Preparatory Mathematics

Tomáš Kalvoda[1]

Antonella Marchesiello (translation)[2]

Jitka Rybníčková (translation)[3]

FAKULTA
INFORMAČNÍCH
TECHNOLOGIÍ
ČVUT V PRAZE

Winter semester 2023/2024, October 25, 2024

[1]KAM FIT ČVUT, tomas.kalvoda@fit.cvut.cz
[2]KAM FIT ČVUT, antonella.marchesiello@fit.cvut.cz
[3]KAM FIT ČVUT, jitka.rybnickova@fit.cvut.cz

Typeset using LaTeX
Source prepared using WooWoo version 0.4.0 and FIT PDF Template v0.2.4
Source code and bug reporting
Tomáš Kalvoda, KAM FIT ČVUT, 2017–2023

Contents

1 Introduction **1**
1.1 Notes to the text . . . 1

2 Mathematics is not only about computing **2**
2.1 Computation and abstraction . . . 2
2.2 The structure of a mathematical text . . . 3
2.3 What is a proof? . . . 5
2.4 A few examples of proofs . . . 5
2.5 What is not a proof? . . . 10

3 Basic concepts **12**
3.1 Note on mathematical notation . . . 12
3.2 Sets and set operations . . . 16
3.3 Number sets . . . 18
3.4 Significant subsets of real numbers . . . 25
3.5 Propositions and logical connectives . . . 26
3.6 Abbreviated writing of sums and products . . . 27
3.7 Factorial and binomial coefficient . . . 31
3.8 Important constants . . . 32

4 Elementary functions **35**
4.1 What is it a function? . . . 35
4.2 The absolute value . . . 38
4.3 Lower and upper integer part . . . 39
4.4 Linear function . . . 39
4.5 Quadratic function . . . 41
4.6 Polynomial function . . . 43
4.7 Roots . . . 45
4.8 Rational function . . . 46
4.9 Trigonometric functions . . . 47
4.10 Exponantiation and logarithm . . . 52

5 Analytical geometry **54**
5.1 Basic notions . . . 54
5.2 The line . . . 56
5.3 The circle and the ellipse . . . 57

6 Warning **59**
6.1 Smart calculators are too smart 59
6.2 Frequently asked questions 60

7 List of the used symbols **63**

Answers to some questions **65**

Bibliography **67**

Index **68**

1 Introduction

1.1 Notes to the text

This text serves as a review of the basic concepts and results of high school mathematics, that the students of the course *Fundamentals of Mathematical Analysis* (BIE-ZMA) should already well know and master. In addition, the topics treated here partially coincide with the first introductory lecture of BIE-ZMA. The course *Preparatory Mathematics* (BIE-PKM) takes place electronically in the first half of the winter semester of the academic year 2019/2020.

The text is divided into several chapters associating thematically similar problems. The purpose of the text is not a systematic presentation of secondary school program, but its review, highlighting important contexts or interpretations of the subjects from a new perspective. For this reason, different chapters and their sections might not follow in logical order.

After these introductory paragraphs, in the second chapter we deal with the meaning of *proof* and the mathematical approach to problem solving. In the third chapter we introduce the mathematical notation and symbols, and discuss the properties of sets and numerical operations. The fourth chapter then presents a brief overview of the so-called elementary functions, especially polynomial functions, rational functions, trigonometric functions, exponential and logarithmic functions. The fifth chapter summarizes the basic methods of describing some geometrical objects on the plane by using analytical geometry.

Now let us summarize some of the conventions used in this text. For the reader's convenience, the text is accompanied by a list of the used symbols. At the very end of the document there is also a relatively detailed index of terms and a few references to used sources or interesting publications.

Significant equations in this document are numbered within the chapters. Equation (3.5) is the equation number 5 in the third chapter. We use the same numbering method for pictures and tables as well. Thus, picture 1.3 means the third pictures in the first chapter. Only references to equations are traditionally indicated by brackets. These links are active in the electronic version of the document. When decimal digits are used, we use a decimal point instead of a decimal comma.

We would like to thank doc. Ing. Stepan Starost, Ph.D. Mgr. Jan Starý, Ph.D., Ing. Daniel Vašata, Ph.D. and Mgr. Lenka Nováková for comments and suggestions. If a kind reader finds errors or confusion in the following lines can always contact the authors of this document preferably by email.

2 Mathematics is not only about computing

> *If people do not believe that mathematics is simple, it is only because they do not realize how complicated life is.*
>
> *John von Neumann*

After passing through high school, students believe that mathematics is nothing but a set of computational procedures (algorithms). But this idea is quite far from reality. The aim of this chapter is to introduce the reader to a more realistic perspective.

2.1 Computation and abstraction

Mathematics has given the world a number of algorithms, computational procedures that can be taken and directly apply to a specific, often very narrowly focused, problem. Let us name the Fast Fourier transform (FFT, application in signal processing, e.g. in the mp3 format), Simplex algorithm (application in machine learning algorithms and optimization problems), or cryptosystems like for example RSA, based on number theory or cryptosystems based on elliptic curves (ECC), etc. Other interesting examples of algorithms can be found in the article [1].

The question, however, is whether it is admissible to reduce IT mathematics only to this computational aspect, as it usually happens in secondary schools. It is not appropriate to perform such a mutilation of university mathematics for several reasons (and not only according to the author of this text). Let us try to mention at least the most important here.

Mathematics is very closely connected with the so-called scientific method of knowledge, which can be said to be the basis of our civilization without much exaggeration. A frequent human goal is to find a deeper understanding of the world and to solve various problems. Mathematics in this activity does not play the role of a mere numerical machine. For any given problem, first it is necessary to analyze it, dismantle it into parts and examine their relationships and behavior. Then, typically, a mathematical model is created so that (more or less) it describes the problem. Subsequently, in the context of this abstract model, one tries to draw conclusions and solve the original problem.

Similarly, it is possible (and very often this is the case) to think at programming in an abstract way, to create programs that solve a given problem. Usually, the programmer is confronted with a real problem that he must first analyze and describe. He thinks about how to consider the problem (for example, create a detailed object or database model) and he proposes a solution. Subsequently, he embarks on the implementation of the solution.

Without a good intuition, based on understanding the problem, its solution is unlikely to be of good quality.

To program logically – i.e. to think abstractly about individual parts of the code – several programming paradigms serve, for example

- procedural (e.g. C, Fortran),
- object-oriented (e.g. C++),
- functionals (e.g. Lisp, Haskell),
- logical (e.g. Prolog).

It is no coincidence that the latter three paradigms are closely inspired by the mathematical way of thinking. The goal of these efforts is to bring order to the problem and improve its understanding. The above paradigms represent different abstract ways to *consider* and *think* models and algorithms.

It is also worth noting that some practical tasks have no effective solution. This may be a small shock to students coming from high school. But school examples are very special kinds of problems, often chosen just to have a nice solution. The absence of an effective solution means that there is no suitable algorithm to effectively address the task. Again, slightly surprising, this fact may not always be a bad thing, and on the contrary, it can have a good use, for example in computer security.

Example 2.1: For example, consider the task of deciding whether a natural number n is a prime or a composite number. We can try to look for factors (nontrivial divisors) of n, but this is a difficult task (for n big). On the other hand, you can effectively decide whether the number n is not prime *without knowing its factors*. On this observation is based the cryptosystem RSA.

At the end of this more abstract part of the text, let us make one more comment. Namely, a university graduate should be able to think about what he/she is doing. The work that can be automated was, is, and will be done by unthinking robots. He/she should also have a desire to learn and explore new things. IT students pay this multiple times. You never know what kind of problem you will be facing in the future, nor do you know where your technology and tools will move in your industry. Mathematics, as a systematic and logical way of thinking, can only help you in this endeavor. Moreover, math is *beautiful*.

2.2 The structure of a mathematical text

The aim of this section is to clarify and emphasize the logical structure of a mathematical text. As a rule, a mathematical text is divided into definitions, sentences and proofs. The reader often encounters the following types of *structures*:

- **Definition** : New concepts are being introduced (defined). In a more informal interpretation new concepts can also be introduced directly in the text (as often done in these notes). The purpose of the definition is to unambiguously anchor (define) concepts. The author of the definition agrees with the reader on what it is the meaning of a term. This is very important. Without clearly defined terms, there is a danger that two people would not be able to agree, because everyone is talking about something else but both use the same name for it.

- **Theorem** : An important statement that deserves a numerical designation in the text, or even to be named after its authors.
- **Proof** : A structure containing evidence of a previous statement, for example a theorem, but also a lemma, corollary (see in the following). Since it is typically longer than the statement formulation, its ending is usually marked with an ending symbol.[1] In BIEZMA we usually use the Halmos symbol of tombstone □. The reader can also often find the abbreviation Q.E.D. coming from the Latin *quod erat demonstrandum* („as it was to be proven"). The reader can find more about proofs in section 2.3.

You might also see:

- **Lemma** [2]: An auxiliary claim that does not have a wider application in itself[3], but it is used in the proof of one of the immediately following theorems.
- **Corollary** : Claims very straightforward from previous theorems, or reformulation of previous theorems into another context. Typically with a very simple proof (practically just a straightforward utilization - i.e. application - of previous theorems).

Remark 2.1: At this point, I would like to take a short note about a frequent student's „mistake". It is often the case to encounter the sentence „to define a theorem" This points to a fundamental misunderstanding by the users of this senseless words. They probably misunderstand the word „define" with „verbatim copy". „To define a theorem" is not possible in principle. You can define a term and then give a certain statement about that term, that is, the theorem. But here you have to prove, verify that the theorem is true. Fortunately, claims in mathematics cannot be defined.

Readers might be more familiar to notations using XML language. The structure of a mathematical text can then be seen as follows:

```
<definition>
  ...
</definition>
<theorem>
  ...
</theorem>
<proof>
  ...
</proof>
```

Apparently, presenting the reader with the text in this way would be typographically crazy. However, it should be noted that the source LaTeX code of this document uses this approach.

Of course, most mathematical texts are not composed only of the above described structures. Additional comments, examples or diagrams are often given for the reader's convenience, explaining further context regarding the discussed topic.

[1] Imagine a terminal XML tag.

[2] Lemma is a statement of medium importance.

[3] Exceptions confirm the rule, such as the well-known „Riesz lemma" or „Riemann-Lebesgue lemma". They are very important in themselves, but still carry the designation „lemma". This is for historical reasons. They were statments used as lemmas in the original papers, but were later used to solve other problems.

This structured approach of writing can be found not only in mathematics, but also in other technical and professional literature. For example, in the IT field, let us mention the documentary genre, or specification of standards, where a strong emphasis is placed on the logical structure of the text.

2.3 What is a proof?

The word **proof** raises irrational resistance in many students. In this chapter, we will try to whitewash its reputation. A proof is nothing more than a logical argument ensuring the validity of a claim. It is an answer to the inquiring question „why?“ In this chapter, we will try to outline the meaning of this term in a broader context and we will show some simple standard proofs.

Students at our faculty often come up with the notion that there is no need for proofs, it is only necessary to know the statements of theorems. However, this is a very short-sighted approach, especially for the following reasons.

- As already mentioned, a proof is nothing but a logical argument. It is based on assumptions and conclusions are reached by logical steps. Therefore, learning a proof improves not only the knowledge of the studied objects, but also the argumentative and expressive skills. It develops the capability of unambiguously describing and expressing ideas.
- The proof reveals to the student why the claim is true. It is then easier to remember its statement (e.g. its assumptions). Without studying the proof, the student loses understanding of the context and resorts to learning sentences by heart (which is not enriching for him[4] nor manageable).
- Most of the proofs, especially the so-called constructive ones, give direct guidance (algorithm) to solve problems.
- No superior authority (teacher, professor, guru) other than logics decides, on the correctness of the proof, and thus the truth of the proven claim. Once proven, it stays proven forever. Such an absoluteness of mathematics is beautiful.

An old concise comparison says: studying mathematics without proofs is like playing football without a ball. In short, mathematics without proofs does not make much sense!

2.4 A few examples of proofs

In this section, we will show some simple proofs of well-known and important statements. The reader will get acquainted to further proofs in the following chapters. In chapter 3.6 we will continue to practice this skill in proving several sum formulas.

Before we begin our first proof, let us refresh a few concepts, which will appear in the proven claim. We recall first the notions of *rational* and *irrational* real number.

Definition 2.1: A real number x, which is the ratio of two integers, is called **rational**. A real number, which is not rational, is called **irrational**.

[4] Except memory training.

Furthermore, let us recall the notions of *coprime* and *non-coprime* numbers.

Definition 2.2: If two integer numbers m and n have common divisors (factors) other than 1, they are said **non-coprime**. We say that two integer numbers m and n are **coprime**, if the only positive integer that divides both of them is 1.

Question 2.1: Which of the following numbers are rational and which are irrational?

$$\frac{\pi}{2},\ \frac{3}{4},\ \sin\frac{\pi}{4},\ \sin\frac{\pi}{6}.$$

Question 2.2: Which of the following pairs of numbers are coprime or non-coprime?

