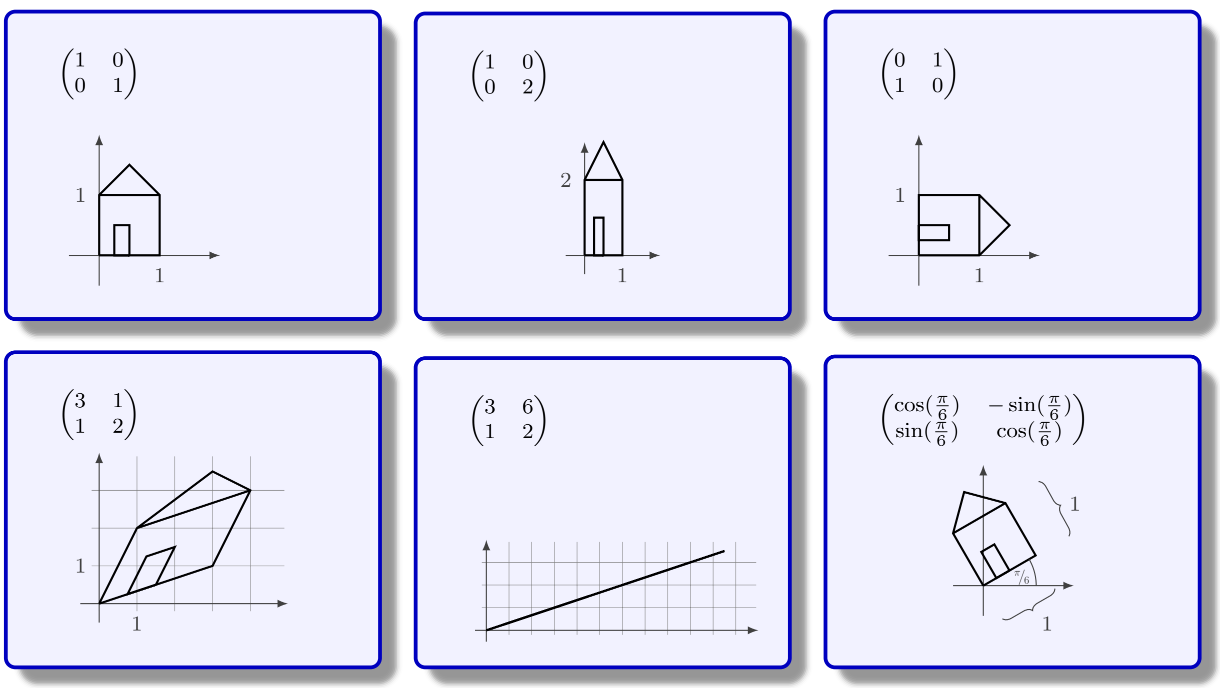
Foundations for Linear Algebra and Analysis

Marko Lindner and Anusch Taraz



TU Hamburg (TUHH)

preliminary version October 21, 2024

Contents

Chapter 1

Foundations

This chapter introduces the basic mathematical concepts that we will need in this course: sets, logic, numbers, sums, products, and functions. Moreover, we will learn how to organize our arguments in a concise manner: we will study how to write (short) mathematical proofs.

1.1 Sets

We start with the following definition:

Definition 1.1. set, element

A set is a collection of certain distinct objects. Every object x in a set S is called an element of S. We write $x \in S$ if x is an element of S, and $x \notin S$ if it is not.

One way to describe a set is by listing all elements in the set, for example $S := \{1, 4, 9\}$.

The colon : in front of the equality sign = in the joint symbol := means that we now define the previously unknown set S.

Alternatively, we can also define a set through the properties that characterize its elements:

S is defined as the set of all square numbers between 1 and 10.

But such a description may not be as precise as we want it. For example: What exactly is a "square number"? And, when we say "between 1 and 10", does this include 1 and 10? To keep such descriptions short and precise, the following notation is used throughout mathematics:

numbers

- $\mathbb{N}$ *is the set of all natural numbers* $1, 2, 3, \ldots$*;*
- $\mathbb{N}_0$ *is the set of all natural numbers together with zero:* $0, 1, 2, 3, \ldots$ *;*
- $\mathbb{Z}$ *is the set of all integers* $\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots$*;*
- $\mathbb{Q}$ *is the set of all rational numbers, thus the fractions* $\frac{p}{q}$ *with* $p \in \mathbb{Z}$ *and* $q \in \mathbb{N}$*;*
- $\mathbb{R}$ *is the set of all real numbers.*

Exercise 1.2. *Which of the following statements are true?*

$$\boxed{3 \in \mathbb{N}}, \qquad \boxed{12034 \in \mathbb{N}}, \qquad -1 \in \mathbb{N}, \qquad 0 \in \mathbb{N}, \qquad \boxed{0 \in \mathbb{N}_0}$$

$$\boxed{-1 \in \mathbb{Z}}, \qquad 0 \notin \mathbb{Z}, \qquad -2.7 \in \mathbb{Z}, \qquad \tfrac{2}{3} \in \mathbb{Z},$$

$$\boxed{\tfrac{2}{3} \in \mathbb{Q}}, \qquad \boxed{-3 \in \mathbb{Q}}, \qquad \boxed{-2.7 \in \mathbb{Q}}, \qquad \sqrt{2} \in \mathbb{Q},$$

$$\boxed{\sqrt{2} \in \mathbb{R}}, \qquad \sqrt{-2} \in \mathbb{R}, \qquad \boxed{-\tfrac{2}{3} \in \mathbb{R}}, \qquad \boxed{0 \in \mathbb{R}}.$$

We say that two sets are <u>*equal*</u>, if they contain the same elements. Here, it does not matter whether the descriptions are the same. In particular, the order of the elements does not matter, or whether an object is nominated several times as an element of the set: $\{1, 4, 9\} = \{9, 1, 4\} = \{9, 4, 1, 9, 1, 1\}$.

Definition 1.3. empty set, quantifiers $\forall$ and $\exists$

A set that does not contain any element is called the <u>empty set</u>. Therefore all empty sets are identical, and we thus speak of **the** *empty set and denote it by* $\varnothing$*.*

Moreover we introduce the notation $\forall$ *("for all") and* $\exists$ *("there exists"), and the colon* $:$ *inside a set stands for "for which it is true that" steht.*

Using these we can now describe sets in a very short and concise way:

Example 1.4. The set $A := \{x \in \mathbb{Z} \colon x^2 = 25\}$ is defined as the set of all integers x, whose square is equal to 25. Obviously, we can see that these are exactly the numbers -5 and 5. Moreover, note that

$$\begin{aligned} \{x \in \mathbb{Z} \colon x^2 = 25\} &= \{-5, 5\}, \\ \{x \in \mathbb{N} \colon x^2 = 25\} &= \{5\}, \\ \{x \in \mathbb{R} \colon x^2 = -25\} &= \varnothing. \end{aligned}$$

In other words, the equation $x^2 = 25$ has one or two solutions, depending on where (i.e. in which set of numbers) you are trying to solve it. And the equation $x^2 = -25$ has no real solution.

Example 1.5. The line

$$B := \{x \in \mathbb{N}\colon 1 \leq x \leq 10 \text{ and } \exists y \in \mathbb{N} \text{ with } y^2 = x\}$$

reads as follows: B is defined as the set of all natural numbers x for which it is true that they lie between 1 and 10 and for which there exists a natural number y, so that $y^2 = x$. In other words, these are again the square numbers between 1 and 10, so $B = \{1, 4, 9\}$. In fact, we can write this even shorter like this:

$$B = \{y^2 \colon y \in \{1, 2, 3\}\}$$

Example 1.6. The line

$$C := \{n \in \mathbb{N}\colon n \geq 2 \text{ and } \forall m \in \mathbb{N} \text{ with } 1 < m < n \text{ the number } m \text{ is not a divisor of } n\}$$

reads as follows: C is defined as the set of all natural numbers that are greater or equal than 2, which do not have a divisor that is greater than 1 and smaller than n. Hence $C = \{2, 3, 5, 7, 11, \ldots\}$, which is exactly the set of prime numbers. Let us check carefully that the number $n = 2$ is indeed an element of C: First it satisfies $n \geq 2$ and second all the numbers $m \in \mathbb{N}$ with $1 < m < 2$ are not a divisor of n (which really is true but might feel a bit strange, because there aren't any such numbers m at all).

Note: At first sight, writing and reading and understanding mathematical descriptions of sets as in the above examples might seem like a somewhat bizarre activity, but it is absolutely essential that you master this language because we will use it over and over again in this course.

Definition 1.7. absolute value of a real number

The absolute value of a number $x \in \mathbb{R}$ is defined by

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

Question 1.8. *Which of the following statements is correct?*

$$\boxed{|-3.14| = 3.14}, \quad \boxed{|3| = 3}, \quad \boxed{|-\tfrac{7}{5}| = \tfrac{7}{5}}, \quad -|-\tfrac{3}{5}| = \tfrac{3}{5}, \quad |0| \text{ is not defined.}$$

Theorem 1.9. two important properties of the absolute value

For two arbitrary numbers $x, y \in \mathbb{R}$ we have

a) $|x \cdot y| = |x| \cdot |y|$,

b) $|x + y| \leq |x| + |y|$.

Let's consider for example $x = 3$ and $y = -2$ and see whether the above statements are true:

a) $|3 \cdot (-2)| = |-6| = 6 = 3 \cdot 2 = |3| \cdot |-2|$, **b)** $|3 + (-2)| = |3 - 2| = 1 \leq 5 = |3| + |-2|$.

We also use the symbols $|\cdot|$ to denote the number of elements in a set, for example $|\{1,4,9\}| = 3$. The number of elements of a set is also called the cardinality of the set.

Finally, we use the following notation to describe the subsets of the real numbers. Let $a, b \in \mathbb{R}$. Then we define

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

Here we call $[a,b]$ a *closed interval* and (a,b) an *open interval*. The intervals $(a,b]$ and $[a,b)$ are called *half-open*.

In the case $a > b$, all of the above intervals are obviously empty. We also define the following unconstrained intervals:

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

1.2 Sums and products

A *sum* is what you get when you add two or more numbers. The numbers that are added are called *summand*. When we are adding so many numbers that we cannot list all of them explicitly, we can try to describe this by using the somewhat informal $\ldots$ symbol. Alternatively, we can use the shorter and more concise symbol $\sum$.

