n-r)!r!} = \binom{n}{r}$.

(iii)
$$\begin{aligned}\binom{n}{r-1} + \binom{n}{r} &= \frac{n!}{(r-1)!(n-(r-1))!} + \frac{n!}{r!(n-r)!} \\ &= \frac{n!}{(r-1)!(n-r+1)!} + \frac{n!}{r!(n-r)!} \\ &= \frac{r \cdot n!}{r!(n-r+1)!} + \frac{(n-r+1) \cdot n!}{r!(n-r+1)!} \\ &= \frac{r \cdot n! + (n-r+1) \cdot n!}{r!(n-r+1)!} = \frac{(n+1) \cdot n!}{r!(n-r+1)!} = \frac{(n+1)!}{r!(n-r+1)!} = \binom{n+1}{r}\end{aligned}$$

3.8 a) $\binom{8}{3}$. b) $2^5 \cdot 3^3 \cdot \binom{8}{3}$.

c) Use Newton's binomial theorem with $x = 1$ and $y = 2$.

d) Use Newton's binomial theorem with $x = 2$ and $y = -1$.

INDEX