1. 7 and 6330079,
2. $\sqrt{2}$ and 2,
3. 5192311 and 36551

Proof by contradiction

We can use the so-called **contradiction**. The idea at the basis of a proof by contradiction is simple. One of the logic axioms says that every statement T must be either true or false. Thus, if we show that the logical opposite (negation) of T is false, then the original statement T is true.

Theorem 2.1: The square root of 2 is irrational.

Proof of the irrationality of $\sqrt{2}$. We *assume* the opposite, that is $\sqrt{2}$ *is* rational. Thus, since it is also a positive number, there exist two natural and coprime integer numbers p and q satisfying

$$\sqrt{2} = \frac{p}{q}.$$

It follows[5] the equality

$$2 = \frac{p^2}{q^2}, \quad \text{thus} \quad 2q^2 = p^2.$$

Since $2q^2$ is even (it clearly can be divided by 2), we see that also p^2 is even (otherwise above we would have an equality between an even and an odd number, which is impossible). The only way this can be true is that p itself is even. Thus,[6] $p = 2k$, where k is a natural number. Substituting this equality into the above equation and dividing both sides by 2, we get $q^2 = 2k^2$. If we use the same argument again, we get that also q is even. Therefore, p and q are non-coprime (both can be divided by 2). But such a situation cannot occur. Since by our assumption p and q are coprime, here we have come to a contradiction with our assumption, which therefore must be false. Thus $\sqrt{2}$ is irrational. □

Let us summarize the principle of the proof by contradiction. We want to be convinced of the truth of a certain claim T (i.e. we want to prove it). We show that the logical opposite (negation) of T is false. Thus, necessarily T must be true.

[5] Since $a = b$, $a^2 = b^2$.

[6] This equality expresses the evenness of p.

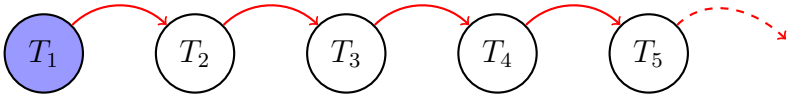


Figure 2.1: Scheme of the proof by mathematical induction. Instead of proving that all T_n are true, for $n = 1, 2, \ldots$, we can just prove that both T_1 and the induction step, i.e. the assertion $T_n \Rightarrow T_{n+1}$ (red arrows) are true.

Proof by mathematical induction

In the following, we illustrate the proof by **mathematical induction**. This type of proof is often used when we have infinitely many statements numbered by natural indices[7], for example $T_1, T_2, T_3, \ldots$ and we need to prove they are *all* true. The proof is done in two steps:

1. proove the first claim T_1,

2. for any natural n prove the so-called **induction step**: if T_n is true, then also T_{n+1} is true.

A graphical representation of this procedure is shown in figure 2.1. The red arrows correspond to the induction step. The starting point, i.e. the proof of T_1, is indicated in blue.

Mathematical induction can be compared to demolish a domino spiral. Each domino piece represents a „statement“ and can be in two states. A piece can be standing, or falling (similarly a statement can be true, or false). If we want to find out if the assembled domino spiral falls, we have two options. We can check all the pieces one by one and see if they fall. The second option is to check:

- if the first piece falls,
- two adjacent pieces are located at such a distance that if the first one falls (the one closer to the first piece) then its neighbor also falls (analog of the induction step).

Then we automatically know that all the pieces would fall. Let us emphasize the substantial difference in these approaches. The second method (ie, mathematical induction) controls the state of only the first piece, while it does not checks whether the others are standing or not, unless they are adjacent.

Let us illustrate the proof by mathematical induction for the so-called binomial theorem. In the statement of the theorem, we use the abbreviated sum, i.e. the summation notation, which the reader can find described more in detail in 3.6. Factorials, bynomial coefficients and general combinatorics are treated in section 3.7.

Theorem 2.2 (Binomial theorem)**:** For any real number a and b and any non negative integer number n, i.e. for $a, b \in \mathbb{R}$ and $n \in \mathbb{N}_0$, the following equality holds

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}. \tag{2.1}$$

Proof of the binomial theorem by mathematical induction. Let us verify that the equality being examined is true for the first n considered, i.e. for $n = 0$. The left-hand side of (2.1) is

[7] The particular numbering does not matter, as it is not important which number we are starting with. We only assume the so-called countability: it is possible to re-number the claims with natural numbers.

$(a+b)^0 = 1$ and for the right-hand side we have

$$\sum_{k=0}^{0} \binom{0}{k} a^k b^{0-k} = 1 \cdot 1 \cdot 1 = 1.$$

The equality $1 = 1$ is certainly true. Now let us assume that (2.1) holds for $n \in \mathbb{N}_0$. Let us verify that (2.1) is true for $n+1$ instead of n. Thus we want to find out whether

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

By direct calcuclation, we get[8]

$$\begin{aligned}
(a+b)^{n+1} &= (a+b)\cdot(a+b)^n \overset{!}{=} (a+b)\sum_{k=0}^{n}\binom{n}{k}a^k b^{n-k} = \\
&= \sum_{k=0}^{n}\binom{n}{k}a^{k+1}b^{n-k} + \sum_{k=0}^{n}\binom{n}{k}a^k b^{n+1-k} = \\
&= \sum_{k=1}^{n+1}\binom{n}{k-1}a^k b^{n+1-k} + \sum_{k=0}^{n}\binom{n}{k}a^k b^{n+1-k} = \\
&= \underbrace{\binom{n}{n}a^{n+1}b^{n+1-(n+1)}}_{a^{n+1}} + \sum_{k=1}^{n}\Bigg(\underbrace{\binom{n}{k-1}+\binom{n}{k}}_{\binom{n+1}{k}}\Bigg)a^k b^{n+1-k} + \\
&+ \underbrace{\binom{n}{0}a^0 b^{n+1-0}}_{b^{n+1}} = \\
&= \sum_{k=0}^{n+1}\binom{n+1}{k}a^k b^{n+1-k}.
\end{aligned}$$

In the equality marked by the exclamation point, we used the inductive assumption (the validity of the relation for n) and then we just performed algebraic operations. If we read the beginning and end of the calculation, we see that we have derived (2.1) for $n+1$, which was our goal. □

The claim of the binomial theorem contains well kown algebraic „formulas“

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

The above formulas represent special cases of the binomial theorem for a particular chosen n ($n = 2, 3$). For such small values of n, the formulas can be easily verified in an alternative way, by brackets expansion. For example for the first formula, thus for $n = 2$ we have

$$(a+b)^2 = (a+b)\cdot(a+b) = a^2 + ab + ba + b^2 = a^2 + 2ab + b^2.$$

[8] Imagine how the computation would appear *without using the summation convetion*!

This calculation effectively proves the binomial theorem for $n = 2$. Although in a similar way we could verify its validity also for $n = 3$, this cannot be considered as a proof of the binomial theorem. We would lack the proof all the claims for $n = 3, 4, 5, \ldots$! Fortunately, we did not have to prove all of them, thanks to the mathematical induction.

The importance ad utility of the binomial theorem can be further demonstrated on a concrete example (someone would say „trick“). Let us imagine that we are going to count 48^2 quickly by our heads. We can take advantage of the fact that the number 48 is close to 50, whose square is easy to calculate. Specifically, according to binomial theorem we have

$$48^2 = (50 - 2)^2 = 50^2 - 2 \cdot 50 \cdot 2 + 4 = 2500 - 200 + 4 = 2304.$$

Question 2.3: What is the sum of the first n odd natural numbers? I.e. what is the value of the sum

$$1 + 3 + 5 + \cdots + (2n - 1) = \sum_{j=1}^{n} (2j - 1), \quad n \in \mathbb{N}$$

equal to? Proove your claim.

Direct proof

Another type of proof is the direct proof. So to speak, without any detours, straightforwardly, we derive the claim from the assumptions. Consider the following theorem.

Theorem 2.3: For any real number a and b and $n \in \mathbb{N}$ the following equality holds

$$a^n - b^n = (a - b) \sum_{k=0}^{n-1} a^k b^{n-1-k}. \tag{2.2}$$

Proof. Let us take $a, b \in \mathbb{R}$ a $n \in \mathbb{N}$. We have to proove the equality (2.2). Let us start from the right-hand side of this equality and gradually adjust it through algebraic manipulation, to get the left-hand side of (2.2). Namely,

$$\begin{aligned}
(a - b) \sum_{k=0}^{n-1} a^k b^{n-1-k} &= a \cdot \sum_{k=0}^{n-1} a^k b^{n-1-k} - b \cdot \sum_{k=0}^{n-1} a^k b^{n-1-k} = \\
&= \sum_{k=0}^{n-1} a^{k+1} b^{n-1-k} - \sum_{k=0}^{n-1} a^k b^{n-k} = \\
&= \sum_{k=1}^{n} a^k b^{n-k} - \sum_{k=0}^{n-1} a^k b^{n-k} = \\
&= a^n + \sum_{k=1}^{n-1} a^k b^{n-k} - b^n - \sum_{k=1}^{n-1} a^k b^{n-k} = \\
&= a^n - b^n.
\end{aligned}$$

In other words, after multiplying the sum by the bracket $(a - b)$, the majority of terms cancel each other by subtraction, leaving only the difference $a^n - b^n$. □

Alternatively, it would be possible to proove theorem 2.3 by mathematical induction (try it!).

There are well known special cases of theorem 2.3:

$$a^2 - b^2 = (a - b)(a + b),$$
$$a^3 - b^3 = (a - b)(a^2 + ab + b^2).$$

These formulas and the general formula 2.2 will be useful (not only) in calculating the limits in the future. What makes theorem 2.3 so useful? It allows us to express the difference of same powers of two numbers by the difference of the numbers themselves. In other words, if we have some information about the difference $a - b$, then using this theorem we can infer something on the difference $a^n - b^n$.

Remark 2.2: The proven equality (2.2) also contained the formula for the sum of the first terms of a geometric sequence with ratio $q \neq 1$ and starting by 1. Indeed, considering the formula in the theorem for $a = q \neq 1$ and $b = 1$, we get

$$q^n - 1 = (q - 1) \sum_{k=0}^{n-1} q^k$$

and dividing by the non zero factor $q - 1$, it follows

$$\sum_{k=0}^{n-1} q^k = \frac{q^n - 1}{q - 1}$$

2.5 What is not a proof?

The previous part of the text dealt with the question of what a proof is and contained several concrete examples of proofs. In this section, we will point out the most frequent errors related to proofs. Thus, we will deal with what it *is not* a proof.

„Proof“ by examples vs. counterexample

The truth of a general statement cannot be based on several specific examples that support its truthfulness. In contrast, the truth of the statement can be *refuted* by just one **counterexample** [9].

Let us see, as a demonstrative case, a claim that Fermat wrote in 1650:[10]

> *For any $n \in \mathbb{N}_0$ the number $2^{2^n} + 1$ is a prime number.*
>
> *Pierre de Fermat*

By exploring the value of the expression $2^{2^n} + 1$ for some small n we obtain the numbers 3, 5, 17, 257, 65 537, which are prime. We have validated the claim for the first five cases.

[9] If somebody tells you that all the cars around the world have a blue or green color, how can you convince him/her of his/her mistake? You go out on the street and *show* him/her a car of red (or other than blue and green) color. I.e. you refute his/her claim by demonstrating a counterexample.

[10] The expression a^{b^c} means a to the power of b^c, and it is different from $(a^b)^c = a^{bc}$.

However, this *does not proove* the truth of the claim for *all* n! Indeed, the next value for $n = 6$ is not a prime number:

$$2^{2^6} + 1 = 18446744073709551617 = 274177 \cdot 67280421310721. \tag{2.3}$$

Of course, in Fermat's time this breakdown of the formula was unknown. The formula (2.3) gives therefore a **counterexample** to Fermat's statement and *refutes* it. In other words it prooves that the statement is *not* true. For sure, examples supporting a claim can be sometimes useful. They could guide a person to guess a general claim. However, the truth of such claim cannot be derived from the examples. E.g., as mentioned above, the binomial theorem 2.2 cannot be proven by verifying his statement only for $n = 1, 2, 3$, because this does not say anything on the cases $n = 4, 5, \ldots$

From the assumption to the claim.

Another common phenomenon is the misunderstanding of the way a proof is conducted. Let us repeat again that the goal is to go from the **assumption** to the **claim** of a theorem/lemma/corollary through logical steps. If you are studying a proof, you should pay attention on where and how the assumptions were used (there is nothing more humorous than a proof in which the assumptions of the theorem do not show up at all). Let us try to illustrate this phenomenon on another rather common error. For simplicity, consider a very simple statement: *the sum of even numbers is an even number.* For the sake of completeness, let us recall that an integer k is called even, when it can be expressed in the form $k = 2\ell$, where ℓ is some other integer (this is the definition of evenness for integer numbers). As a proof, some students would write: „When I add two even numbers, I must get an even number again." Is this a proof? Of course not, it repeats what it is to be proven, it only says that the claim *must* be true. Even if that *must* is written in large font and blood, it will not be a reason (proof) for the statement to be true. A correct (direct) proof would look like this: let us take two even numbers, let us say $a, b \in \mathbb{Z}$. They are even (here it is the assumption) and therefore, by definition, there exist some integers k and ℓ such that $a = 2k$ a $b = 2\ell$. Thus, considering their sum, according to the distributive law, it applies that

$$a + b = 2k + 2\ell = 2(k + \ell),$$

Thus, we see that $a + b$ is actually the double of the integer number $k + \ell$, and so it is by definition even! I hope the reader will appreciate the difference between „obviousness" and the real proof shown above, now. In the previous paragraph, based on assumptions, definition and properties of integers (distributive law, closeness with respect to sum), it has been shown that the statement is true.