Here are some examples. When we write $1 + 2 + 3 + \ldots + n$, it should be pretty clear that we are talking about the sum of the natural numbers from 1 to n. But when we look at the sum

$$3 + 7 + 15 + \ldots + 127,$$

then maybe it is less clear which numbers we are actually talking about. Instead we write

$$\sum_{i=2}^{7} (2^i - 1).$$

For those who have done some programming, this can be read like a `for`-loop:

for-loop for the above sum

```
sum := 0;
for i:=2 to 7 do {
  sum := sum + (2^i-1);
}
```

For those who haven't met a for-loop yet, we can also describe it in words:

Between us: Increase the counter i from 2 to 7 in steps of size 1 compute $2^i - 1$ everytime and add everything together

counter:	$i = 2,$	*first summand:*	$2^i - 1 = 2^2 - 1 =$	$4 - 1 =$	3
counter:	$i = 3,$	*second summand:*	$2^i - 1 = 2^3 - 1 =$	$8 - 1 =$	7
counter:	$i = 4,$	*third summand:*	$2^i - 1 = 2^4 - 1 =$	$16 - 1 =$	15
counter:	$i = 5,$	*fourth summand:*	$2^i - 1 = 2^5 - 1 =$	$32 - 1 =$	31
counter:	$i = 6,$	*fifth summand:*	$2^i - 1 = 2^6 - 1 =$	$64 - 1 =$	63
counter:	$i = 7,$	*last summand:*	$2^i - 1 = 2^7 - 1 =$	$128 - 1 =$	127

Let us look at a few more examples:

Example 1.10.

$$\sum_{i=1}^{10} (2i - 1) = 1 + 3 + 5 + \ldots + 19 \stackrel{?}{=} 100$$

$$\sum_{i=-10}^{10} i = -10 - 9 - 8 - \ldots - 1 + 0 + 1 + \cdots + 8 + 9 + 10 \stackrel{?}{=} 0$$

Multiplication works very similarly. Here we multiply several <u>*factors*</u> to obtain a <u>*product*</u>, and for this we use the symbol $\prod$. For example:

$$\prod_{i=1}^{8} (2i) = (2 \cdot 1) \cdot (2 \cdot 2) \cdot (2 \cdot 3) \cdot \ldots \cdot (2 \cdot 8) \stackrel{?}{=} 10321920.$$

For the product of the first n natural numbers there is a special notation:

$$n! := \prod_{i=1}^{n} i = 1 \cdot 2 \cdot \ldots \cdot n$$

is called n <u>*factorial*</u>. Observe that we define $0! = 1$.

For these sums and products, the same rules apply as for sums and products that are written in the usual way. Here is an example for the distributive law:

$$2 \cdot \sum_{i=5}^{7} 2^i = 2\left(2^5 + 2^6 + 2^7\right) = 2^6 + 2^7 + 2^8 = \sum_{i=5}^{7} 2^{i+1} = \sum_{i=6}^{8} 2^i. \tag{1.1}$$

The transformation that happened at the last equality sign is called an *index shift*: start and end the counter i at a value that is one higher than before, but replace the term $i+1$ by the term i. This trick is useful to combine two sums that look different at first sight. Here is another example for this:

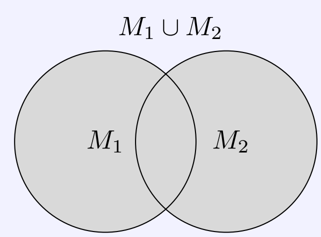
$$\sum_{i=1}^{10} 3^i - \sum_{i=1}^{10} 3^{i+1} = \sum_{i=1}^{10} 3^i - \sum_{i=2}^{11} 3^i = 3^1 + \left(\sum_{i=2}^{10} 3^i\right) - \left(\sum_{i=2}^{10} 3^i\right) - 3^{11} = 3^1 - 3^{11}. \quad (1.2)$$

1.3 Operations with sets

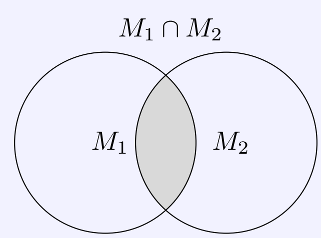
Consider two sets M_1 and M_2. How can they be combined to form a new set?

Definition 1.11. connecting sets

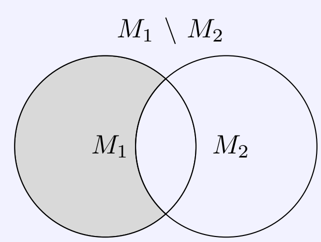
*The union $M_1 \cup M_2$ of two sets denotes the set whose elements are exactly those objects that are elements of M_1 **or** M_2.*



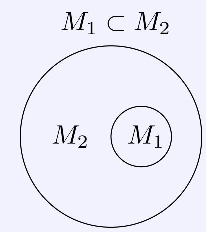
*The intersection $M_1 \cap M_2$ of two sets denotes the set whose elements are exactly those objects that are elements of M_1 **and** M_2.*



*Moreover $M_1 \setminus M_2$ denotes the set of all objects that are an element of M_1 **and not** an element of M_2.*



We write $M_1 \subset M_2$ if all elements of M_1 are also elements of M_2. In this case we call M_1 a <u>subset</u> of M_2. In particular this holds if $M_1 = M_2$ or if $M_1 = \varnothing$ and M_2 is an arbitrary set.



Question 1.12. *Which of the following statements are true?*

$$\{1,3\} \cup \{2,4\} = \{1,2,4\}, \qquad \boxed{\{1,2\} \cup \{3,4\} = \{3,2,4,2,1\}}, \qquad \boxed{\mathbb{N} \cup \mathbb{Z} = \mathbb{Z}}.$$

$$\boxed{\{1,2,4\} \cap \{3,4,5\} = \{4\}}, \qquad \boxed{\{1,3\} \cap \{2,4\} = \varnothing}, \qquad \mathbb{N} \cap \mathbb{Z} = \mathbb{N}_0.$$

$$\{1,2,4\} \setminus \{3,4,5\} = \{1\}, \qquad \boxed{\mathbb{N}_0 \setminus \mathbb{N} = \{0\}}, \qquad \boxed{\mathbb{N} \setminus \mathbb{Z} = \varnothing}.$$

$$\boxed{[3,5] \cup [5,7] = [3,7]}, \qquad [3,5] \cup (5,7) = (3,7), \qquad \boxed{[3,5) \cup (5,7) = [3,7) \setminus \{5\}}.$$

$$\boxed{\mathbb{N} \setminus \mathbb{Z} = \varnothing}, \qquad \mathbb{Z} \setminus \mathbb{N} = \{-x \colon x \in \mathbb{N}\}, \qquad \boxed{\mathbb{N} \subset \mathbb{N}_0}, \qquad \mathbb{Z} \subset \mathbb{N}_0, \qquad \boxed{(\mathbb{Z} \setminus \mathbb{Q}) \subset \mathbb{N}}.$$

$$\boxed{\mathbb{N} \subset \mathbb{N}}, \qquad \boxed{-3 \in \mathbb{Z} \setminus \mathbb{N}_0}, \qquad \boxed{\tfrac{3}{7} \in \mathbb{Q} \setminus \mathbb{Z}}, \qquad \boxed{\sqrt{2} \in \mathbb{R} \setminus \mathbb{Q}},$$

Exercise 1.13. *Which of the following statements are true? Give reasons or find counterexamples.*

- **a)** $(\mathbb{Q} \setminus \mathbb{R}) \subset \mathbb{N}_0$.
- **b)** *Suppose A, B, C are three arbitrary sets. Then it is true that* $A \cup (B \cap C) = (A \cup B) \cap C$.
- **c)** *Suppose A, B, C are three arbitrary sets. Then it is true that* $A \cap (B \cap C) = (A \cap B) \cap C$.
- **d)** *Suppose A, B, C are three arbitrary sets. Then it is true that* $A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C)$.

Exercise 1.14. *Describe the following sets and compute their cardinalities.*

- **a)** $X_1 := \{x \in \mathbb{N} \colon \exists a, b \in \{1,2,3\} \text{ with } x = a - b\}$
- **b)** $X_2 := \{(a - b) \colon a, b \in \{1,2,3\}\}$
- **c)** $X_3 := \{|a - b| \colon a, b \in \{1,2,3\}\}$
- **d)** $X_4 := \{1, ..., 20\} \setminus \{n \in \mathbb{N} \colon \exists a, b \in \mathbb{N} \text{ with } 2 \leq a \text{ and } 2 \leq b \text{ and } n = a \cdot b\}$.
- **e)** $X_5 := \{S \colon S \subset \{1,2,3\}\}$.

When we want to describe the union or intersection of several sets $M_1, \ldots, M_k$, we use a notation that is similar to the one for sums and products. We define

$$\bigcup_{i=1}^{k} M_i := M_1 \cup \ldots \cup M_k \qquad \text{und} \qquad \bigcap_{i=1}^{k} M_i := M_1 \cap \ldots \cap M_k.$$

The left set consists of those objects that are elements of **at least one** of the sets $M_1, \ldots, M_k$. The right set consists of those objects that are elements of **all** of the sets $M_1, \ldots, M_k$.

Example 1.15.

$$\bigcup_{i=1}^{4} \{2i\} = \{2\} \cup \{4\} \cup \{6\} \cup \{8\} = \{2, 4, 6, 8\},$$

$$\begin{aligned} \Big(\bigcup_{i=1}^{4} \{2i-1, 2i\}\Big) \setminus [2,6] &= \Big(\{1,2\} \cup \{3,4\} \cup \{5,6\} \cup \{7,8\}\Big) \setminus [2,6] \\ &= \{1,2,3,4,5,6,7,8\} \setminus [2,6] = \{1,7,8\}, \end{aligned}$$

$$\bigcap_{i=1}^{3} \{i-1, i, i+1\} = \{0,1,2\} \cap \{1,2,3\} \cap \{2,3,4\} = \{2\}.$$

At the end of this section we will study how many different subsets of a given size one can find in a set with n elements. For example, suppose we want to count subsets with exactly 2 elements out of the set $M = \{a, b, c, d, e\}$. We have 5 possibilities for the choice of the first element, and then 4 possibilities for the choice of the second element, thus altogether $5 \cdot 4 = 20$ combinations. However, here a combination is a sequence of 2 different elements from M, so we would count the combination a, c and the combination c, a as two different combinations, although they lead to the same subset $\{a, c\}$. Every subset will thus be generated twice by the 20 combinations, so in total there are exactly 10 subsets.

Correspondingly, for general $k, n \in \mathbb{N}$ with $k \leq n$, we can generate

$$\underbrace{n \cdot (n-1) \cdot \ldots (n-k+1)}_{k \text{ factors}} = \frac{n \cdot (n-1) \cdot \ldots \cdot 2 \cdot 1}{(n-k) \cdot (n-k-1) \cdot \ldots \cdot 2 \cdot 1} = \frac{n!}{(n-k)!}$$

combinations, where we do respect the ordering. Out of these combinations we then generate k-element subsets by ignoring the ordering. In this way we generate each subset $k!$ times, because this is the number of ways one can order k different elements. So in total, there are exactly

$$\binom{n}{k} := \frac{n!}{k!\,(n-k)!} \tag{1.3}$$

k-element subsets of an n-element set. This expression is call the binomial coefficient of n and k and we sometimes say "n choose k".

In the following, we note a few elementary properties of the binomial coefficient.

Theorem 1.16. properties of the binomial coefficient

Let $n, k \in \mathbb{N}_0$ with $k \leq n$. Then:

a) $\binom{n}{k} = \binom{n}{n-k}$,

b) $\binom{n}{0} = \binom{n}{n} = 1$,

c) $\binom{n}{1} = \binom{n}{n-1} = n$.

d) *If in addition $k \geq 1$, then* $\binom{n}{k} + \binom{n}{k-1} = \binom{n+1}{k}$.

Proof. The above statements can either be verified by using the defining formula in (1.3) or by using the combinatorial interpretation as the number of subsets of a given set. Here we explain this for the statements a) and d).

The statement in a) follows immediately from

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

To verify the statement in d) we consider a set $M := \{x_1, \dots, x_{n+1}\}$ with $n+1$ different elements. On the right hand side of the equation in d) we count the k-element subsets of M. Now to the left hand side. Suppose we first count all k-element subsets of M that do not contain the element x_{n+1}. The number of these is exactly $\binom{n}{k}$. Then we count those that do contain the element x_{n+1}. The number of these is exactly $\binom{n}{k-1}$, because we choose $k-1$ elements from the set $\{x_1, \dots, x_n\}$. In total we have counted all k-element subsets of M here, too. □

1.4 Proofs

We start with a real-world example.

$$\text{If I am in Hamburg, then I am in Germany.} \tag{1.4}$$

Here we are looking at a connection of the two statements

$$A = \text{“I am in Hamburg.”} \qquad \text{and} \qquad B = \text{“I am in Germany.”}$$

and we agree with the connection made in (1.4), because it has never happened to us that A occurs without B occuring. Instead of using the words “if” and “then” we will express connections like the one in (1.4) through the arrow “$\Rightarrow$”. In this case:

$$\text{I am in Hamburg.} \quad \Rightarrow \quad \text{I am in Germany.} \qquad \text{In short: } A \Rightarrow B \tag{1.5}$$

Implications: If we write "$A \Rightarrow B$", then this means that:

- *If A occurs, then B occurs.*
- *We say: A is sufficient for B.*
- *It is impossible for A to occur without B occuring.*
- *A cannot occur without B.*
- *We say: B ist necessary for A.*

We call the coennection $A \Rightarrow B$ an implication und say that statement A implies statement B.

The same holds for the examples

$$\begin{aligned} \text{It rains.} \quad &\Rightarrow \quad \text{The street gets wet.} \\ \text{The phone rings.} \quad &\Rightarrow \quad \text{The battery is not empty.} \end{aligned}$$

However we could be tempted to argue against the connections in the above examples, because maybe we are talking about one of the 20 American cities called Hamburg, or the street could be covered by trees and thus avoid getting wet depite some rain, or the phone could be connected be charging and thus ringing despite an empty battery. In Mathematics, we will not have to indulge into discussions as these, but will always seek to be on completely safe grounds.

Let us look at the connection of two statements about a natural number n:

$$n \text{ is a multiple of } 6. \quad \Rightarrow \quad n \text{ is a multiple of } 3. \tag{1.6}$$

None of the statements if true for every $n \in \mathbb{N}$, but that's okay because this is nore required when looking at an implication. We need to check whether everytime **when** n is a multiple of 6 ist, **then** n is also a multiple of 3. Let's first try it by looking at some multiples of 6 such as $6, 12, 18, 24$, and yes, they are all multiples of 3, too: $6 = 2 \cdot 3$ and $12 = 4 \cdot 3$ and $18 = 6 \cdot 3$ and $24 = 8 \cdot 3$.

But this is not a proof. We only tried some multiples of 6, and there are infinitely many of them, and we cannot try them all. On the other hand, when we tested our examples, we realized the following: $24 = 4 \cdot 6$ and $24 = 8 \cdot 3$. In other words, 3 fits twice as many times into 24 as 6 does. And this is true in general. To transform this argument into a clean proof, we first need a proper definition for when n is a multiple of 6.

Definition 1.17. Multiples of 6

A number $n \in \mathbb{N}$ is called a multiple of 6, if there is a number $k \in \mathbb{N}$, such that $n = 6 \cdot k$ holds.

This number k measures how often 6 fits into the number n, and therefore it has to be a natural number. Correspondingly, a number $n \in \mathbb{N}$ is called a <u>*multiple of* 3</u>, if there is a number $\ell \in \mathbb{N}$, such that $n = 3 \cdot \ell$ holds.

Now we look at the implication in (1.6). We have:

$$
\begin{aligned}
n \text{ is a multiple of } 6 \quad &\Rightarrow \quad \text{there is a } k \in \mathbb{N} \text{ with } n = 6 \cdot k \\
&\Rightarrow \quad \text{there is a } k \in \mathbb{N} \text{ with } n = (3 \cdot 2) \cdot k \\
&\Rightarrow \quad \text{there is a } k \in \mathbb{N} \text{ with } n = 3 \cdot \underbrace{(2 \cdot k)}_{=:\ell} \qquad (1.7) \\
&\Rightarrow \quad \text{there is an } \ell \in \mathbb{N} \text{ with } n = 3 \cdot \ell \qquad (1.8) \\
&\Rightarrow \quad n \text{ is a multiple of } 3.
\end{aligned}
$$

What exactly happened when we went from line (1.7) to line (1.8)? In line (1.7) we knew that there is a $k \in \mathbb{N}$ such that $n = 3 \cdot (2 \cdot k)$. Now we just define $\ell := 2k$ because it perfectly suits our needs. First, we know in this way that $\ell \in \mathbb{N}$ and second we have that $n = 3 \cdot \ell$ as claimed in (1.8). By the way, it is exactly here (where we define $\ell = 2k$) that we see again that 3 fits twice as many times into n as 6 does.

This was our first formal proof! We have written it out very carefully to get acquainted with the language and notation. In the future, we will be more brief.

Next we generalize 1.17 to integers n and general $a \in \mathbb{Z}$ instead of 6 or 3.

Definition 1.18. mulitples, even and odd numbers

A number $n \in \mathbb{Z}$ is called a <u>multiple</u> of a number $a \in \mathbb{Z}$, if there exits a $k \in \mathbb{Z}$, such that $n = a \cdot k$ gilt. A number $n \in \mathbb{Z}$ is called an <u>even number</u>, if it is a multiple of 2, thus a number of the form $n = 2p$ with $p \in \mathbb{Z}$. An <u>odd number</u> $n \in \mathbb{Z}$ is a number of the form $n = 2q + 1$ with a $q \in \mathbb{Z}$.

Theorem 1.19. even + odd = odd

If $n \in \mathbb{Z}$ is even and $m \in \mathbb{Z}$ is odd, then $n + m$ is odd.

Proof. Since n is even and m is odd, we know that there are integers p and q, so that $n = 2p$ and $m = 2q + 1$. Hence

$$n + m = 2p + 2q + 1 = 2(p + q) + 1 = 2r + 1,$$

where $r := p + q$ satisfies $r \in \mathbb{Z}$. This proves that $n + m$ is odd. □

Exercise 1.20. *Prove the following statements:*

a) *If $n \in \mathbb{Z}$ is odd and $m \in \mathbb{Z}$ is odd, then $n + m$ is even.*

b) *If $n \in \mathbb{Z}$ is odd and $m \in \mathbb{Z}$ is odd, then $n \cdot m$ is odd.*

c) *If $n \in \mathbb{Z}$ is even and $m \in \mathbb{Z}$ is an arbitrary number, then $n \cdot m$ is even.*
d) *If $n \in \mathbb{Z}$ is even, then so is $-n$. Wenn $n \in \mathbb{Z}$ is odd, then so is $-n$.*
e) *If $n \in \mathbb{Z}$ is even, then $n+1$ is odd. If $n \in \mathbb{Z}$ is odd, then $n+1$ is even.*
f) *Every number $n \in \mathbb{Z}$ is wither even or odd.*
g) *The sum of any three consequtive integers is a multiple of 3.*

Theorem 1.21. n and n^2 always have the same parity

Let $n \in \mathbb{N}$. Then it is true that:
a) *n is even $\Rightarrow$ n^2 is even,*
b) *n is even $\Leftarrow$ n^2 is even,*
c) *n is even $\Leftrightarrow$ n^2 is even.*

Although it is intuitively clear, let us spell out that

$$A \Leftarrow B \text{ means } B \Rightarrow A \text{ (which we have defined earlier),}$$

and

$$A \Leftrightarrow B \text{ means that } A \Rightarrow B \text{ and } A \Leftarrow B \text{ hold both,}$$

in other words A and B are either both true or both false.

To understand the difference between $A \Rightarrow B$ and $A \Leftrightarrow B$, look again at (1.5) and (1.6) and compare it to Theorem 1.21 c).

Proof of Theorem 1.21. **a)** Let n be even. By Exercise 1.20 c) we have that $n^2 = n \cdot n$ is even.

b) Let n^2 be even. We first try a direct proof. There exists a $p \in \mathbb{Z}$ mit $n^2 = 2p$. We now need to show that n is also even. We have that $n = \sqrt{n^2} = \sqrt{2p} = \sqrt{4p/2} = 2\sqrt{p/2} = 2q$ with $q := \sqrt{p/2}$. But it is not clear why this q is an integer, which we would need to show that n is even.) We therefore try a new approach and use the technique of a **proof by contradiction**:

Let n^2 be even. We want to show that n is even. **Assume** n is not even. By Exercise 1.20 f) then n must be odd. By Exercise 1.20 b) then $n^2 = n \cdot n$ would be odd and this not even. This contradicts our requirement that n^2 is even! Hence our **assumption** that n is not even was wrong. So n is indeed even.

c) follows from parts a) und b). $\square$

Proof by contradiction, negation and contraposition

If we want to prove $A \Rightarrow B$ by a contradiction, then we assume that A holds but B does not hold. From this we try to deduce that A does not hold, contradicting our earlier condition that A holds.

Suppose that $\neg A$ and $\neg B$ denote the negation of A and B respectively, i.e., they are true if and only if A and B are false, respectively. Then our proof by contradiction attempts to show that $\neg B \Rightarrow \neg A$. Sometimes this is easier than showing $A \Rightarrow B$, see for example Theorem 1.21 b).

The implication $\neg B \Rightarrow \neg A$ is also called the contraposition of the original implication $A \Rightarrow B$. The contraposition $\neg B \Rightarrow \neg A$ is equivalent to the implication $A \Rightarrow B$.

Let's again look at our introductory Example 1.5:

$$\begin{array}{rrcl} A \Rightarrow B: & \text{I am in Hamburg.} & \Rightarrow & \text{I am in Germany.} \\ \neg B \Rightarrow \neg A: & \text{I am not in Germany.} & \Rightarrow & \text{I am not in Hamburg.} \end{array}$$

Both statements say indeed the same (namely that Hamburg lies in Germany).

Between us: contraposition

You obtain the contraposition of $A \Rightarrow B$ by swapping A and B and putting a negation sign $\neg$ in front of both: $\neg B \Rightarrow \neg A$.
In particular it is clear that the contraposition of the contraposition is again $A \Rightarrow B$.