Obvious proof

To conclude, let us point out the meaning of the word „obvious". A claim is **obvious**, just when his proof immediately comes to your mind. Not because you believe it is true, but you do not really know why.

3 Basic concepts

If I have seen further it is by standing on the shoulders of giants.

Isaac Newton

3.1 Note on mathematical notation

Every programming language requires that code be written using correct **syntax**. If a programmer does not comply with the syntax of a language their code may be incomprehensible and hence inapplicable, for the compiler or interpreter of the language. Although there is no firmly codified notation in mathematics it is good to follow established notation. In this subchapter we will sum up the most commonly used notation.

Remark 3.1: Students are often surprised that mathematical notation and terminology is not clearly and globally codified. There is the ISO 80000-2 standard which aims to fix some symbols and names but it is not very widespread. Uniform nomenclature is not used for historical reasons but also because of the different needs of different areas of mathematics. Matematics is live and creative and it does not make sense to bind it with any ISO standard. Even in painting and art there are many styles using different tools to achieve similar results. Similarly, why is there not only one programming language? And it is good. But what is globally true is the logical structure of mathematics and the way mathematics is built. In other words, it does not matter what symbols we use or which language we speak, what matters is *how* and *what rules we follow*.

Equality and equations

First we will analyze the meaning of the most important of symbols, the **equals sign** $=$. In programming languages as well as in mathematical notation the symbol $=$ plays a crucial role. Unfortunately, in each of these areas it is used slightly differently, which can often be very confusing. In the vast majority of programming languages the meaning of the symbol `=` is **assignment**. For instance, this line of code

```
a = 2
```

often means that from this moment onwards the value of the variable `a` is `2`. So does the line of code

```
a = a + 1
```

say to the computer that the new value of the variable `a` is the old value of `a` increased by 1. Furthermore, in programming we often encounter the symbol == which tests actual equality of two objects. For example, the line of code

```
a == b
```

is evaluated as `true`, if the objects `a` and `b` are equal[1]. Otherwise, it is evaluated as `false`.

The situation with matematical notation is a bit more complicated. Basically, we can say that the *context* in which the symbol $=$ is used plays a most important role. The basic function of the symbol $=$ is to denote **equality** of two known objects. In this way we can formulate a claim, e.g.

$$a = b, \tag{3.1}$$

where a and b are certain defined objects, which is either true or not. For natural number 4 the equality $4 = 4$ is true, for for numbers 4 and 3 the equality $4 = 3$ is false. In this sense the matematical symbol $=$ is close to the programming symbol == discussed above.

The symbol $=$ is also used to write down an **equation**. For instance, in the equation

$$x^2 - 1 = 0 \tag{3.2}$$

x stands for an **unknown**, an object to be determined with the property that after we substitute it in the equation (3.2) we get equality between the left-hand side and the right-hand side of this equation. Such instances of x are then called **solutions** of the equation (3.2). In this case the equation (3.2) has two solutions, the numbers 1 and -1, and no other real number is a solution. Indeed, after substituting 1 or -1 into the equation (3.2) we get an equality $0 = 0$, which is true. On the other hand if we substitute for instance 2 for x then we get an equality $3 = 0$, which is false[2].

The symbol $=$ is furthermore used to denote assignment in the programming sense. It can usually be easily seen from the context if it is the author's intention. Let's take a closer look at the following text sample.

> *Assume we have a rectangle with sides of length $a = 3$ and $b = 4$. We will denote the length of the rectangle diagonal with c. By the Pythagoras' theorem we have that $c = \sqrt{a^2 + b^2}$, i.e. in our case $c = 5$.*

The first two uses of the symbol $=$ marked with red mean assignment. From that moment on the symbols a and b have specific values. In programming slang we would say that variables a and b were inicialized. The second sentence of the paragraph does not contain the symbol $=$ but its meaning is the same because it unequivocally defines the symbol c. Finally, the last sentence *claims* that the blue equalities are true. Here it does not concern assignment/definition/initialization but the validity of a certain relationship between defined objects a, b and c.

Sometimes we use the symbol $:=$ to denote assignment. We usually choose this symbol when we want to emphasize that a new object has been introduced. The symbol on the left-hand side of $:=$ is then *defined* by the expression on the right-hand side of $:=$. Here we

[1] The notion of equality may depend on the type of a particular object.

[2] Note that the examples in this paragraph only serve to explain the property of „being a solution of an equation". We are not talking about how to effectively find a solution and whether it can be done for a given equation at all. We will learn more about this problem in BIE-ZMA.

would like to warn the reader that CAS[3] Mathematica uses the discussed symbols in a slightly different way. We will discuss this topic in more detail in chapter 6.

Variable notation

Let us now summarize some common conventions for naming that we will use in this document as well as in the BIE-ZMA course. Although the choice of names used for objects is entirely up to the author, it is good to follow these unwritten rules.

- We use letters from the end of the Latin alphabet to name unknowns in equations, for example x, y or z.
- We use letters from the beginning of the Latin alphabet to name known – previously defined – objects or parameters of a problem, for example a, b, c, etc. We often use the Greek alphabet for numerical values, i.e. $\alpha, \beta, \gamma, \ldots$
- For **summation indices** (see Section 3.6 below) and integer quantities we often use letters i, j, k, ℓ, m or n. When using the letter i we must be careful not to confuse it with the imaginary unit denoted also by[4] i.
- We use capital letters $A, B, C, \ldots$ to name sets. We also usually use capital letters of the latin alphabet to denote points in a plane (space).
- We use letters r, s, t to parametrize geometrical objects (lines, circles, areas, etc.).

Brackets

Next, let's mention the role of brackets in mathematical notation. We use brackets to indicate function (mapping) argument, to specify the order of execution of operations or to mark intervals and points. Without parentheses, many algebraic expressions would not make sense[5]. In the rest of this subchapter, we will discuss in more detail just such cases of using brackets.

If we have a function f and an element a from the domain of f, then $f(a)$ denotes the function value of f in a. To be more precise, $f(a)$ is a number, on the other hand f is an abstract object of the function type. Therefore, this use of parentheses exactly matches the usage you will find in programming languages. If f and a have already been defined then the meaning of $f(a)$ is: call the function f with argument a and return $f(a)$. The value of a can be seen as input and $f(a)$ as output of the function f. Graphically, we can imagine this situation as in Figure 3.1.

However, sometimes we call the whole expression $f(x)$ a function. We often use this point of view if we also want to tell the reader what the variable will be called (here x). In some cases, brackets around function arguments are omitted, in particular when we want to improve readability and simplify notation. E.g. we often write $\sin\alpha$ instead of $\sin(\alpha)$ or $\ln 2$

[3] Computer Algebra System.

[4] Therefore, we try to distinguish the imaginary unit at least typographically, compare i and i. For the sake of completeness, note that especially in physical (e.g. electrical) literature, the imaginary unit is often denoted by j, whereas the letter i is reserved for instantaneous current value.

[5] They would not be unambigously defined. For example, consider the expression $2 \cdot 3 + 5$. Without the introduction of *conventional* priority of operations we cannot determine if it means $2 \cdot (3 + 5)$ or $(2 \cdot 3) + 5$.

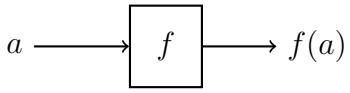


Figure 3.1: Function f and its functional value. a is the input and $f(a)$ is the output. The function f itself is a „black box“ which transfers input to output.

instead of $\ln(2)$. We must however take care to avoid any misunderstanding. For example, the expression

$$\ln 2 \cdot 3 \tag{3.3}$$

could be interpreted as

$$\ln(2 \cdot 3) \quad \text{or} \quad \ln(2) \cdot 3.$$

Of course, these numbers *are not* the same. Using a calculator[6] we can easily verify that the two expressions are approximately equal to

$$\ln(2 \cdot 3) = \ln(6) \approx 1.791\,759\,469\,23,$$
$$\ln(2) \cdot 3 \approx 2.079\,441\,541\,68.$$

Especially with „manual“ calculation[7] these inaccuracies may lead to catastrophic errors. Therefore it is better to write multiplicative factors in front of functions. Here, the expression $3 \ln 2$ is defined unambiguously, as opposed to the expression in (3.3).

Let's remind the reader that for some functions we use special notation which does not require brackets. For instance, square root is denoted by $\sqrt{x}$, cube root by $\sqrt[3]{x}$ and the absolute value by $|x|$. The reader is also familiar with the floor (resp. ceiling) of a real number x denoted by the symbol $\lfloor x \rfloor$ (resp. $\lceil x \rceil$).

Parentheses are furthermore used to specify the order of algebraic operations. For example, the expression

$$\Big(a + (c/2)\Big) \cdot 3$$

should be understood as follows: first divide c by two and add a, then multiply this number by three. Without brackets,

$$a + c/2 \cdot 3,$$

it would (without the order of operations *convention* [8]) not be clear how to evaluate this expression. In this respect mathematics does not differ from programming languages. The majority of programming languages employs operator precedence (see e.g. C Operator Precedence).

Remark 3.2: It may seem that what we describe here is really elementary and well understood by all students. Unfortunately, the number of errors that arise in tests because of such inaccuracies as

$$\ln(1 + x) = \ln 1 + x = \ln(1) + x = x$$

shows that it is not something that should be neglected in this text.

[6] How does a calculator/computer find these values? Can we even trust it? We will answer this question in BIE-ZMA after studying Taylor series of functions.

[7] For instance in a test.

[8] Yes, the fact is only a convention.

Indices

At the end of this section we will mention the importance of upper and lower indices. **Upper indices** (or **superscripts**) are usually used to denote exponents, for instance

$$3^5, \quad a^n, \quad e^2 \quad \text{etc.}$$

Sometimes we use upper indices to denote vector components or the complex conjugate of a complex number a. Often we can see a^* instead of $\overline{a}$. In BIE-ZMA we will use upper indices to denote higher-order derivatives of functions.

Lower indices (or **subscripts**) are used to indicate either the order of an element in a sequence, or more generally, dependence of a given quantity on an integer parameter. This notation is similar to indexing array elements. In programming, `a[2]` means practically the same thing as our a_2. We will study sequences in more details in BIE-ZMA.

3.2 Sets and set operations

By a **set** we mean a collection of objects specified by enumeration, or by properties that the set elements must satisfy[9]. If the number of elements is small or if they can be simply listed, we write for instance

$$A = \{\pi, \mathrm{e}\}, \quad B = \{1, 2, 3, \ldots\}. \tag{3.4}$$

The set A contains exactly two elements (the numbers π and e). The set B consists of all natural numbers (readers must be clear about what elements to substitute for the three dots). If x is an element of A, we write $x \in A$, in the opposite case x is not an element of A and we write $x \notin A$. For the set A defined in (3.4) it is true that $\pi \in A$, but $1 \in A$ is false.

The **empty set**, i.e. a set containing no elements at all is denoted by the symbol $\emptyset$. If we want to list all elements of it we write

$$\emptyset = \{\}.$$

On the other hand, $\{\emptyset\}$ is a set consisting of the empty set $\emptyset \in \{\emptyset\}$, and therefore it is not empty.

If N is a set and $A(x)$ a formula about x, an element of N, then the set

$$C = \{x \in N \mid A(x)\}$$

consists of all $x \in N$ for which $A(x)$ is true. Here, $A(x)$ stands for a property whose truth depends on the actual value of the variable x. As an example, let $N = \mathbb{Z}$ and let $A(x)$ be the statement „x is an even number“. Then $A(2)$ is true but $A(3)$ is not. The set of all even integers can be described as follows

$$D = \{m \in \mathbb{Z} \mid m \text{ is divisible by two}\}.$$

We can also describe the set by enumerating it, $D = \{\ldots, -4, -2, 0, 2, 4, \ldots\}$, which may be slightly confusing. We can compare sets according to the elements they contain. We will call

[9] This naive definition can generally lead to logical paradoxes, perhaps the best known is Russell's paradox. By considering only „small“ subsets of number sets we will avoid all such problems. The notion of a set is studied in great detail by set theory, for example Zermelo-Fraenkel set theory from the beginning of the twentieth century.

a set A a **subset** of a set B, if and only if every element of A is also an element of B. In that case we write $A \subset B$ (A is contained in B) or $B \supset A$ (B contains A). The property of being a subset is what we call an *ordering* on sets. This ordering is not complete in the sense that there are (you will easily find them) sets A and B such that neither $A \subset B$ nor $B \subset A$.

Remark 3.3: Let's draw attention to a frequent misunderstanding here. Set inclusion (the property of being a subset) defined above is not strict. More precisely, for every set A we have that $A \subset A$. I.e. if $A \subset B$ then there need not be an element of B which is not contained in A. This remark relates to Remark 3.1. In principal, there are two approaches to the notation for strict (excludes equality) and non-strict (allows equality) inclusion:

1. $A \subset B$ denotes non-strict inclusion and $A \subsetneq B$ denotes strict inclusion,
2. $A \subseteq B$ denotes non-strict inclusion and $A \subset B$ denotes strict inclusion.