Finding the negation of a statement is sometimes not as simple as it looks. In Theorem 1.21 it was still obvious:

$$\begin{array}{rl} A: & n \text{ is even.} \\ \neg A: & n \text{ is not even (hence odd).} \end{array}$$

What characterizes the negation $\neg A$ of a statement A? In principle, this is easy: it must always be true that either A or $\neg A$ hold. It must never be true that none of them holds, and it must never be true that both of them hold. We practice this with an example.

Question 1.22. *What is the negation of the following statement R?*
$R:$ *"'In this room there is a[1] red chair."'*

A: In this room there are no chairs.
B) In this rool there is a chair that is not red.
C) All chairs in this room are green.
D) All chairs in this room are not red.

Statement A is not the negation of R, because if for example the room had exactly two green chairs and nothing else, then none of the two statements would be true. Statement B is not the negation of R, because if for example the room had a red and a green chair, then both statements would be true. Statement C is not the negation of R, because if

[1]Recall: When we say "there is a", then we mean "there is at least one". There could also be two, three or more.

for example the room had a blue chair and nothing else, then none of the two statements would be true. Statement D is indeed the negation of R.

Exercise 1.23. *What is the negation of the following statement P?*
P : *"All persons in this room have a cold."*

a) At most two persons in this room have a cold.
b) One person in this room has a headache.
c) Nobody in this room has a cold.
d) In this room there is a person who does not have a cold.
e) Not all persons in this room have a cold.

We could, in the same manner as above, run through these statements and check whether they could be true at the same time as P (or whether they could be false at the same time as P) and hence rule them our. But this time we take a different approach: Let R be the set of persons in this room and let S be the set of those persons in the world who currently have a cold. Then we can write statement P as follows:

$$P: \qquad \forall x \in R : x \in S$$

The negation can therefore be written as:

$$\neg P: \qquad \neg(\forall x \in R : x \in S) \tag{1.9}$$

In other words: Not all the persons in this room have a cold. This is answer e). But we can reformulate (1.9). Instead of saying "not all of them have a cold", we can also say that "there is (at least) one who does not have a cold", hence

$$\neg P: \qquad \exists x \in R : \neg(x \in S) \tag{1.10}$$

which is answer d). So both are equivalent to $\neg P$ (and thus equivalent to each other).

The process of transforming (1.9) into (1.10) can be described as follows: We move the symbol "$\neg$" from left to right. When passing the symbol "$\forall$", this symbol switches to "$\exists$". Now the symbol "$\neg$" ends up to the right of "$\exists$". In short: "$\neg\forall = \exists\neg$". Or in other words: "not (all elements satisfy...)" $\Leftrightarrow$ "there is (at least) one element that does not satisfy"

The same works when switching the roles of "$\forall$" and "$\exists$". Here "$\neg\exists = \forall\neg$", or in other words:
"there is no element with ..."$\Leftrightarrow$ "all elements have no...".

Using these two simple transformation rules

Between us: negating for–all and there-exists ($\forall$ and $\exists$)

"$\neg\forall = \exists\neg$" *and* "$\neg\exists = \forall\neg$"

we can now also find negations of longer constructions such as the following.

Exercise 1.24. *What is the negation of the following statement?*
R: "At every wheel of this car there is at least one loose screw"

a) At every wheel of this car all screws are tightened.
b) There is a wheel of this car with one a tightened screw.
c) There is a wheel of this car where all screws are tightened.
d) At every wheel of this car there is a tightened screw.

1.5 Proof by induction

In this section we study a proof method that is particularly useful for proving statements involving natural numbers $n \in \mathbb{N}$. We introduce this technique via the following example and will then deduce the general method from it.

Theorem 1.25. sum of the first n natural numbers

Let $n \in \mathbb{N}$. Then

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

Proof. The proof consists of three steps.

Induction base: We first check the statement for the case $n = 1$. On the left hand side, we have only one summand, namely 1. On the right hand side we have the term $1 \cdot (1+1)/2 = 1$, hence the statement is correct.

Induction hypothesis: Next we assume that the statement is true for the number $n \in \mathbb{N}$.

Induction step: Based on the correctness of the statement for the number n, we now want to deduce that it is also true for the number $n+1$. So here our goal is to show that

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

We argue as follows:

$$\begin{aligned}\sum_{i=1}^{n+1} i &= 1 + \ldots + n + (n+1) = \left(\sum_{i=1}^{n} i\right) + (n+1) \\ &\overset{(IH)}{=} \frac{n(n+1)}{2} + (n+1) = (n+1)\left(\frac{n}{2}+1\right) = (n+1)\frac{n+2}{2}.\end{aligned}$$

In the last line we first applied the induction hypothesis (IH) and then factored-out the term $n+1$. □

Think of this method as climbing a stairway. The first step is the statement for $n = 1$, the second step is the statement for $n = 2$, and so on. We want to show that we can *stand on each step*, meaning that the corresponding statement is true.

In the induction base, we test whether we can stand on the first step. Next, in the induction hypothesis, we assume that we stand on the n-th step. And in the induction step, we show that based on this assumption, we can reach the next step. Using this strategy, we have shown that we can stand on each step.

We practice this method in the next example.

Theorem 1.26. mulitples of 3 via a proof by induction

Let $m \in \mathbb{N}$. Then $2^{2m} - 1$ is a multiple of 3.

Proof. Before we start the proof, we recall that by Definition 1.18 a number n is a multiple of 3, if there exists a number $k \in \mathbb{Z}$ with $n = 3k$.

Induction base: We check the above statement for the case $m = 1$. Obviously $2^{2\cdot 1} - 1 = 3$ is a multiple of 3.

Induction hypothesis: Next we assume that we have shown the above statement for the number $m \in \mathbb{N}$.

Induction step: Based on the correctness of the statement for the number m, we now want to deduce that it is also true for the number $m+1$. So here our goal is to show that the number $2^{2(m+1)} - 1$ is a multiple of 3. In order to apply the induction hypothesis, we have to modify this term in such a way that we can find the term $2^{2m} - 1$ inside. Here is one way to do this:

$$\begin{aligned} 2^{2(m+1)} - 1 &= 2^{2+2m} - 1 = 2^2 \cdot 2^{2m} - 1 = 4 \cdot 2^{2m} - 1 = 4\left(2^{2m} - 1 + 1\right) - 1 \\ &= 4\left(2^{2m} - 1\right) + 4 - 1 = 4\left(2^{2m} - 1\right) + 3. \end{aligned}$$

Now we can apply the induction hypothesis: we know that there is a $k \in \mathbb{Z}$ such that $2^{2m} - 1 = 3k$ and hence

$$2^{2(m+1)} - 1 \overset{(IH)}{=} 4 \cdot 3k + 3 = 3(4k+1).$$

Since $4k+1$ is an integer, we have shown that $2^{2(m+1)} - 1$ is a multiple of 3, which is what we wanted to show. $\square$

Exercise 1.27. *Let $m \in \mathbb{N}$. Give a proof by induction that $3^{2m+4} - 2^{m-1}$ is a muliple of 7.*

Proofs by induction can also be used to to prove inequalities. Here is an example, where we construct a sequence of real numbers $a_0, a_1, a_2, \dots$ by setting the starting value $a_0 := 1$ and then defining recursively that $a_{n+1} := \sqrt{a_n + 2}$ for all $n \in \mathbb{N}_0$. In this way, we obtain

$$a_0 = 1, \quad a_1 = \sqrt{a_0 + 2} = \sqrt{1+2} = \sqrt{3} \approx 1.732$$

$$a_2 = \sqrt{a_1 + 2} = \sqrt{\sqrt{3} + 2} \approx \sqrt{3.732} \approx 1.932$$

and so on. This sequence seems to grow, but we would like to show that all of its members remain strictly smaller than 2. Intuitively this is clear, because the new term a_{n+1} can only reach or exceed the value 2 if the term inside the square root reaches or exceeds the value 4, but then a_n would have had to reach or exceed the value 2 already. The following proof by induction formalises this approach.

Theorem 1.28. a sequence that doesn't reach or exceed a given value

Set $a_0 := 1$ and define $a_{n+1} := \sqrt{a_n + 2}$ for all $n \in \mathbb{N}_0$. Then we have $a_n < 2$ for all $n \in \mathbb{N}_0$.

Proof. **Induction base:** Since we have to prove the statement for all $n \in \mathbb{N}_0$, the base case is given by $n = 0$. By definition we have $a_0 = 1 < 2$.

Induction hypothesis: Next we assume that we have shown the above statement for the number $n \in \mathbb{N}$.

Induction step: Our goal is to take the inequality $a_n < 2$ and deduce from it the inequality $a_{n+1} < 2$. This can be done as follows:

$$a_{n+1} = \sqrt{a_n + 2} \overset{(IH)}{<} \sqrt{2 + 2} = \sqrt{4} = 2,$$

which completes the induction step and thus the proof. □

Next we will see an example for a proof by induction where the focus is not on some computation but on a combinatorial argument.

Theorem 1.29. number of subsets in an n-element set

Let $n \in \mathbb{N}$ and M be a set with $|M| = n$. Then there are exactly 2^n different subsets of the set M.

Proof. **Induction base:** We check the statement for the case $n = 1$. Let M be an arbitrary set with $|M| = 1$, say $M = \{x\}$. Then there are exactly two subsets of M, namely $M_1 = \emptyset$ and $M_2 = \{x\}$.

Induction hypothesis: Next we assume that we have shown the above statement for the number $n \in \mathbb{N}$.

Induktionsschritt: Now consider an arbitrary set M' with exactly $n + 1$ elements, say $M' = \{x_1, \ldots, x_n, x_{n+1}\}$. We need to show that there are exactly 2^{n+1} subsets of M'. We divide the family of all subsets of M' into two classes: those that do not contain the x_{n+1} (call this Class 1), and those that do contain the element x_{n+1} (call this Class 2).

How many subsets are there in Class 1? These are exactly the subsets of the set $M := \{x_1, \dots, x_n\}$, and by induction hypothesis there are exactly 2^n of them.

How many subsets are there in Class 2? We generate these by first choosing the element x_{n+1} and then adding an arbitrary subset of the set $M := \{x_1, \dots, x_n\}$. Again, by induction hypothesis, these are exactly 2^n subsets, this time in Class 2.

In total we therefore have exactly $2^n + 2^n = 2 \cdot 2^n = 2^{n+1}$ subsets of the set M', which is what we wanted to prove. □

To conclude this section we will present the binomial theorem and prove it by induction. What is this theorem about? From school we know that $(a+b)^2 = a^2 + 2ab + b^2$. What happens when we want to compute higher powers of $a+b$ than just the square?

Theorem 1.30. binomial theorem

Let $a, b \in \mathbb{R}$ and $n \in \mathbb{N}$. Then

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

Before we prove this theorem, let us first spell out what it says for small values of n:

$$\begin{aligned}
(a+b)^1 &= \binom{1}{0} a^0 b^1 + \binom{1}{1} a^1 b^0 = b + a, \\
(a+b)^2 &= \binom{2}{0} a^0 b^2 + \binom{2}{1} a^1 b^1 + \binom{2}{2} a^2 b^0 = b^2 + 2ab + a^2, \\
(a+b)^3 &= \binom{3}{0} a^0 b^3 + \binom{3}{1} a^1 b^2 + \binom{3}{2} a^2 b^1 + \binom{3}{3} a^3 b^0 = b^3 + 3ab^2 + 3a^2 b + a^3.
\end{aligned}$$

Proof of Theorem 1.30. We have already checked the base case $n = 1$ above. For the induction step we argue as follows:

$$\begin{aligned}
(a+b)^{n+1} = (a+b)(a+b)^n &\overset{(IH)}{=} (a+b)\left(\sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}\right) \\
&\overset{(*)}{=} \sum_{k=0}^{n} \binom{n}{k} a^{k+1} b^{n-k} + \sum_{k=0}^{n} \binom{n}{k} a^k b^{n+1-k} \\
&\overset{(**)}{=} \sum_{k=1}^{n+1} \binom{n}{k-1} a^k b^{n-(k-1)} + \sum_{k=0}^{n} \binom{n}{k} a^k b^{n+1-k} \\
&= a^{n+1} + b^{n+1} + \sum_{k=1}^{n} \binom{n}{k-1} a^k b^{n+1-k} + \sum_{k=1}^{n} \binom{n}{k} a^k b^{n+1-k}
\end{aligned}$$

$$
\begin{aligned}
&= a^{n+1} + b^{n+1} + \sum_{k=1}^{n} \left(\binom{n}{k-1} + \binom{n}{k} \right) a^k b^{n+1-k} \\
&\overset{\text{Thm 1.16}}{=} a^{n+1} + b^{n+1} + \sum_{k=1}^{n} \binom{n+1}{k} a^k b^{n+1-k} \\
&= \sum_{k=0}^{n+1} \binom{n+1}{k} a^k b^{n+1-k}.
\end{aligned}
$$

For the equality sign marked by $(*)$ we have simply multiplied the sum with the factor a and b respectively. For the equality sign marked by $(**)$ we did an index shift for the first sum: the counter k begins and ends now at a value that is increased by one, and consequently in the summand we replace the term k by the term $k-1$. We already saw this technique in the examples (1.1) and (1.2) in Section 1.2.

At the end of the transformation we have reached the claimed expression for the case $n+1$, which concludes the proof. □

1.6 Functions and Maps

Definition 1.31. function, map

Let X and Y be two arbitrary sets. A rule f that assigns to every $x \in X$ a unique $y \in Y$ is called a function or a map from X to Y. In this case we write $f(x)$ for y and call X the domain of f and Y the codomain of f. This is the notation:

$$
\begin{aligned}
f : X &\to Y \\
x &\mapsto f(x)
\end{aligned}
$$

Attention! two arrows

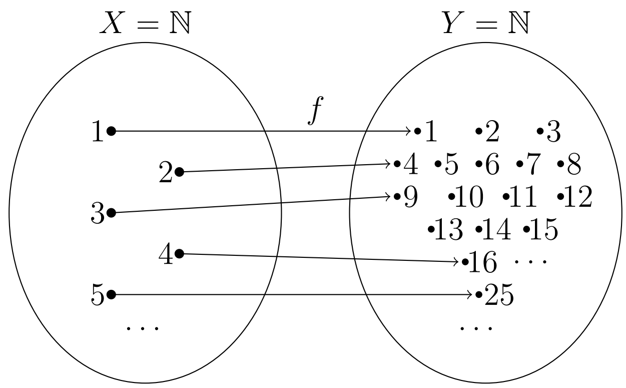
Note that we use the arrow $\to$ between the two sets, and the arrow $\mapsto$ between the two elements.

Between us: Think of a function as machine that converts x into y.

$$\xrightarrow{x} \boxed{f} \xrightarrow{y}$$

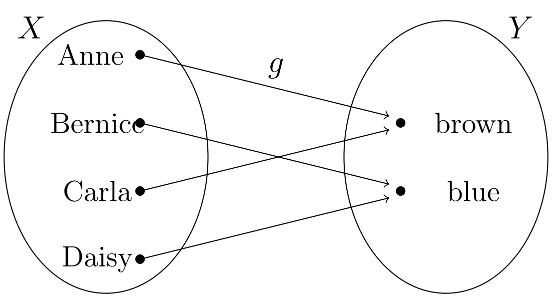
$$x = \textit{input}, \quad f = \textit{machine}, \quad y = \textit{output}$$

Example 1.32. a) $f : \mathbb{N} \to \mathbb{N}$ with $f : x \mapsto x^2$, in other words $f(x) = x^2$. This function assigns to every natural number its square.



b)

$$\begin{aligned} g : \{\text{Anne, Bernice, Carla, Daisy}\} &\to \{\text{brown, blue}\} \\ x &\mapsto \text{colour of eyes of } x \end{aligned}$$



c)

$$\begin{aligned} Sunshine : \text{Days of the year 2022} &\to \{0, 1, 2, \ldots, 24\} \\ t &\mapsto \text{number of hours of sunshine on day } t \text{ in Hamburg} \end{aligned}$$

e.g. $Sunshine(22.07.2022) = 13$.

d)

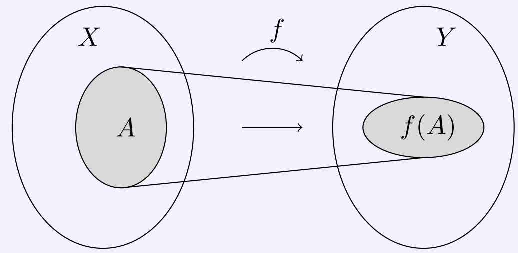
$$\begin{aligned} Month : \{1, 2, \ldots, 12\} &\to \{\text{January, February,} \ldots \text{,December}\} \\ n &\mapsto \text{Name of the } n\text{-th month in the year} \end{aligned}$$

e.g. $Month(3) = \text{March}$.

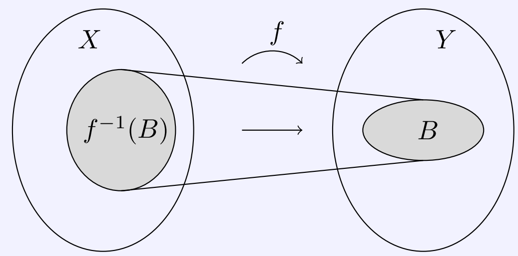
Definition 1.33.

Let $f : X \to Y$ be a function and consider subsets $A \subset X$ and $B \subset Y$.

$f(A) := \{f(x) : x \in A\}$ is called image of the set A (with respect to f).
In the special case $A = X$ we also speak of the image of f:
$\mathrm{Image}(f) := f(X) = \{f(x) : x \in X\}$.



$f^{-1}(B) := \{x \in X : f(x) \in B\}$
is called preimage of the set B.



Let's practice this with another example.

Example 1.34. Consider the function $f : \mathbb{Z} \to \mathbb{Z}$ with $f : x \mapsto x^2$ and observe that, although this is the same operation as in Example 1.32 a), it is a different function, as the domain and codomain are different. Here we have

$$f(\{-2,3\}) = \{4,9\}, \quad f(\{-2,2\}) = \{4\}, \quad f^{-1}(\{4,9\}) = \{-3,-2,2,3\}$$

and $\mathrm{Image}(f) = f(\mathbb{Z}) = \{0,1,4,9,\ldots\}$.

In general, we will be looking at two different situations.

A: given: $x \in X$, looking for: $y \in Y$ with $f(x) = y$
Usually this is simple, because the function f tells us how to compute y from x, and by Definition 1.31 there is exactly one such y.

B: given: $y \in Y$, looking for: $x \in X$ with $f(x) = y$
Usually this is more difficult. We are looking for a preimage x of y.

Definition 1.35. solving the equation $f(x)=y$

The computation of a preimage x of y with respect to a function f in Situation **B** *above is also denoted as "We solve the equation $f(x) = y$", and we call x a solution of the above equation.*

The next question is therefore whether, for a given $y \in Y$, there **exists** a solution x of $f(x) = y$, and if yes, **how many**. This leads us directly to the following definition:

Definition 1.36. injective, surjective, bijective

A function $f : X \to Y$ is called

- *surjective, if every $y \in Y$ has (**at least one**) preimage x,*
- *injective, if every $y \in Y$ has **at most one** preimage x,*
- *bijective (or invertible), if f is surjective and injective,*
  *i.e. if every $y \in Y$ has **exactly one** preimage x.*

In other words:

Between us: surjective, injective, bijective

A function $f : X \to Y$ is ...

surjective $\Leftrightarrow$ *every $y \in Y$ gets hit by **at least** 1 arrow*
$\Leftrightarrow$ $f(X) = Y$
$\Leftrightarrow$ *the image of f is equal to the codomain of f*
$\Leftrightarrow$ *the equation $f(x) = y$ has a solution for every $y \in Y$*

injective $\Leftrightarrow$ *every $y \in Y$ gets hit by **at most** 1 arrow*
$\Leftrightarrow$ *for all $x_1, x_2 \in X$ we have* $\quad (x_1 \neq x_2 \quad \Rightarrow \quad f(x_1) \neq f(x_2))$
$\Leftrightarrow$ *for all $x_1, x_2 \in X$ we have* $\quad (f(x_1) = f(x_2) \quad \Rightarrow \quad x_1 = x_2)$
$\Leftrightarrow$ *the equation $f(x) = y$ has a **unique** solution for all $y \in f(X)$*

bijective $\Leftrightarrow$ *every $y \in Y$ gets hit by **exactly** 1 arrow*
$\Leftrightarrow$ *the equation $f(x) = y$ has a **unique** solution for all $y \in Y$*

In Example 1.32 our functions had the properties:

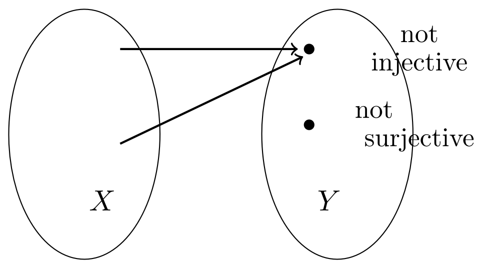
a) injective, but not surjective

b) surjective, but not injective

c) not surjective, not injective

d) surjective and injective, and therefore bijective

Summarizing these properties once more in one picture:



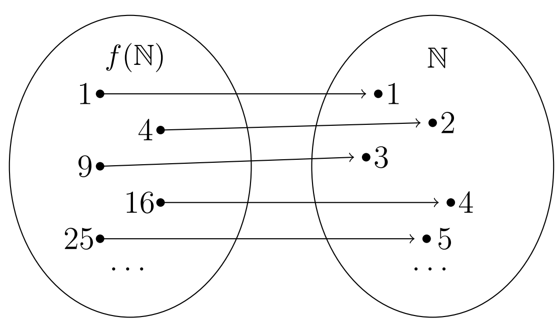
Recall that for every function $f : X \to Y$ it is true that every $x \in X$ is assigned to a unique image $y \in Y$. Now if a function f is injective, this means that in addition every $y \in f(X)$ has a unique preimage x. The function

$$\begin{aligned} f(X) &\to X \\ y &\mapsto \text{its unique preimage } x \\ \text{i.e. } f(x) &\mapsto x \end{aligned}$$

is called the *inverse function* or just *inverse* of f and is denoted[2] by $f^{-1} : f(X) \to X$.