In this text and in the majority of courses at FIT you will meet the first approach. As a matter of fact, we do not even use the symbol for strict inclusion as it is not needed in most cases. It is always a good idea to find out what approach is used in the text.

We say that two sets A and B **are equal** if $A \subset B$ and at the same time $B \subset A$. Set equality is naturally written as $A = B$. This definition of equality gives us instructions how to prove equality of two sets, it is enough to verify both inclusions.

Set operations

We will recall basic operations with sets. For two sets A and B, their **intersection** is defined as the set of all elements which are in A and in B simultaneously. The intersection of two sets is denoted by $A \cap B$. Symbolically, we can describe this set as

$$A \cap B := \{x \mid x \in A \text{ and } x \in B\}.$$

The **union** of two sets A and B consists of all elements that are A or[10] in B. We denote it by $A \cup B$ and we write

$$A \cup B := \{x \mid x \in A \text{ or } x \in B\}.$$

The two operations can be naturally generalised to any number of sets. Let I be any (so called index) set and let A_i be a set for every $i \in I$. Then we put

$$\bigcap_{i \in I} A_i := \{x \mid x \in A_i \text{ for every } i \in I\},$$
$$\bigcup_{i \in I} A_i := \{x \mid \text{there exists } i \in I \text{ such that } x \in A_i\}.$$

Example 3.1: For example, for each natural i put

$$A_i = \left(1, 1 + \frac{1}{i}\right),$$

i.e. A_i is an open interval from 1 to $1 + \frac{1}{i}$. The intersection and union of these sets are

$$\bigcap_{i \in \mathbb{N}} A_i = \emptyset \qquad \bigcup_{i \in \mathbb{N}} A_i = (1, 2).$$

[10] This „or“ is not exclusive.

Another important set operation is the **difference**. of sets A and B, $A \setminus B$, which consists of all elements that are in A but not in B. Symbolically,

$$A \smallsetminus B := \{x \in A \mid x \notin B\}.$$

If A is a subset of a fixed set X, then $A^c := X \smallsetminus A$ is called the **complement** of the set A. However, X must be defined beforehand!

Question 3.1: What is $A \smallsetminus B$ and $B \smallsetminus A$ if $A = (1, 3)$ and $B = \langle 2, 4)$?

Note that while for any two sets A and B we have that

$$A \cup B = B \cup A \quad \text{and} \quad A \cap B = B \cap A,$$

this property (commutativity) is not valid for set difference. In general, the set $A \smallsetminus B$ is different from the set $B \smallsetminus A$.

Another basic operation on sets is the **Cartesian product**. Cartesian product of two sets A and B, written as $A \times B$, is the set containing all **ordered pairs** [11] of elements from A and B, i.e. pairs (a, b), where $a \in A$ and $b \in B$. We call a (resp. b) the first (resp. second) component of (a, b). Formally,

$$A \times B := \big\{(a, b) \,\big|\, a \in A \text{ a } b \in B\big\}.$$

Similarly, we can define the Cartesian product of more sets. For example, $A \times B \times C$ represents the set of all ordered triples of elements from A, B and C.

3.3 Number sets

In this part of the text, we will narrow our attention to sets of numbers. These sets will be one of the main objects of our interest in BIE-ZMA

Natural numbers

We denote the set of **natural numbers** [12] by $\mathbb{N}$,

$$\mathbb{N} := \{1, 2, 3, \ldots\}.$$

Natural numbers abstract the notion of the „count“ of objects. Figure 3.2 shows three sets of different geometrical shapes. Examples (a), (b) and (c) have the property of always having three shapes. We express this observation by stating that there are three shapes there and we denote it by Arabic numeral 3.

Note that the set of natural numbers is closed under multiplication and addition. More precisely, by multiplying and adding two natural numbers, we get a natural number again:

$$\text{if } a, b \in \mathbb{N} \text{ then } a + b \in \mathbb{N},$$
$$\text{if } a, b \in \mathbb{N} \text{ then } a \cdot b \in \mathbb{N}.$$

[11] It is necessary to distinguish between an ordered pair (a, b) and a set $\{a, b\}$. The sets $\{a, b\}$ and $\{b, a\}$ are the same, but ordered pairs (a, b) and (b, a) are generally not (for different a and b). An ordered pair contains information about the order of its elements, as opposed to a set.

[12] We denote the set of natural numbers with zero by $\mathbb{N}_0 := \{0, 1, 2, 3, \ldots\}$.

(a) (b) (c)

Figure 3.2: Groups in (a), (b) and (c) have a common feature, each group contains 3 shapes.

To appreciate positional notation of numbers using Arabic[13] numerals try to consider the problem of performing algebraic operations (addition, multiplication, subtraction) using the Roman numeral system. It's not easy, is it? Arabic numerals in Europe were promoted by Leonardo from Pisa (known as Fibonacci) in the beginning of the thirteenth century. In 1202 he published the *Liber abbaci* („The Counting Book"), which greatly aided the development of business and science. A courious reader can find out more interesting facts about the „first computational revolution" in this engaging book [3].

Integers

The set $\mathbb{N}$ is, however, not closed under subtraction of two natural numbers. We can also formulate this fact with the use of addition by saying that the equation

$$a = b + x \tag{3.5}$$

for some natural numbers $a, b \in \mathbb{N}$ may not have a solution x in natural numbers. Consider e.g. $a = 4$ and $b = 5$. In other words, we cannot express the concept of „debt" and „empty count" using only natural numbers.

To eliminate these shortcomings, we need to add zero and negative numbers to natural numbers. Thus we get the set of **integers**,

$$\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}.$$

In this set we can multiply, add and subtract, but the result of division is outside of this set. I.e. there need not be an integer solution to the equation

$$a = b \cdot x \tag{3.6}$$

for some integers a and b. This operation can be motivated by the need to divide an object into several parts. For example, when dividing one pizza ($a = 1$) into eight pieces ($b = 8$) we get eighths of pizza ($x = \frac{1}{8}$). We have to move to rational[14] numbers.

Rational numbers

The set of **rational numbers** consists of solutions to the equation (3.6) with non-zero b, which we write as fractions

$$\mathbb{Q} = \left\{ \frac{p}{q} \;\middle|\; p \in \mathbb{Z},\ q \in \mathbb{N},\ p, q \text{ coprime} \right\}. \tag{3.7}$$

[13] In fact, they came from India and were brought to Europe by Arab traders.

[14] Ratio – quotient.

We define addition and multiplication of fractions using operations in $\mathbb{Z}$ as follows[15]

$$\frac{p}{q}+\frac{r}{s}:=\frac{ps+qr}{qs},\quad \frac{p}{q}\cdot\frac{r}{s}:=\frac{pr}{qs},\quad \text{where}\quad \frac{p}{q},\,\frac{r}{s}\in\mathbb{Q}.$$

We can simplify the right-hand sides of these terms by dividing by common factors so we always get an element of the set (3.7). Integers are naturally included in the set of rational numbers, i.e. $\mathbb{Z}\subset\mathbb{Q}$, as fractions $\frac{p}{1}$, where $p\in\mathbb{Z}$, while algebraic operations are preserved.

Rational numbers $\mathbb{Q}$ together with addition $+$ and multiplication $\cdot$ satisfy important relationships

$$a+(b+c)=(a+b)+c,\quad a\cdot(b\cdot c)=(a\cdot b)\cdot c, \tag{3.8}$$

$$a\cdot(b+c)=(a\cdot b)+(a\cdot c) \tag{3.9}$$

valid for all rational numbers a,b,c. We call equalities (3.8) the **associative laws** for addition, resp. multiplication. Only thanks to these laws we can omit parentheses when writing chains of additions or multiplications since the final result actually does not depend on parentheses[16]. We call the equality in (3.9) the **distributive law**. The reader is certainly intimately familiar with it, because it can be used to perform the „factoring out“ operation. To be able to omit parentheses on the right-hand side of (3.9) we introduce the convention of precedence of multiplication over addition. An important element of the set of rational numbers is the number 0 which satisfies

$$0+a=a+0=a,$$

for any rational number a. For every rational a there is a rational number denoted by $-a$ with the property that

$$a+(-a)=(-a)+a=0.$$

The relationship between 0 and addition is analogous to the relationship between the number 1 and multiplication. For every rational number a we have that

$$1\cdot a=a\cdot 1=a.$$

Finally, for any non-zero rational number a there exists a rational number denoted by a^{-1} having the property that

$$a\cdot a^{-1}=a^{-1}\cdot a=1.$$

The previous paragraph can be summed up by saying that the set of rational numbers $\mathbb{Q}$ together with addition $+$ and multiplication $\cdot$ forms a **field**. The area of mathematics which studies[17] number fields is called general algebra. Finite[18] fields are widely used in modern encryption algorithms and generally, in computer security.

[15] At first glance, the definition of addition may seem incomprehensible. However, the motivation is simple. Imagine that we want to express what fraction of a pizza represent $\frac{2}{3}$ and $\frac{1}{4}$ of a pizza. To achieve this, we must first think about how to express these quantities in a „comparable“ way. Thirds and quarters can be completely divided into twelfths. So we have $\frac{8}{12}$ and $\frac{3}{12}$ of a pizza, in total $\frac{8+3}{12}=\frac{11}{12}$ of a pizza. Addition of fractions is just a generalization of this observation to all fractions. You certainly know this procedure under the name „conversion to a common denominator.“

[16] E.g. $(4+2)+1=4+(2+1)=4+2+1=7$. Note that this is not automatically true for an arbitrary binary operation. For example, if we consider division $\div$, $a\div b:=\frac{a}{b}$, then $\frac{1}{4}=(2\div 4)\div 2\neq 2\div(4\div 2)=1$.

[17] Among others.

[18] Having a finite number of elements.

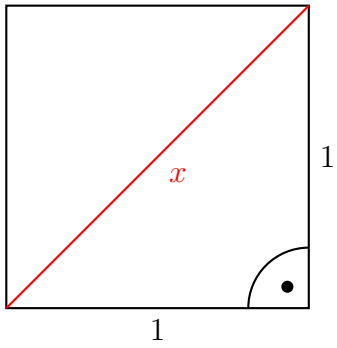


Figure 3.3: Square with side of length 1 and diagonal of length x.

In the set of rational numbers, we can therefore perform the so-called algebraic operations of addition, subtraction, multiplication and division (by non-zero numbers). This „numerical environment“ is fully sufficient to perform simple accounting and business operations that motivated the development of algebra in the Middle Ages. Unfortunately (or maybe fortunately) this numerical set is not sufficient to describe a number of practical problems. On the other hand, even such an old concept as rational numbers cannot be fully modelled on modern computers (as we do not have infinite memory).

Real numbers

At the beginning of this chapter we showed that natural numbers and integers are „not enough“. It was always necessary to add more numbers to meet our requirements. Similar situation also occurs in the case of rational numbers. This set is already closed under binary algebraic operations of addition and multiplication, but this time we encounter difficulties in analyzing the following geometric problem. Consider a square with side of length 1 (a rational number), see Figure 3.3.

We want to know the length of its diagonal. It can be constructed using a ruler and compasses. In Figure 3.3 it is denoted by x. According to the Pythagoras' theorem,

$$1^2 + 1^2 = x^2. \tag{3.10}$$

So $x^2 = 2$. We call this positive number x the square root of two and denote it by $\sqrt{2}$. We can easily show that this number is *not* rational as we have already shown in Theorem 2.1. So we face a serious problem. The length of the red line in Figure 3.3 cannot be expressed as a rational number! Does it mean that we cannot use the concept of a diagonal in this case? No, it just demonstrates the imperfection of rational numbers which will be solved by introducing the real numbers.

Other important irrational numbers are Ludolf's[19] number (traditionally marked by Greek letter π) or Euler's[20] constant (traditionally marked by Latin letter e). In a sense, there are considerably more[21] irrational numbers than rational numbers, one can say that a „typical“ real number is irrational. We will learn more about the relationship of these two sets in

[19] Ludolph van Ceulen, 1540 – 1610, a mathematician of Dutch origin, dedicated his life to calculating the number π to 35 decimal places that are even engraved on his tombstone.

[20] Leonhard Euler, 1707 – 1783, Swiss mathematician and physicist.

[21] Let us emphasize this idea. The reader may feel that we are adding only a few irrational numbers to rational numbers. But quite the opposite is true!

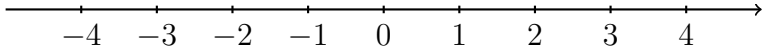


Figure 3.4: Number line

BIE-ZMA. The reader certainly knows that numbers can be imagined as points lying on a straight line, called the **number line**. A significant point corresponding to zero is selected on the line and a number a is plotted on the line at the distance of $|a|$ from 0. Positive numbers are placed on the right and negative numbers on the left of 0.

If we plotted only rational numbers on the line the resulting line would be „punctured“. For instance, there would be holes at the distance of $\sqrt{2}$ (to the right as well as left) from 0. To fill in the number line we must consider also irrational numbers. The requirement for the non-puncteredness of the real line is more accurately expressed by the „axiom of completeness“. We will deal with this issue in more detail in one of the first BIE-ZMA lectures.

Interestingly enough, it may not be easy to decide on rationality or irrationality of a number. There are numbers about which we *do not know* to which set they belong. An example is the **Euler-Mascheroni** constant defined by the formula[22]

$$\gamma := \lim_{n\to+\infty} \left(\sum_{k=1}^{n} \frac{1}{k} - \ln n \right) \approx 0.5772156649.$$

More information on this particular issue can be found in [5].

Complex numbers

It might seem that after adding irrational numbers to the rational ones no additional numbers are needed. Note that the geometrical consideration of the past paragraph can be simply reduced to the requirement (see the equation (3.10)) that the equation

$$x^2 - 2 = 0$$

have a solution in a given number set (here $\pm\sqrt{2} \in \mathbb{R}$). But a simple variation of this equation

$$x^2 + 1 = 0, \tag{3.11}$$

does not have a real solution[23] either. This equation can be solved by introducing an imaginary unit (we denote it by i), which satisfies $\mathrm{i}^2 = -1$ and hence is also a solution of the equation (3.11). We call i the **complex unit**. This new number can be multiplied by and added to any real number. In this way we get the **complex numbers**,

$$\mathbb{C} = \{a + b\mathrm{i} \mid a, b \in \mathbb{R}\}.$$

If $z = a + b\mathrm{i}$ is a complex number then the real number a is called the **real part** of z and the real number b the **imaginary part** of z. Two complex numbers are equal when their real parts and their imaginary parts are equal. We denote the real part of a complex number z

[22] You will learn more about limits in BIE-ZMA.

[23] That should be obvious. For any real number x its square x^2 is non-negative and so $x^2 + 1$ is always greater than or equal to one and it can never equal zero.

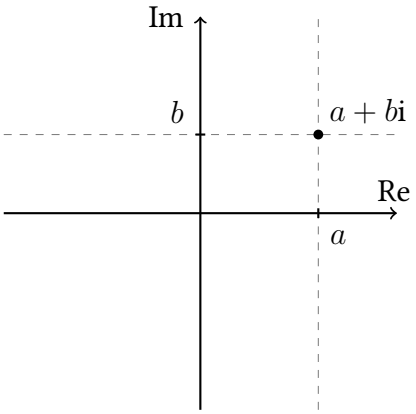


Figure 3.5: Complex plane.

by Re z and the imaginary part by Im z. Real numbers are naturally included in the set of complex numbers as we can identify a real number a with a complex number $a + 0\mathrm{i}$.

Algebraic operations on $\mathbb{C}$ are defined as follows:

$$(a + b\mathrm{i}) + (c + d\mathrm{i}) := (a + c) + (b + d)\mathrm{i},$$

$$(a + b\mathrm{i}) \cdot (c + d\mathrm{i}) := (ac - bd) + (ad + bc)\mathrm{i}, \quad a + b\mathrm{i},\ c + d\mathrm{i} \in \mathbb{C}. \tag{3.12}$$

Note that if $d = b = 0$ then $a + c$ and $a \cdot c$ has the same meaning as in real numbers. The set $\mathbb{C}$ together with these operations forms a field.

We can imagine complex numbers as points in the **complex plane**. We call the horizontal axis the **real axis** and the vertical axis the **imaginary axis**. A complex number $a + \mathrm{i}b$ is then represented by a point with coordinates (a, b), see Figure 3.5.

We define the **absolute value of a complex number** as

$$|a + b\mathrm{i}| := \sqrt{a^2 + b^2}, \quad a, b \in \mathbb{R}.$$

In the complex plane, we can imagine the absolute value of a complex number $a + b\mathrm{i}$ as the length of the segment joining 0 and $a + b\mathrm{i}$. We call $a - b\mathrm{i}$ the **complex conjugate** of $a + b\mathrm{i}$, $a, b \in \mathbb{R}$. The complex conjugate is thus obtained by reflection about the real axis.

Addition of complex numbers can be imagined as the addition of vectors (we add their „corresponding components“). Multiplication of complex numbers can be represented as rotation and scaling in the complex plane. This is not at all obvious but it can be derived from the definition of multiplication (3.12), see Figure 3.6. In particular, multiplication by the imaginary unit i can be seen, in the complex plane, as rotation by the angle $\frac{\pi}{2}$ relative to the origin of the coordinate system which corresponds to 0, counterclockwise.

The reason to introduce complex numbers may seem artificial. Now, the question is whether or not, when we examine solutions of polynomial equations other than (3.11), we will need another complex unit. This question was answered by Gauss[24] in his famous *Fundamental theorem of algebra*: every polynomial of degree n with complex number coefficients has n roots in the complex numbers[25]. So complex numbers are sufficient to solve polynomial equations.

[24] Johann Carl Friedrich Gauss (30 April 1777 – 23 February 1855) was a German mathematician.

[25] We count roots according to their multiplicity (e.g. the polynomial $x^2 - 4$ has two roots 2 and 2).

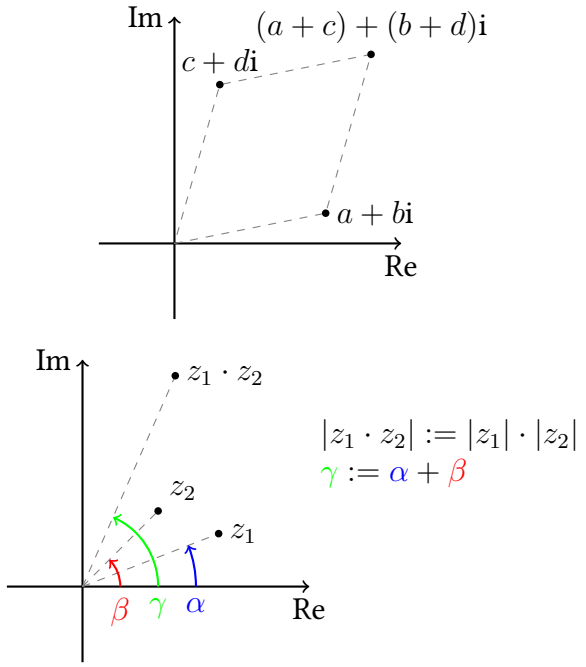


Figure 3.6: Geometric interpretation of addition and multiplication of complex numbers.

A number of mathematical methods applied in practice inherently use complex numbers. For instance the Fourier transform (resp. *Fast Fourier Transform*, FFT), used to analyze signal, could be only awkwardly described without the complex number apparatus. Without complex numbers it would be very difficult to formulate quantum physics, the theory behind a number of modern technologies that may completely change the issue of IT security in the near future.

At the end of this chapter, we would like to remark that complex numbers can be further extended to the (non-commutative) **field of quaternions**. This field has three complex units (i, j and k). In total there are four units (one real 1 and three „complex“ ones), thus the name. Relationships between these units are defined by formulas

$$\mathrm{i}^2 = \mathrm{j}^2 = \mathrm{k}^2 = -1 \quad \text{and} \quad \mathrm{ijk} = -1. \tag{3.13}$$

From these relationships you can derive other products of different combinations of units.

Question 3.2: From the definition in (3.13) derive the products

$$\mathrm{ij} \quad \text{and} \quad \mathrm{ji}.$$

The set

$$\mathbb{H} = \{a + b\mathrm{i} + c\mathrm{j} + d\mathrm{k} \mid a, b, c, d \in \mathbb{R}\},$$

together with operations defined analogously to complex numbers was introduced by Hamilton[26]. Why do we mention quaternions? Quaternions can be used to calculate, for example, the rotation of vectors in three-dimensional space. They are used by a number of algorithms implemented in graphics cards. If you are interested see here [2].

[26] Sir William Rowan Hamilton (4 August 1805 – 2 September 1865) was an Irish physisist and mathematician. After discovering the relationships in (3.13) he engraved them on a bridge in Dublin.

Question 3.3: Plot the following complex numbers in the complex plane.

$$\text{a) } z = (4+3\mathrm{i})(1-2\mathrm{i}), \quad \text{b) } z = (2-\mathrm{i})^2,$$
$$\text{c) } z = \mathrm{i}(1+\mathrm{i}), \quad \text{d) } z = \frac{1}{2+\mathrm{i}}.$$

3.4 Significant subsets of real numbers

In this chapter we will recall the definition of intervals and introduce some new notions describing the properties of subsets of real numbers.

Intervals represent important subsets of real numbers. For $a, b \in \mathbb{R}$, $a < b$, we define:

$$\begin{aligned}
(a,b) &= \{x \in \mathbb{R} \mid a < x < b\} && \text{open interval,}\\
[a,b] &= \{x \in \mathbb{R} \mid a \le x \le b\} && \text{closed interval,}\\
[a,b) &= \{x \in \mathbb{R} \mid a \le x < b\} && \text{left-closed and right-open interval,}\\
(a,b] &= \{x \in \mathbb{R} \mid a < x \le b\} && \text{right-closed and left-open interval,}\\
(a,+\infty) &= \{x \in \mathbb{R} \mid a < x\} && \text{open interval.}
\end{aligned}$$

The unbounded intervals $[a,+\infty)$, $(-\infty,a)$ and $(-\infty,a]$ are defined analogously.

Furthermore, for subsets of the real axis, we will recall the following definition. We call a set $A \subset \mathbb{R}$ **bounded from above** (resp. **below**), if there exists a constant $K \in \mathbb{R}$ such that for every $x \in A$, $x < K$ (resp. $x > K$). We call a set $A \subset \mathbb{R}$ **bounded**, if it is bounded from above as well as from below.

Let $A \subset \mathbb{R}$. We call a number $a \in A$ a **maximum of the set** A, if for every $x \in A$ we have that $x \le a$. We call a number $b \in A$ a **minimum of the set** A, if for every $x \in A$ we have that $x \ge b$. In other words, a maximum (resp. minimum) of a set A of real numbers is such an element of it which is greater (resp. less) than or equal to all other elements of the set. We also denote the maximum (resp. minimum) of a set A by $\max A$ (resp. $\min A$).

A maximum (respectively minimum) of a set defined in this way need not always exist. For instance, there is no minimum nor maximum of the set $(1,2)$ as numbers 1 and 2 do not belong to $(1,2)$. This problem can be solved by introducing an *infimum* and a *supremum* of a set which represent generalizations of minimum and maximum. We will study these notions in more detail in BIE-ZMA lectures.

Question 3.4: Which of the sets below are bounded from above, from below or bounded?

1. $\left\{\frac{1}{n} \,\middle|\, n \in \mathbb{N}\right\}$,
2. the set of all prime numbers,
3. the set of all solutions of the inequation $x^2 - (\pi+1)x + \pi > 0$,
4. $\{\sin x \mid x \in \mathbb{R}\}$.

Question 3.5: Determine the maxima and minima of the following sets if they exist.

1. $A = \{2, -1, 3\}$,
2. $B = (4, a]$, where $a > 4$ is a fixed parameter,

3. $C = \{(-1)^n \mid n \in \mathbb{N}\}$,

4. $D = \{2k - 3 \mid k \in \mathbb{N}\}$,

5. $E = \{2k - 3 \mid k \in \mathbb{Z}\}$.

Question 3.6: Prove or disprove this claim: every set which is bounded from above has a maximum.

3.5 Propositions and logical connectives

It is advantageous to write matematical statements in an abbreviated form using the symbolism of predicate logic. This area of mathematics will be discussed in detail in the Mathematical logic course (BIE-MLO). Using this approach, logical structure of statements that might otherwise be hidden from the reader behind sentences of natural (in our case English) language will emerge. At this point we will only briefly summarize the basics that are already known to the reader.

An **elementary proposition** is a sentence for which we can decide whether or not it is true. We denote propositions by capital letters $A,\ B,\ C, \ldots$ We often meet propositions which depend on a parameter x. We call them predicates and denote by $A(x)$. Different values of x therefore yield different predicates $A(x)$. Here are a couple of examples.

- Let x be an inhabitant of the Earth. $A(x)$ denotes the statement „x is a man“. If a denotes the author of this text then $A(a)$ is false.
- Let x be a natural number. $B(x)$ denotes the statement „x is even“. Then for instance $B(2)$ and $B(4)$ are true but $B(99)$ is not.

Let's recall basic **propositional connectives** (operations), which serve to construct more complex propositions from simpler ones. They are:

- $\neg A$, **negation**, A is false.
- $A \wedge B$, **conjunction**, A and B are true at the same time.
- $A \vee B$, **disjunction**, A is true or B is true.
- $A \Rightarrow B$, **implication**, if A is true then so is B, A implies B.
- $A \Leftrightarrow B$, **equivalence**, A is true if and only if B is true, A is equivalent to B.

The truth values of propositional connectives are determined by the truth table below depending on truth values of elementary propositions A and B.

A	B	$\neg A$	$A \wedge B$	$A \vee B$	$A \Rightarrow B$	$A \Leftrightarrow B$
0	0	1	0	0	1	1
0	1	1	0	1	1	0
1	0	0	0	1	0	0
1	1	0	1	1	1	1

In order to quantify variables in propositional formulas, we introduce three **quantifiers**

- $\forall$, **universal quantifier**, for every, for all.
- $\exists$, **existential quantifier**, there exists, for some.
- $\exists!$, $\exists_1$, there exists just one.