Example 1.37. The inverse function of f in Example 1.32 a) is given by

$$\begin{aligned} f^{-1} : \{1, 4, 9, 16, 25, \dots\} &\to \mathbb{N} \\ m &\mapsto \sqrt{m} \\ \text{or } n^2 &\mapsto n \end{aligned}$$

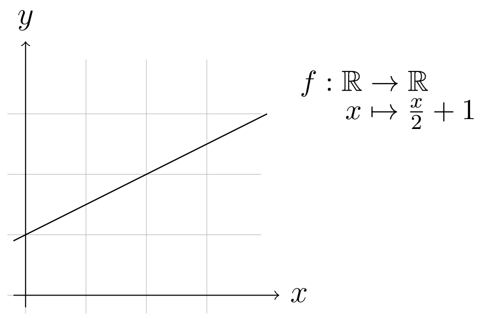


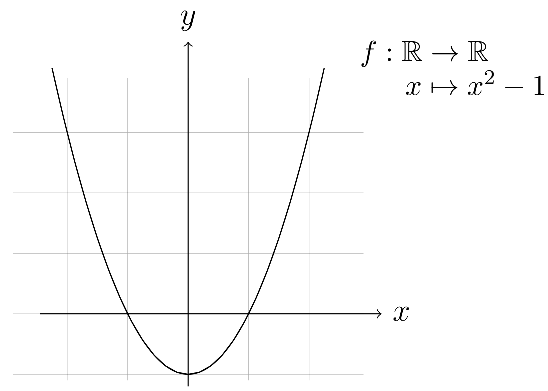
Notice that the domain of f^{-1} is not all of $\mathbb{N}$, but only $f(\mathbb{N})$, i.e. the square numbers.

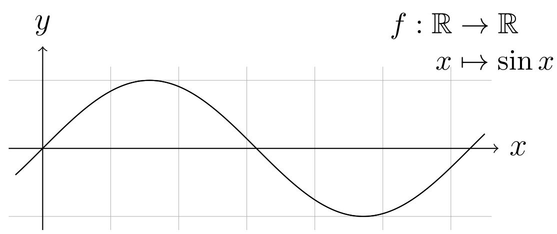
If f is not only injective, but also surjective (and thus bijective), we have the additional property that $f(X) = Y$, i.e. every $y \in Y$ has a unique preimage and therefore f^{-1} maps all elements of Y to X (and not just the elements of $f(X)$).

For functions $f : \mathbb{R} \to \mathbb{R}$ we can draw the graph $\{(x, f(x)) : x \in X\}$ in the plane. Here are some examples:

[2] Careful readers might think that we have a clash of notation here: On the one hand $f^{-1}(B)$ now denotes the image of B with respect to the inverse function f^{-1}. On the other hand $f^{-1}(B)$ was earlier defined as the preimage of the set B with respect to the function f. But these sets are identical!



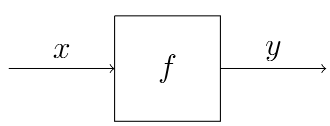




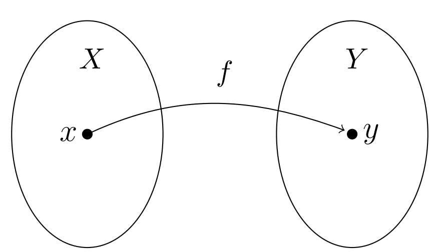
Looking at the graph, we can later read off many nice properties of f (e.g. continuity, differentiability, monotonicity, extreme points, derivatives, integrals,...).

Question 1.38. *Can we read off injectivity and surjectivity of a function when looking at its graph? (If yes, how?)*

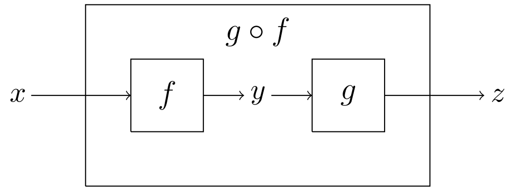
We again look at the picture of how a function $f : X \to Y$ maps elements from a set X to a set Y:



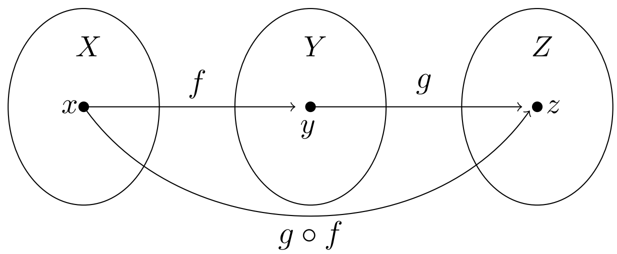
more precisely



and start to wonder how we concatenate two functions one after the other:



more precisely:



So let $f : X \to Y$ and $g : Y \to Z$ be two functions. We call the function

$$g \circ f : X \to Z$$

with

$$g \circ f : x \mapsto g(\underbrace{f(x)}_{y})$$

the *concatenation* or *composition* of the functions f and g.

Example 1.39. **a)** $f : \mathbb{R} \to \mathbb{R}$, $x \mapsto x^2$; $g : \mathbb{R} \to \mathbb{R}$, $x \mapsto \sin(x)$

$$\begin{aligned} g \circ f : \mathbb{R} &\to \mathbb{R} \\ x &\mapsto \sin(x^2) \\ f \circ g : \mathbb{R} &\to \mathbb{R} \\ x &\mapsto (\sin(x))^2 \end{aligned}$$

Note that the order matters. The functions $g \circ f$ and $f \circ g$ are not the same!

b) Let X be an arbitrary set. The function $id_X : X \to X$ with $x \mapsto x$ is called *identity*.
If the set X is clear from the context, then we write id instead of id_X. For any arbitrary function $f : X \to X$ it is true that

$$f \circ id = f = id \circ f.$$

If $f : X \to Y$ is bijective and $f^{-1} : Y \to X$ is its inverse function, then we have

$$f \circ f^{-1} = id_Y \quad \text{and} \quad f^{-1} \circ f = id_X.$$

This is why a bijective function is also called invertible.

Example 1.40. Consider $X = [0,2]$ and $Y = [0,4]$. The function $f : X \to Y$ with $f(x) = x^2$ is invertible. The inverse function is $f^{-1} : Y \to X$ with $f^{-1}(y) = \sqrt{y}$, because

$$\begin{aligned} \forall y \in Y: \quad & (f \circ f^{-1})(y) &=& f(f^{-1}(y)) &=& (\sqrt{y})^2 &=& y &=& id_Y(y) \\ \forall x \in X: \quad & (f^{-1} \circ f)(x) &=& f^{-1}(f(x)) &=& \sqrt{x^2} &=& x &=& id_X(x). \end{aligned}$$

Exercise 1.41. *Suppose $f : Y \to Z$ and $g : X \to Y$ are invertible functions. Is $f \circ g$ also invertible? If yes, what does the inverse function look like? (Hint: Put on your socks, then your shoes. How do you reverse this process?)*

Observe that we can also concatenate functions $f : X \to Y_1$ and $g : Y_2 \to Z$, where the codomain Y_1 of f is not identical with the domain Y_2 of g. Consider for example

$$f : \mathbb{N} \to \mathbb{R}, x \mapsto x^4 \quad \text{und} \quad g : \mathbb{Z} \to \mathbb{R}, x \mapsto \sqrt{x}.$$

At first sight we could fear problems here for the definition of $g \circ f$, because the values generated by f might not lie in the domain of g, in which case g could not process them. In this example, however, this is not the case because the image $f(\mathbb{N})$ of f is indeed a subset of $\mathbb{N}$ and thus of $\mathbb{Z}$, which is given as domain of g. So here we have

$$g \circ f : \mathbb{N} \to \mathbb{R}, x \mapsto \sqrt{x^4} = x^2.$$

In general, for the concatenation of $f : X \to Y_1$ and $g : Y_2 \to Z$ to $g \circ f : X \to Z$ it suffices that $f(X) \subset Y_2$.

1.7 Trigonometry

Which angle does this give?

In this section, we will define the trigonometric functions sin, cos and tan. For this we need the unit circle. This is the ciricle with radius 1 around the origin $\binom{0}{0}$.

The unit circle has a circumference of 2π. Every point P on the unit circle can be described by the length of the arc between P and the point $\binom{1}{0}$. This length is positive if we start in $\binom{1}{0}$ and then turn anticlockwise. This length is negative if we start in $\binom{1}{0}$ and then turn clockwise. For example the point $\binom{0}{1}$ is described by an arc of length $\frac{1}{2}\pi$ or an arc of length $-\frac{3}{2}\pi$.

For every real number $\alpha \in \mathbb{R}$ we let P_α be the point on the unit circle whose arc has length α. We use this number α to measure the angle between the positive x-axis and the line segment connecting the origin and P_α.

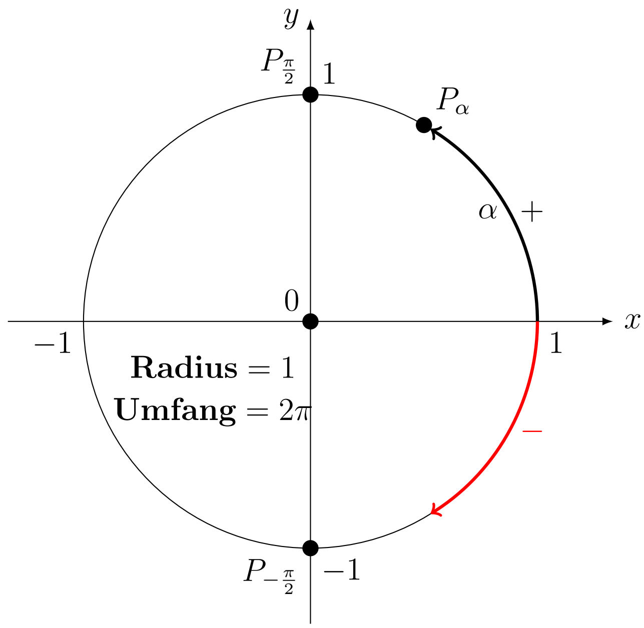


Figure 1.1: Unit circle with an arc of length α and the corresponding point P_α

So, for example, the angle of 180° is described by π, and the angle 90° by $\frac{\pi}{2}$. Correspondingly, $-\frac{\pi}{2}$ describes the angle of 90° with negative orientation, i.e. clockwise direction. If $\alpha > 2\pi$, then we go around the unit circle several times, and the same is true for $\alpha < -2\pi$. For example $P_{5\pi} = P_{3\pi} = P_\pi = P_{-\pi} = P_{-3\pi} = \binom{-1}{0}$.

We are now ready to define $\sin(\alpha)$ and $\cos(\alpha)$.

Definition 1.42. sin, cos

We denote the x-coordinate of P_α by $\cos(\alpha)$*, and the y-coordinate by* $\sin(\alpha)$*.*

This gives us the graphs of the functions $\sin(\alpha)$ and $\cos(\alpha)$ in Figure 1.2.

Theorem 1.43. basic properties of sin and cos

The following properties hold for every $\alpha \in \mathbb{R}$:

- **a)** $-1 \leq \cos(\alpha) \leq 1$ *and* $-1 \leq \sin(\alpha) \leq 1$*, because P_α is always a point on the unit circle.*
- **b)** $\cos(\alpha) = \cos(-\alpha)$ *and* $\sin(-\alpha) = -\sin(\alpha)$ *owing to the symmetry of the circle.*
- **c)** $(\cos(\alpha))^2 + (\sin(\alpha))^2 = 1$ *owing to Pythagoras' theorem.*
- **d)** $\cos(\alpha + 2\pi) = \cos(\alpha)$ *and* $\sin(\alpha + 2\pi) = \sin(\alpha)$ *owing to the periodicity of P_α.*

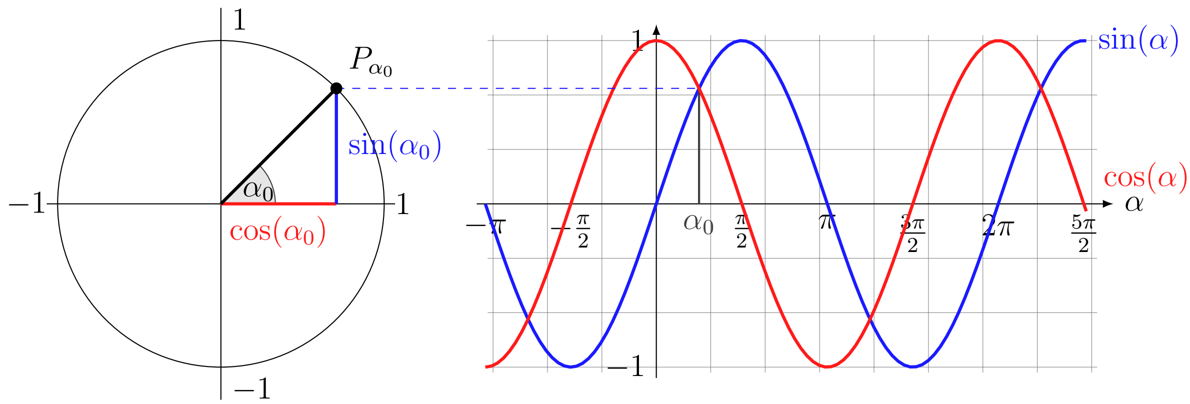


Figure 1.2: The functions sin (blue) and cos (red) in the interval $[-\pi, +\frac{5}{2}\pi]$.

e) *In particular, this implies that the zeros of* sin *and* cos *are as follows:*

$$\sin(\alpha) = 0 \;\Leftrightarrow\; \alpha \in \{0, \pm\pi, \pm 2\pi, \pm 3\pi, \ldots\}$$

$$\cos(\alpha) = 0 \;\Leftrightarrow\; \alpha \in \{\pm\tfrac{1}{2}\pi, \pm\tfrac{3}{2}\pi, \pm\tfrac{5}{2}\pi, \ldots\}$$

Moreover, using elementary geometric properties, we also have the following values:

α	0	$\pi/6$	$\pi/4$	$\pi/3$	$\pi/2$
$\cos(\alpha)$	1	$\frac{1}{2}\sqrt{3}$	$\frac{1}{2}\sqrt{2}$	$\frac{1}{2}$	0
$\sin(\alpha)$	0	$\frac{1}{2}$	$\frac{1}{2}\sqrt{2}$	$\frac{1}{2}\sqrt{3}$	1

Furthermore, the following formulae are often useful:

Theorem 1.44. angle sum identities for sin and cos

For all $\alpha, \beta \in \mathbb{R}$ it is true that:

$$\cos(\alpha+\beta) = \cos(\alpha)\cos(\beta) - \sin(\alpha)\sin(\beta),$$
$$\sin(\alpha+\beta) = \sin(\alpha)\cos(\beta) + \cos(\alpha)\sin(\beta).$$

Here is an example of how these theorems can be applied.

Example 1.45. Using Theorem 1.44 it is true that for arbitrary $\alpha \in \mathbb{R}$:

$$\sin\left(\alpha + \tfrac{\pi}{2}\right) = \sin(\alpha)\underbrace{\cos\left(\tfrac{\pi}{2}\right)}_{0} + \cos(\alpha)\underbrace{\sin\left(\tfrac{\pi}{2}\right)}_{1} = \cos(\alpha)$$

In other words: If we shift the graph of the sine function by $\frac{\pi}{2}$ to the left, we get the graph of the cosine function.

Using sin and cos we can now define the tangent and the cotangent function as follows:

$$\begin{aligned} \tan(\alpha) &:= \frac{\sin(\alpha)}{\cos(\alpha)} && \textit{for all } \alpha \neq \tfrac{\pi}{2} + n\pi, n \in \mathbb{Z}, \quad (\textit{thus } \cos(\alpha) \neq 0), \\ \cot(\alpha) &:= \frac{\cos(\alpha)}{\sin(\alpha)} && \textit{for all } \alpha \neq n\pi, n \in \mathbb{Z}, \quad (\textit{thus } \sin(\alpha) \neq 0). \end{aligned}$$

In other words, $\tan(\alpha)$ denotes the ratio of the y-coordinate to the x-coordinate of the point P_α, i.e. the slope (height : width) of the line segment from origin to P_α.

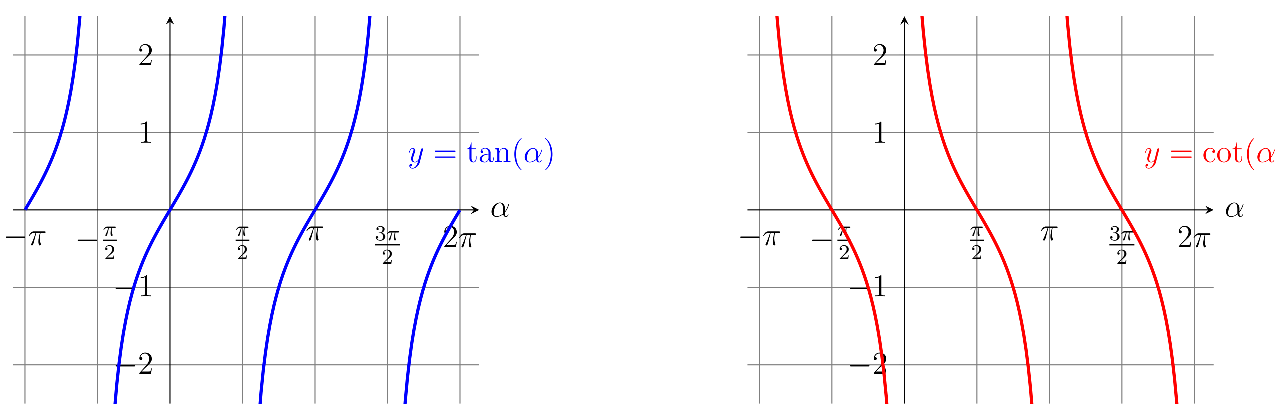


Figure 1.3: The functions tan (blue) and cot (red) in the interval $[-\pi, +2\pi]$.

From the properties of the sine and the cosine function we obtain the following properties of the tangent und the cotangent function. For all $\alpha \in \mathbb{R}$ and all $n \in \mathbb{Z}$ we have:

$$\begin{aligned} \tan(-\alpha) &= -\tan(\alpha) \quad \text{and} \quad \cot(-\alpha) = -\cot(\alpha) \\ \tan(\alpha + n\pi) &= \tan(\alpha) \quad \text{and} \quad \cot(\alpha + n\pi) = \cot(\alpha). \end{aligned}$$

We introduced the trigonometric functions in this section via the coordinates of a point P_α on the unit circle. This may look quite a bit different from the way you learned this in school. There one usually considers a right triangle—this is a triangle with a right angle, i.e. an angle of $90°$. The side of the triangle opposite of the right angle is called *hypotenuse*. Now fix one of the other two angles and call it α. The side of the triangle opposite of α is called *opposite*. Finally the side that together with the hypotenuse encloses α is called *adjacent*. Using these one then usually defines

$$\sin(\alpha) = \frac{\text{opposite}}{\text{hypotenuse}}, \quad \cos(\alpha) = \frac{\text{adjacent}}{\text{hypotenuse}}, \quad \tan(\alpha) = \frac{\text{opposite}}{\text{adjacent}}.$$

Compare this to our definitions using the unit circle as in Figure 1.2. There the length of the hypotenuse is given by the radius of the unit circle, which is 1. Hence the above definitions become

$$\begin{aligned} \sin(\alpha) &= \text{opposite} = y\text{-coordinate of } P_\alpha \\ \cos(\alpha) &= \text{adjacent} = x\text{-coordinate of } P_\alpha \\ \tan(\alpha) &= \frac{\text{opposite}}{\text{adjacent}} = \frac{\sin(\alpha)}{\cos(\alpha)}, \end{aligned}$$

which matches our definitions here.