If a variable x ranges over all real numbers, we write $\forall x \in \mathbb{R}$. Similarly, if we say there exists an integer k, we write $\exists k \in \mathbb{Z}$. For clarity, we separate quantifiers in a formula by parentheses.

Example 3.2: A natural number p greater than 1 is a prime number, if every natural number k which is a factor of p is equal to 1 or to p itself. When we write it using quantifiers and propositional connectives we get this formula

$$(p > 1) \wedge (\forall k \in \mathbb{N})\big(k|p \;\Rightarrow\; (k = 1 \;\vee\; k = p)\big),$$

here we use $k|p$ to denote the predicate with the meaning „k is a factor of p“.

Example 3.3: Goldbach's conjecture is a simple mathematical statement which has been numerically tested for milions of cases but which has not been proved yet. This conjecture says that every even natural number greater than 2 can be expressed as the sum of two primes. If we denote the set of all primes by P and the set of all even numbers by $2\mathbb{N}$ then we can write Goldbach's conjecture as a formula

$$(\forall n \in 2\mathbb{N})((n > 2) \Rightarrow (\exists k, l \in P)(n = k + l)).$$

At the end of this section we will clarify one term frequently used (not only) in mathematical literature, which is that of a „sufficient“ and a „necessary“ conditions. If $A \Rightarrow B$ is true then A is a **sufficient condition for** B and B is a **necessary condition for** A.

The reason to use these names should be obvious. If $A \Rightarrow B$ is true and if we know that A is true then B must be true as well! Therefore A is *sufficient* for B to be true. On the other hand, if $A \Rightarrow B$ is true and if we know that B is false then A must be false as well. I.e. for A to be true B must *necessarily* be true.

3.6 Abbreviated writing of sums and products

Very often we come across the need to sum a finite sequence of numbers $a_1, a_2, \ldots, a_n$, or to discus the properties of such a sum. Instead of a lengthy and potentially ambiguous[27] expression

$$a_1 + a_2 + \cdots + a_n \tag{3.14}$$

we write

$$\sum_{k=1}^{n} a_k.$$

The summation sign, the symbol $\sum$ [28], is the enlarged capital Greek letter „S“ (*sum* in English, *summa* in Latin). A „local variable“ k is called the **index of summation**, 1 is the **lower**

[27] The reader could possibly misunderstand what to add instead of „dots“. It could happen that we do not give the readers easily comprehensible information, but an IQ test. The situation is further complicated if, in addition, each of the summands is a sum itself. For instance: $1 + 0 + 0 + 2 + 10 + 4 + 40 + \cdots + 365596 = ?$

[28] We also say *sigma* notation.

bound of summation and n the **upper bound of summation**. It does not matter what we call the summation index. For instance, the summations

$$\sum_{k=1}^{n} a_k \quad \text{and} \quad \sum_{j=1}^{n} a_j$$

are equal because they represent the same sum (3.14), which of course does not depend on any summation index (it does not contain k or j). Note, however, that the summation index under the summation sign as well as in the summands is always the same. On the other hand,

$$\sum_{k=1}^{n} a_j = \underbrace{a_j + a_j + \cdots + a_j}_{n\times} = k \cdot a_j,$$

which is something totally different.

Because addition is associative and commutative, (see equation (3.8)) we have that

$$\sum_{k=1}^{n}(a_k + b_k) = \sum_{k=1}^{n} a_k + \sum_{k=1}^{n} b_k. \tag{3.15}$$

Indeed, we can use the associative and commutative laws for addition and arrange the summands in a suitable way. Similarly, because of the distributive law (see equation (3.9)) it is true that

$$\sum_{k=1}^{n}(c \cdot a_k) = c \cdot \sum_{k=1}^{n} a_k, \tag{3.16}$$

where $c \in \mathbb{R}$ is a constant, i.e. a number independent on k. This equation represents the generalization of a familiar operation of „factoring out in front of brackets“. It is essential for both equations (3.15) and (3.16) that the lower bounds and the upper bounds are the same.

Let's demonstrate this concept on a concrete example. We want to talk about the sum of all natural numbers from 3 to 10. The shorthand is the following

$$S = 3 + 4 + 5 + 6 + 7 + 8 + 9 + 10 = \sum_{k=3}^{10} k. \tag{3.17}$$

Compare this expression to the use of the `for` cycle for finding this sum in C.

```
int main()
{
  int sum = 0;
  for (int k = 3; k <= 10; k++) sum += k;
  cout << 'The sum is: ' << sum << endl;
  return 0;
}
```

In order to calculate using the summation notation, it is helpful to know how to manipulate summation indices. For instance, the sum S in (3.17) can be also written as (we sum in the reverse order)

$$S = \sum_{k=1}^{8}(11 - k) = 10 + 9 + 8 + 7 + 6 + 5 + 4 + 3,$$

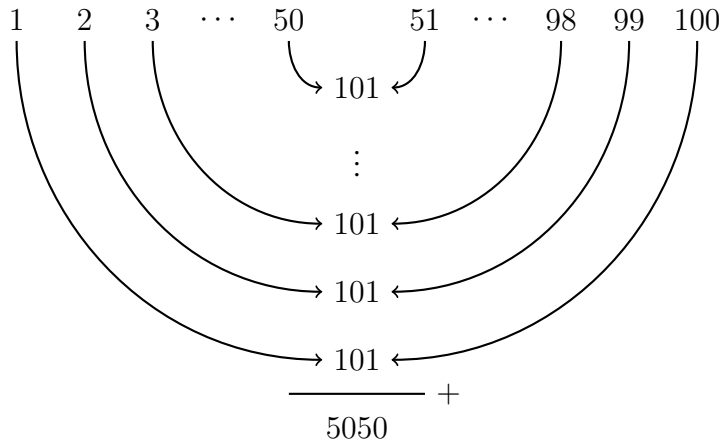


Figure 3.7: Gauss' trick for summing the first one hundred natural numbers.

or (the index of summation starts from 1 and we sum in the same order as originally)

$$S = \sum_{k=1}^{8} (2 + k).$$

The point of this paragraph is *One sum can be expressed in a number of equivalent ways.*

Sometimes the change of the bounds of summation has no influence on the result, such as here

$$\sum_{k=1}^{n} k^2 = \sum_{k=0}^{n} k^2.$$

We just added one summand for $k = 0$, and $0^2 = 0$.

Example 3.4 (Gauss trick)**:** The story goes that in elementary school, children were given the task to sum up all numbers from 1 to 100. To the surprise of the teacher, the young Gauss came up with an answer really quickly. He did not add the numbers one by one, but he noticed that if he adds the first number (i.e. 1) and the last number (i.e. 100) he gets 101. If he adds the second number (i.e. 2) and the one before last (i.e. 99), then he gets 101 again. If this way we can go all the way to $50 + 51 = 101$. This method is pictured in Figure 3.7. So, the result is

$$50 \cdot 101 = 5050.$$

The general formula for the sum of all numbers from 1 to some n is

$$\sum_{k=1}^{n} k = \frac{n(n+1)}{2} = n \cdot \frac{n+1}{2}. \tag{3.18}$$

The proof of Gauss' summation trick. Using the summation notation we can express Gauss' thoughts like this

$$\sum_{k=1}^{100} k = \sum_{k=1}^{50} \big(k + (101 - k)\big) = \sum_{k=1}^{50} 101 = 50 \cdot 101 = 5050.$$

Note that we can use the same trick for adding numbers from number 1 to an arbitrary number n:

$$2\sum_{k=1}^{n} k = \sum_{k=1}^{n} k + \sum_{k=1}^{n}(n+1-k) = \sum_{k=1}^{n}\big(k+(n+1-k)\big) =$$
$$= \sum_{k=1}^{n}(n+1) = n(n+1)$$

Thus we get the famous formula (3.18). □

To appreciate this result, one should consider the difference between the given task (to add up numbers from 1 to 100) and the formula. On the left-hand side of the equality

$$\sum_{k=1}^{100} k = \frac{100\cdot(100+1)}{2}$$

we have to carry out in total 99 operations of addition compared with one addition, multiplication and division on the right-hand side. That is why Gauss was the only one to get a good result. Note that if we increase n, the number of operations on the left-hand side will also increase, however, the number of operations required to evaluate Gauss' formula will be still the same. Implementing this particular sum using simple summation would therefore be considerably inefficient. Using Landau notation, this observation can be expressed by stating that the computational complexity of the sum itself is $\mathcal{O}(n)$ and of Gauss' formula it is $\mathcal{O}(1)$. You will learn about Landau notation in BIE-ZMA and especially BIE-ZDM lectures.

Another sum which can be expressed explicitly without the summation sign is shown in the next example.

Example 3.5 (Součet prvních několika členů geometrické posloupnosti)**:** For any real q different from 1 and a natural n we have that

$$\sum_{k=1}^{n} q^{k-1} = \frac{1-q^n}{1-q}. \tag{3.19}$$

The proof of the sum of a geometric sequence formula. We denote the expression in question by

$$S_n := \sum_{k=1}^{n} q^{k-1}, \quad n\in\mathbb{N}.$$

Note what this expression does when we multiply it by the quotient q. From the definition of S_n we have that

$$\begin{aligned} S_{n+1} &= 1+q+q^2+q^3+\cdots+q^{n-1}+q^n = 1+q\big(1+q+\cdots+q^{n-2}+q^{n-1}\big) = \\ &= 1+qS_n, \\ S_{n+1} &= S_n+q^n, \end{aligned}$$

which is valid for any positive natural n. By comparing the two formulas for S_{n+1} we get the equality

$$1+qS_n = S_n+q^n, \quad n\in\mathbb{N},$$

whence

$$S_n(1-q) = 1 - q^n, \quad n \in \mathbb{N}.$$

Assuming that $q \neq 1$, the formula (3.19) immediately follows. Alternatively, we could also refer to Remark 2.2. □

Question 3.7: Can we remove the assumption that $q \neq 1$ in the example above? Is it then necessary to change the formula (3.19)?

Question 3.8: To practise basic operations with sums calculate the sums below

$$\sum_{k=1}^{5} 1, \quad \sum_{k=1}^{6} k - \sum_{k=1}^{6} (k+1).$$

Question 3.9: Which of the below expressions can be uniquely interpreted (i.e. evaluated) without further specifications?

$$\text{a)} \sum_{k}^{4} k+1, \quad \text{b)} \, j \sum_{j=1}^{30} 30k,$$

$$\text{c)} \sum_{j} 2j, \qquad \text{d)} \sum_{j=1}^{2j} \sin j.$$

Abbreviation of product

Analogously to summation, there is an abbreviated notation for product. We use the Greek capital letter $\prod$ (read pi, product). For instance, the product of the first ten natural numbers can be written as

$$1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9 \cdot 10 = \prod_{k=1}^{10} k.$$

We work with products in a similar way as with sums. The only difference is that we use multiplication instead of addition; the underlying concept is the same. For example, we have that

$$\prod_{k=1}^{n} a_k \cdot b_k = \Big(\prod_{k=1}^{n} a_k\Big) \cdot \Big(\prod_{k=1}^{n} b_k\Big),$$

$$\prod_{k=1}^{n} c \cdot a_k = c^n \prod_{k=1}^{n} a_k.$$

3.7 Factorial and binomial coefficient

The **factorial** of a positive natural number n is defined as

$$n! := \prod_{k=1}^{n} k.$$

The factorial of zero is defined separately, $0! := 1$. The factorial of negative integers is not defined.

The factorial can be extended to all real numbers with the exception of negative integers. This extention is represented by a special function Γ, which has the property that $\Gamma(n+1) = n!$ for $n \in \mathbb{N}_0$ and, moreover, $\Gamma(x+1) = x\Gamma(x)$ for $x \in \mathbb{R} \setminus \{\ldots, -2, -1, 0\}$. The reader will certainly meet the Γ function in the Probability and Statistics course (BIE-PST).

The **binomial coefficient** is often used in practical calculations. For a natural n and integer k such that $0 \leq k \leq n$ we define

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

Although this definition looks confusing, the actual meaning of a binomial coefficient $\binom{n}{k}$ is simple. This number represents the number of possible selections of k items out of n objects where the order of selection does not matter and where we do not allow repeted selection of an item.

Often it is useful to know all binomial coefficients for a given n. Here, the **Pascal's triangle** will come in handy. First we will observe the equality

$$\binom{n}{k-1} + \binom{n}{k} = \binom{n+1}{k}. \tag{3.20}$$

Indeed,

$$\begin{aligned}\binom{n}{k-1} + \binom{n}{k} &= \frac{n!}{(n-k+1)!(k-1)!} + \frac{n!}{(n-k)!k!} = \\ &= \frac{n!}{(n-k)!(k-1)!}\left(\underbrace{\frac{1}{n-k+1} + \frac{1}{k}}_{\frac{n+1}{(n-k+1)k}}\right) = \\ &= \frac{(n+1)!}{(n-k+1)!k!} = \binom{n+1}{k}.\end{aligned}$$

Now imagine all binomial coefficients organised as a **Pascal's triangle**. The formula (3.20) then says that the sum of neighbouring binomial coefficients will be located one row below. See Figure 3.8.