We will now study the inverse functions of the trigonometric functions. In many situations we know the values of $\sin(\alpha)$ or $\cos(\alpha)$ and want to deduce the value of α. We have already seen that this is usually not possible, because for example $\cos(\alpha) = 0$ is true for $\alpha = \frac{\pi}{2}$ and also for $\alpha = \frac{3}{2}\pi$ (and thus correspondingly for $\alpha + 2\pi$). On the other hand for $\alpha \in [0, \pi]$ the function cos is strictly decreasing from $+1$ to -1 and attains every value between $+1$ and -1 exactly once. Hence in this interval cos has an inverse function and we can define

$$\arccos : [-1, 1] \to [0, \pi]$$

by

$$\arccos(x) := \alpha \quad \Leftrightarrow \quad \cos(\alpha) = x \ \text{ and } \ \alpha \in [0, \pi].$$

For the inverse of the sine function this works analogously, because for $\alpha \in [-\frac{\pi}{2}, \frac{\pi}{2}]$ the function sin is strictly increasing from -1 to $+1$ and attains every value between -1 and $+1$ exactly once. Its inverse function can therefore be defined by

$$\arcsin : [-1, 1] \to [-\tfrac{\pi}{2}, \tfrac{\pi}{2}]$$

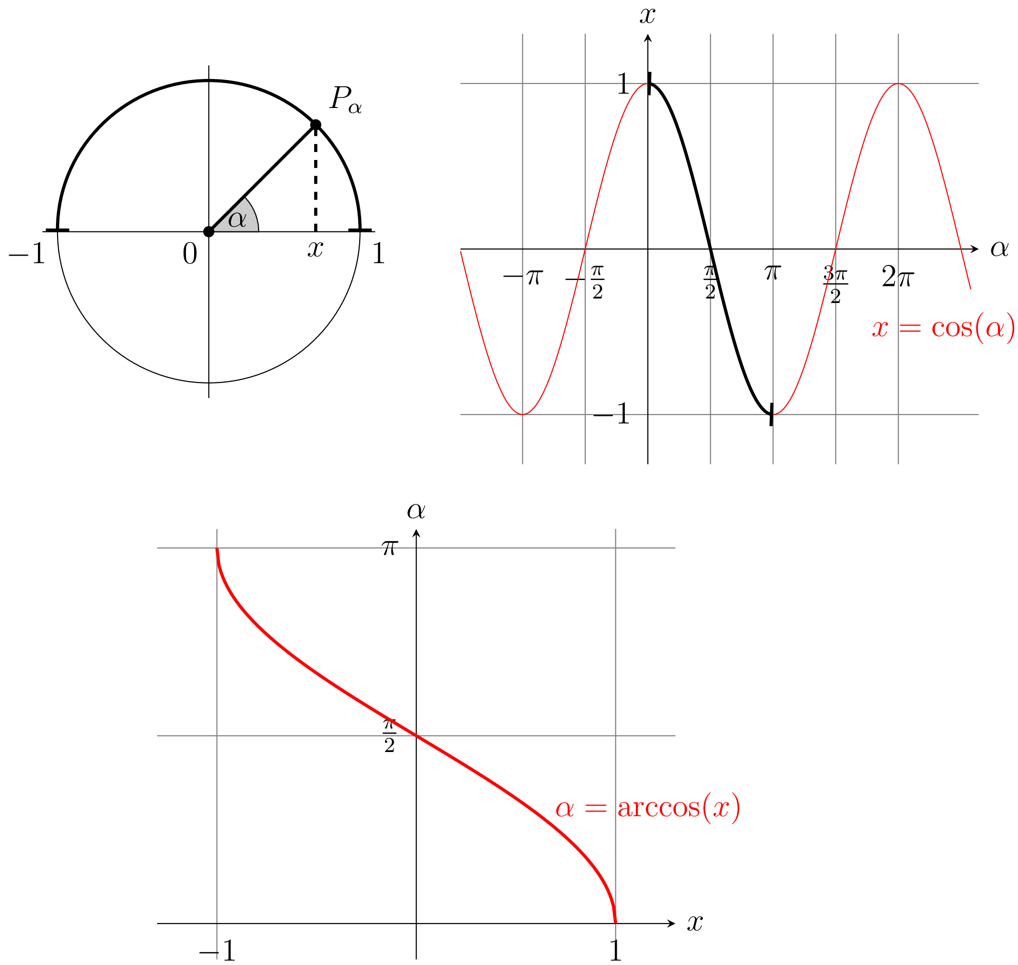


Figure 1.4: The function $\arccos(x)$ in the interval $[-1, +1]$.

and

$$\arcsin(y) := \alpha \quad \Leftrightarrow \quad \sin(\alpha) = y \text{ and } \alpha \in [-\tfrac{\pi}{2}, \tfrac{\pi}{2}].$$

Example 1.46. We solve the equation $\cos(\alpha) = \frac{1}{2}$. For this we compute $\arccos(\frac{1}{2}) = \frac{\pi}{3}$ and can thus be sure that $\alpha = \frac{\pi}{3}$ is the only solution in the interval $[0, \pi]$. Owing to the periodicity of cos we then obtain further solutions of the form $\frac{\pi}{3} + 2n\pi$ for all $n \in \mathbb{Z}$.

But there are more solutions, because the property $\cos(2\pi - \alpha) = \cos(\alpha)$ tells us that

$$\tfrac{1}{2} = \cos(\tfrac{\pi}{3}) = \cos(2\pi - \tfrac{\pi}{3}) = \cos(\tfrac{5\pi}{3}),$$

and thus there is another solution at $\frac{5\pi}{3}$. Again owing to the periodicity we then find other solutions of the form $\frac{5\pi}{3} + 2n\pi$ for all $n \in \mathbb{Z}$.

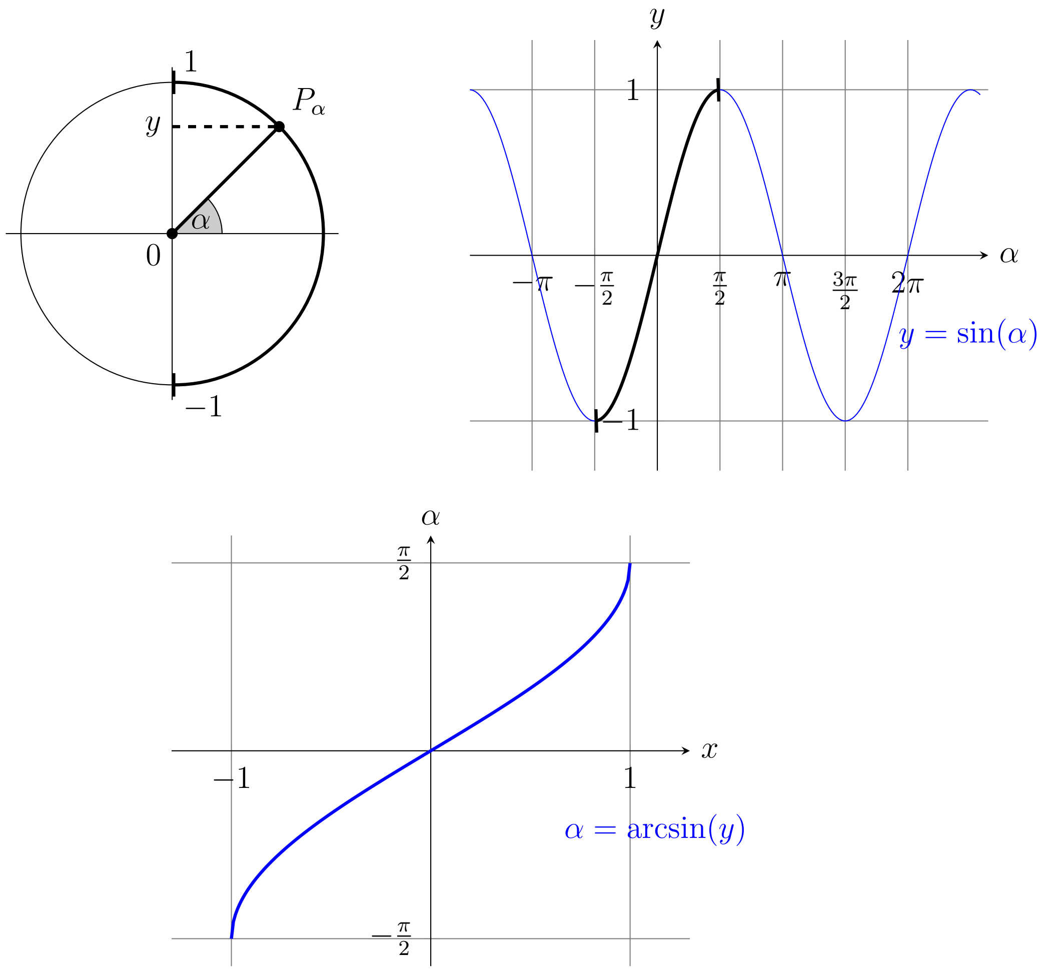


Figure 1.5: The function $\arcsin(y)$ in the interval $[-1, +1]$.

Similarly to the above we define

$$\arctan : \mathbb{R} \to [-\tfrac{\pi}{2}, \tfrac{\pi}{2}] \qquad \text{and} \qquad \operatorname{arccot} : \mathbb{R} \to [0, \pi]$$

via

$$\begin{aligned} \arctan(z) := \alpha \quad &\Leftrightarrow \quad \tan(\alpha) = z \ \text{ and } \ \alpha \in [-\tfrac{\pi}{2}, \tfrac{\pi}{2}], \\ \operatorname{arccot}(z) := \alpha \quad &\Leftrightarrow \quad \cot(\alpha) = z \ \text{ and } \ \alpha \in [0, \pi]. \end{aligned}$$

Exercise 1.47. *Let's go back to our question at the beginning:*
If we see a slope ot 10%, what angle does this represent?

Here we are looking for an angle α, where the line segment from the origin to P_α has a slope of $10\% = \frac{10}{100} = \frac{1}{10}$. We thus have $\tan(\alpha) = \frac{1}{10}$ and therefore $\alpha = \arctan(\frac{1}{10}) \approx 0.09967 \approx 5.7°$.

Exercise 1.48. *What about a slope of 100%?*

Here we have $\tan(\alpha) = 100\% = \frac{100}{100} = 1$. Hence $\alpha = \arctan(1) = \frac{\pi}{4} = 45°$.

Summary

- *Sets* group objects (*elements*) of the same kind together.
- Important symbols and operations: $\in,\ \notin,\ \varnothing,\ \forall,\ \exists,\ \subset,\ \not\subset,\ \cap,\ \cup,\ \setminus$
- Symbols for sums and products such as Σ, Π give short and precise definitions of long sums and products.
- Implication $A \Rightarrow B$: If A holds, then B must also hold.
- Equivalence $A \Leftrightarrow B$: If A holds, then so does B. And the other way round!
- The contraposition of $A \Rightarrow B$ is given by $\neg B \Rightarrow \neg A$.
- Easy way to remember: $\neg\forall = \exists\neg$ and $\neg\exists = \forall\neg$.
- A *function* or *map* $f : X \to Y$ assigns to every $x \in X$ exactly one $y \in Y$.
- f is *surjective*: Every $y \in Y$ gets "hit" at least once.
- f is *injective*: Every $y \in Y$ gets "hit" at most once.
- f is *bijective*: Every $y \in Y$ gets "hit" exactly once.
- If $f : X \to Y$ is bijective, then the *inverse function* $f^{-1} : Y \to X$ assigns to every $y \in Y$ the unique $x \in X$ that is mapped to y by f.
- The composition $g \circ f : X \to Z$ executes the maps $f : X \to Y$ and $g : Y \to Z$ one after the other: $(g \circ f)(x) = g(f(x))$.
- The trigonometric functions $\sin,\ \cos,\ \tan,\ \cot$ describe the ratios between the side lengths in a right triangle. If we imagine the triangle inside the unit circle, the hypotenuse has length 1 and we can forget about deviding by 1 when looking at $\sin$ and $\cos$.
- The trigonometric functions are bijective when limited to the appropriate intervals. Their inverse functions $\sin^{-1},\ \cos^{-1},\ \tan^{-1},\ \cot^{-1}$ are called $\arcsin,\ \arccos,\ \arctan,\ \operatorname{arccot}$.

Index