The rows of a Pascal's triangle are enumerated starting from zero, i.e. the 0th row contains only 1, the first row reads $1, 1$, the second row reads $1, 2, 1$, etc. This method of enumeration is chosen so that $\binom{n}{k}$ lie in row n. It also makes it easer to remember the binomial theorem (see equation 2.1), the coefficients for $(a+b)^n$ are placed in row n.

3.8 Important constants

In applications we often encounter the need to use **Euler's number** e and **Ludolph's number** π. Approximate values of these constants with precision of one thousand decimal places are

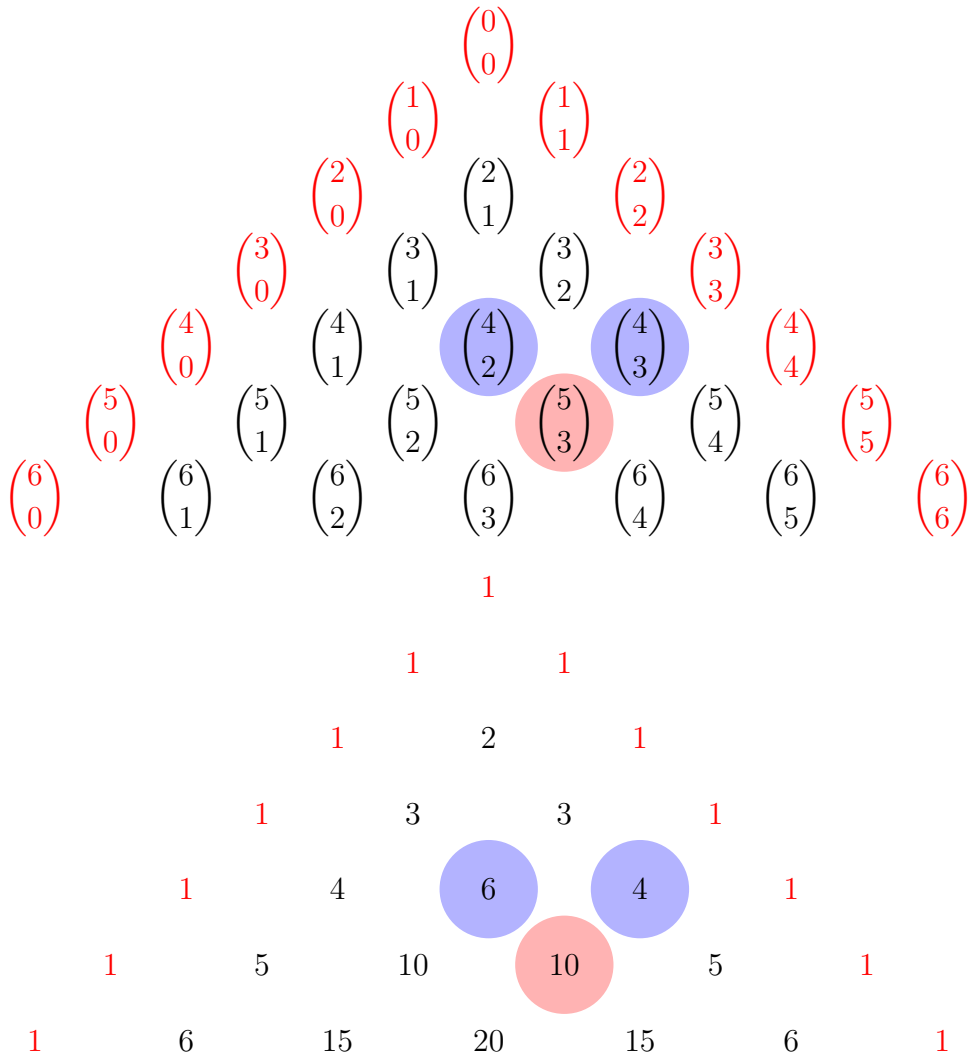


Figure 3.8: Pascal's triangle.

given below.

$$\pi \approx 3.14159265358979323846264338327950288419716939937510582097494459230781$$
$$640628620899862803482534211706798214808651328230664709384460955058223$$
$$172535940812848111745028410270193852110555964462294895493038196442881$$
$$097566593344612847564823378678316527120190914564856692346034861045$$
$$432664821339360726024914127372458700660631558817488152092096282925409$$
$$171536436789259036001133053054882046652138414695194151160943305727036$$
$$575959195309218611738193261179310511854807446237996274956735188575$$
$$272489122793818301194912983367336244065664308602139494639522473719070$$
$$217986094370277053921717629317675238467481846766940513200056812714526$$
$$356082778577134275778960917363717872146844090122495343014654958537$$
$$105079227968925892354201995611212902196086403441815981362977477130996$$
$$051870721134999999837297804995105973173281609631859502445945534690830$$
$$264252230825334468503526193118817101000313783875288658753320838142061$$
$$717766914730359825349042875546873115956286388235378759375195778185778$$
$$053217122680661300192787661119590921642019 \ldots$$

$$
\begin{aligned}
e \approx 2.&71828182845904523536028747135266249775724709369995957496696762772407\\
&66303535475945713821785251664274274663919320030599218174135966290435\\
&72900334295260595630738132328627943490763233829880753195251019011573\\
&83418793070215408914993488416750924476146066808226480016847741185374\\
&23454424371075390777449920695517027618386062613313845830007520449338\\
&26560297606737113200709328709127443747047230696977209310141692836819\\
&02551510865746377211125238978442505695369677078544996996794686445490\\
&59879316368892300987931277361782154249992295763514822082698951936680\\
&33182528869398496465105820939239829488793320362509443117301238197068\\
&41614039701983767932068328237646480429531180232878250981945581530175\\
&67173613320698112509961818815930416903515988885193458072738667385894\\
&22879228499892086805825749279610484198444363463244968487560233624827\\
&04197862320900216099023530436994184914631409343173814364054625315209\\
&61836908887070167683964243781405927145635490613031072085103837505101\\
&15747704171898610687396965521267154688957035035\ldots
\end{aligned}
$$

The definition of Euler's number will be discussed in detail in BIE-ZMA. It is not necessary to stress out the importance of π. One application of e is related to its being used as the base of the natural logarithm that we will be discussing in section 4.10.

4 Elementary functions

In this chapter we first discuss the concept of function and further summarize the properties of several known types of real functions of a real variable f.

4.1 What is it a function?

For the purposes of this text, the term „function“ is understood as follows:

Definition 4.1 (Real function of a real variable)**:** Let us have a non-empty set of real numbers $A \subset \mathbb{R}$. By **Real function of a real variable** (abbreviated function) f we mean an *unambiguous rule* that assigns to each number of A a unique real number. We denote such a function as $f : A \to \mathbb{R}$. If the function f assings to $a \in A$ the number b, we write $f(a) = b$. The number a is said **pre-image** of the number b and b is said **image** of a through the function f. We also say that $f(a)$ is the **value of the function** f at the point a.

Example 4.1: Let us consider the set $A = [-1, 1]$. Let us try to construct the function g such that „to each x in the set A it corresponds the real number y satisfying $x^2 + y^2 = 1$“. Can g be uniquely specified as a function $g : A \to \mathbb{R}$? Let us take $x \in A$. We ask if $y \in \mathbb{R}$ such that $x^2 + y^2 = 1$ can be found unambiguously. This is equivalent to solve the equality

$$y^2 = 1 - x^2. \tag{4.1}$$

Since $x \in A$, $1 - x^2 \geq 0$ and therefore the equation (4.1) has two solutions (for $x \neq \pm 1$)

$$y = \pm\sqrt{1 - x^2}.$$

Which y should we take? This is not an anumbiguous way to assign a number y to every x in A, as required in the definition of function. Therefore, we cannot construct a function as asked in this example. We need to slightly adjust the entry.

Example 4.2: Consider the set $A = [-1, 1]$. Let us try to construct a function g as follows: „to every x in the set A we assign a non-negative real y such that $x^2 + y^2 = 1$“. Can g be uniquely specified as a function $g : A \to \mathbb{R}$ in this way? We can start as in the previous example. Thus we solve (4.1) with respect to y for given $x \in A$. However now we realize that the equation has just one *non-negative* solution

$$y = \sqrt{1 - x^2}.$$

This y is the image of a given $x \in A$. Therefore, after this consideration, we see that g is now well defined aas a function. We can write g more explicitly as

$$g(x) = \sqrt{1 - x^2}.$$

Speaking of functions it is very often necessary to talk about displayed objects and possible functional values.

Definition 4.2: Let us take a function $f : A \to \mathbb{R}$ as defined in 4.1. We say that the set A is the **domain** of f and we denote it as D_f. The set

$$H_f := \{b \in \mathbb{R} \mid (\exists a \in D_f)(f(a) = b)\} \tag{4.2}$$

is said **image set** (or range) of the function f.

In the previous example the domain of the fuction g id $D_g = [-1, 1]$. Remember the meaning of the symbols used in equation (4.2). The set H_f contains all the real numbers b for which there exists a in the domain of f such that $f(a) = b$. We often denote the domain of the function f also without index, i.e. $D(f)$.

Here let us point out a frequent mistake. When a function $f : A \to \mathbb{R}$ is given, $\mathbb{R}$ *is not necessarely its image set.* For example, the function sin, that we will describe later, is in the usual notation denoted as 4.1 funkce sin : $\mathbb{R} \to \mathbb{R}$. However its image set is $H_{\sin} = [-1, 1]$, which certainly it is not the whole real axis.

The reader is certainly used to introduce a function as $f(x)$, using an explicit formula indicating what operations need to be done with the (real) x to get its image $f(x)$. This is not the only (nor most common) way to denote a function f. You will see other notations in BIE-ZMA. If a function is given thorugh a formula, without any further comment, then the set of all real x, for which $f(x)$ has meaning as a real number, is called the **natural domain** of the function f.

Example 4.3: Suppose a function is specified by the formula

$$h(z) = \sqrt{z^2 - 3z + 2},$$

without any comment on the domain. Its domain is then the above mentioned natural domain. We have to find it. For the square root to make sense, we need that its argument is non-negative, thus z belonging to the natural domain of h must satisfy

$$0 \leq z^2 - 3z + 2 = (z - 2)(z - 1)$$

The product of two real numbers is non-negative, if the given numbers are both non-negative or both non-positive. Thus z belong to D_h if it satisfies $z \geq 2$ and simultaneously $z \geq 1$ (i.e. $z \geq 2$) or $z \leq 2$ and simultaneously $z \leq 1$ (tj. $z \leq 1$). Therefore the natural domain of our function is

$$D_h = (-\infty, 1] \cup [2, +\infty).$$

Example 4.4: Not every formula specifies a function. For example, the expressions

$$\sqrt{-1 - x^2}, \quad \ln \ln \sin(x),$$

have no sense in the set of real numbers x.

To illustrate a function we can use its **graph**. If we introduce two orthogonal coordinate axes, denoted by default x (horizontal axis, independent variable) and y (vertical axis, dependent variable), we call graph of the function f the set which contains the pairs $(x, y) \in \mathbb{R} \times \mathbb{R}$ such $y = f(x)$. It holds then

$$\text{graph } f = \{(x, f(x)) \in \mathbb{R} \times \mathbb{R} \mid x \in D_f\}.$$

Now we will deal with several kinds of known functions. An overview of the properties of many functions can be found, for example, in [4].

Properties of functions

In order to easily talk about the behavior of functions, it is worthwhile introducing some useful terms. By slope, we distinguish the following types of functions:

Definition 4.3: A function f with domain $D_f \subset \mathbb{R}$ is said to be, on the set $A \subset D_f$,

- **increasing**, if $(\forall x, y \in A)\big(x < y \Rightarrow f(x) \leq f(y)\big)$,
- **stricly increasing**, if $(\forall x, y \in A)\big(x < y \Rightarrow f(x) < f(y)\big)$,
- **decreasing**, if $(\forall x, y \in A)\big(x < y \Rightarrow f(x) \geq f(y)\big)$,
- **strictly decreasing**, if $(\forall x, y \in A)\big(x < y \Rightarrow f(x) > f(y)\big)$,
- **monotonic**, if it is increasing or decreasing,
- **strictly monotonic**, if it is strictly increasing or strictly decreasing.

Here again, the reader is reminded that our nomenclature is not widely used in every country, it is used in Anglo-Saxon literature. It is therefore more likely that the reader will encounter it when searching the Internet and studying English literature.

In terms of symmetry, we distinguish between odd, even and periodic functions.

Definition 4.4: A function f is said

- even, if $(\forall x \in D_f)((-x \in D_f)$ and $(f(-x) = f(x)))$,
- odd, if $(\forall x \in D_f)((-x \in D_f)$ and $(f(-x) = -f(x)))$,
- periodic with period $T > 0$, if $(\forall x \in D_f)((x + T \in D_f)$ and $(f(x) = f(x + T)))$.

The graph of an even function is axially symmetrical with respect to the y axis. The graph of an odd function is symmetric with respct to the origin of the coordinates axis. The function value of an aperiodic function at a point x does not change with a shift to the point $x + T$, T being the period.

Finally, let us recall the notion of injective function here.

Definition 4.5: We call a function $f : D_f \to \mathbb{R}$ **injective**, when for very *different* number a and b from the domain of the function f also the functional values $f(a)$ and $f(b)$ are different. Equivalently, in symbols

$$(\forall a, b \in D_f)(a \neq b \Rightarrow f(a) \neq f(b)).$$

Alternatively, the requirement in the definition can be reformulated as follows: a function f is injective, if for every $a, b \in D_f$ such that $f(a) = f(b)$, ti holds that $a = b$.

Example 4.5: For example the function $f(x) = x^2$ defined on the whole $\mathbb{R}$ is not injective. The requirement in the definition is not met: it is enough to choose two different numbers, as for example $a = 1$ a $b = -1$, for which obviously $f(1) = f(-1)$. In contrast, the function $f(x) = x^3$ defined on the whole $\mathbb{R}$ is injective. Indeed, let us take two $a, b \in \mathbb{R}$ such that $f(a) = a^3 = b^3 = f(b)$. Does it follow from this that $a = b$? The use of a known algebraic formula results in equality

$$0 = a^3 - b^3 = (a - b)(a^2 + ab + b^2). \tag{4.3}$$

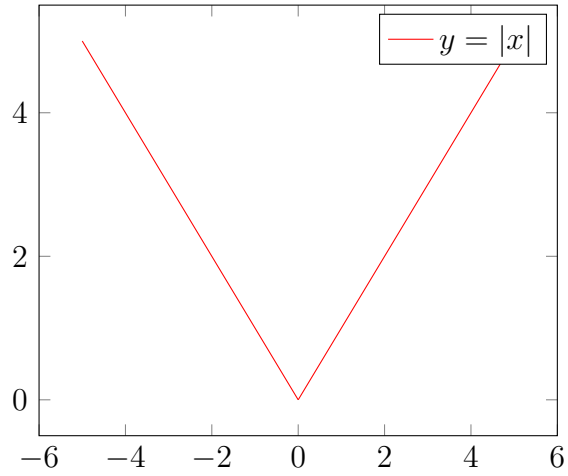


Figure 4.1: Graph of the absolute value.

The expression in the second bracket is zero only if $a = b = 0$. We can make sure of this by adjusting the square:

$$a^2 + ab + b^2 = a^2 + 2a\frac{b}{2} + \frac{b^2}{4} + \frac{3}{4}b^2 = \left(a + \frac{b}{2}\right)^2 + \frac{3}{4}b^2$$

If at least one of a, b is non-zero, then from (4.3) it necessarily follows $a = b$.

Remark 4.1: Frequent student myths include the statement: *The function f is injective when every element in the domain has just one image.* This statement applies to every function (it is in the definition of function)! It does not express the injectivity of the function.

4.2 The absolute value

For a real number x we set

$$|x| := \begin{cases} x, & x \geq 0, \\ -x, & x < 0. \end{cases} \tag{4.4}$$

The function $|x|$ is called **absolute value**. The notation used in equation (4.4) should be interpreted as follows: For given x grater or equal to 0, then $|x|$ is defined as x and in the case x is negative, $|x|$ is defined as $-x$. The graph of the function absolute value is plotted in picture 4.1.

Now let us summarize a few basic properties of the absolute value. Its The domain of the absolute values is the whole set of real numbers, i.e. $D_{|x|} = \mathbb{R}$. The image set of the absolute value is given by the set of all non-negative real umbers, thus $H_{|x|} = [0, +\infty)$. Indeed, from definition (4.4) we obtain the inequality $|x| \geq 0$ for every x and on the other hand for any $y \geq 0$ it holds $|y| = y$. Furthermore, directly from definition (4.4) it clearly follows that for every real x and y it holds

$$|-x| = |x|, \quad x \leq |x|, \quad -x \leq |x| \tag{4.5}$$

and (think about it!)

$$|x \cdot y| = |x| \cdot |y|, \quad \left|\frac{x}{y}\right| = \frac{|x|}{|y|} \quad \text{for } y \neq 0.$$

An important property of absolute value is the so-called **triangular inequality**.

Theorem 4.1 (triangular inequality)**:** For every real x and y the following inequality holds

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

Proof. Consider any real x and y. We have

- if $x + y \geq 0$, then $|x+y| = x + y \leq |x| + |y|$,
- if $x + y < 0$, then $|x+y| = -(x+y) = -x - y \leq |x| + |y|$.

Obviously, for every real z it applies $z \leq |z|$. □

Question 4.1: Prove or refute the claim: for every $x \in \mathbb{R}$ it holds $\sqrt{x^2} = x$.

4.3 Lower and upper integer part

Other frequently used and useful functions are the **lower integer part** and the **upper integer part** of a real number.

The lower integer part of a real number x is defined as the gratest integer number which is smaller than or equal to x and we denote it as $\lfloor x \rfloor$. Similarly, the upper integer part of a real number x is defined as the smallest integer number that is greater than or equal to x and we denote it as $\lceil x \rceil$. Thus, we could explicitly write (we just express symbolically what we have written in the previous sentences):

$$\lfloor x \rfloor = \max\{m \in \mathbb{Z} \mid m \leq x\},$$
$$\lceil x \rceil = \min\{m \in \mathbb{Z} \mid m \geq x\}.$$

The domain of the upper and lower integer part is the whole real line $\mathbb{R}$. Trivially, according to its definition, we are able to costruct $\lfloor x \rfloor$, resp. $\lceil x \rceil$, for every real number x. The set of values of these functions is then given by the set of all the integers, i.e. $\mathbb{Z}$. The graphs of the upper and lower integer parts are shown in the figure 4.2.

4.4 Linear function

We call **linear function** [1] any function, for which there exists costants $a, b \in \mathbb{R}$ such that

$$f(x) = ax + b \tag{4.6}$$

holds for every $x \in \mathbb{R}$. The graph of a linear function is a straigh line, see picture 4.3.

The domain of a linear function is the whole real line $\mathbb{R}$. If $a \neq 0$, then the image set of function (4.6) is given by the set of all real numbers. In the case $a = 0$ the image set of the function (4.6) is the set $H_f = \{b\}$. In short,

$$D_f = \mathbb{R},$$
$$H_f = \begin{cases} \mathbb{R}, & a \neq 0, \\ \{b\}, & a = 0. \end{cases}$$

[1] From the latin *linearis*, that means „straight“ or „direct“.

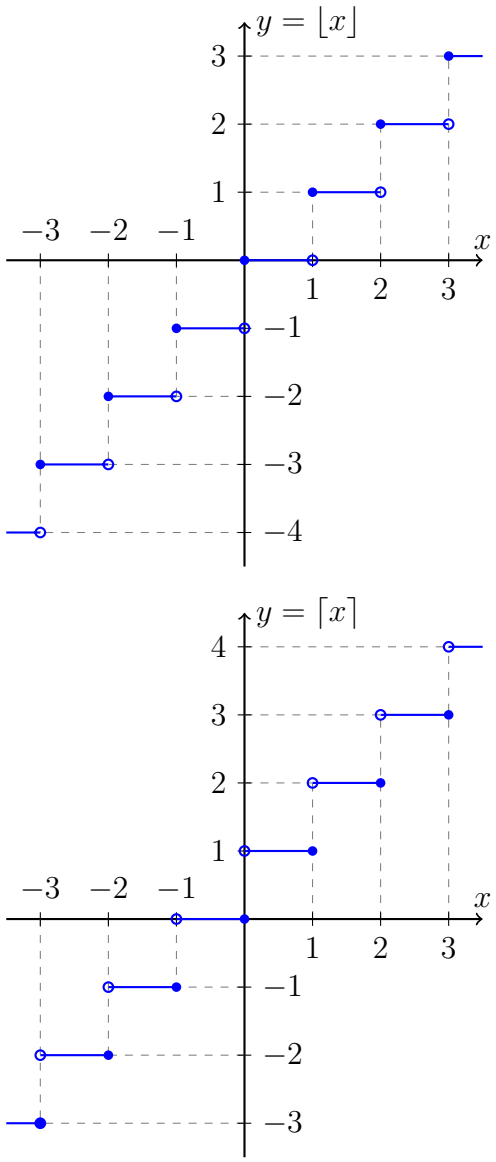


Figure 4.2: Graph of the lower (above) and upper (below) integer part.

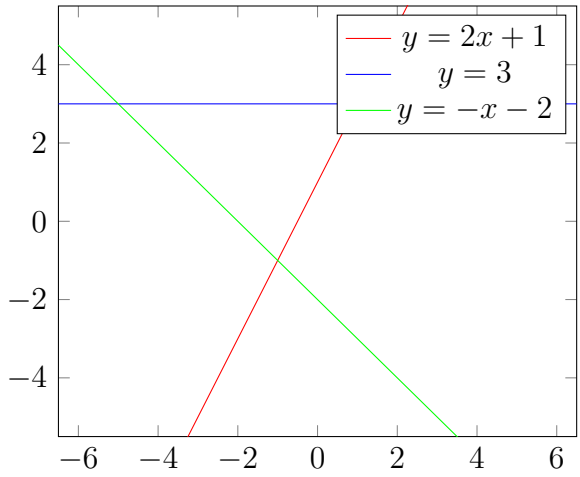


Figure 4.3: Graph of a linear function.

In the special case with vanishing a, i.e. $f(x) = b$, we speak of **constant function**.

The roots of a linear function are easy to find, for example the equation $ax + b = 0$ has solution $x = \frac{-b}{a}$ if a is not zero. In case $a = 0$ and b is not vanishing, then the corresponding equation has no solution and no intersection with the x axis exists. In case both a and b equal to zero, we have the zero fuction, whose roots are given by the set of all real numbers.

Question 4.2: At the beginning of this section it was said that the graph of each linear function is a straight line. On the contrary, is every straigh line the graph of a linear function?

Question 4.3: Above examples of a linear function $f(x) = ax + b$ have been metioned, which have just one, or no intersection with the x axis. Do they exhaust all the possibilities regarding the number of intersection with the x axis?

Remark 4.2 (Terminology)**:** In the second semester, you will study Linear Algebra (BIE-LIN), where the term *linear operator* plays a central role. At this point the reader should note that the word „linear“ in linear algebra means to require the following property:

$$f(x + \alpha y) = f(x) + \alpha f(y)$$

for all the vectors x, y and all the numbers α. This condition is satisfyed by the linear function introduced here only if $b = 0$, i,e. only when theirs graphs pass through the origin of the coordinates system. Our linear function $f(x) = ax + b$ for non-vaishing b is called in linear algebra **affine** function (operator).

4.5 Quadratic function

We call **quadratic function** a function f for which there exist constants $a, b, c \in \mathbb{R}$, with $a \neq 0$ such that

$$f(x) = ax^2 + bx + c \tag{4.7}$$

for every $x \in \mathbb{R}$. The domain of such a function is by definition the whole real line $\mathbb{R}$. The graph of a quadratic function is a **parabola**, see picture 4.4. The coordinates of the vertex of the parabola are easily revealed after **squaring**:

$$\begin{aligned} ax^2 + bx + c &= a\left(x^2 + 2 \cdot \frac{b}{2a} \cdot x + \left(\frac{b}{2a}\right)^2\right) + c - \frac{b^2}{4a} = \\ &= a\left(x + \frac{b}{2a}\right)^2 + c - \frac{b^2}{4a}. \end{aligned} \tag{4.8}$$

This adjustment is motivated by the simple requirement that the independent variable x occurs only in a squared expression. This is accomplished with the clever addition and subtraction of quadratic terms as shown here.

The squared bracket in (4.8) is always non-negative. From there it follows that the vertex of the parabola is located at the coordinate point

$$\left(-\frac{b}{2a}, c - \frac{b^2}{4a}\right).$$

From equation (4.8) it is evident that the sign of the coefficient a decides whether all functional values are greater (smaller) than or equal to $c - \frac{b^2}{4a}$. The image set of the quadratic function is therefore

$$H_f = \begin{cases} \left[c - \frac{b^2}{4a}, +\infty\right), & a > 0, \\ \left(-\infty, c - \frac{b^2}{4a}\right], & a < 0. \end{cases}$$

A well known formula applies to find the intersections $x_\pm$ of the function f with the x axis:

$$x_\pm = \frac{1}{2a}\Big(- b \pm \sqrt{b^2 - 4ac}\Big). \tag{4.9}$$

The equation $ax^2 + bx + c = 0$ has therefore real solutions only under the assumption of non-negativity of the **discriminant** $b^2 - 4ac$.

Proof of the formula for the roots of a quadratic function. The formula for the roots can be derived from a modification to a square. Looking for roots, i.e. solving the equation $ax^2 + bx + c = 0$ and by using the equality (4.8), we get

$$\left(x + \frac{b}{2a}\right)^2 = \frac{b^2 - 4ac}{4a^2}.$$

From here, the solution can be expressed as follows:

$$x = -\frac{b}{2a} \pm \frac{\sqrt{b^2 - 4ac}}{2|a|}.$$

Finally, by using the sign $\pm$, we can write in compact form

$$x_\pm = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a},$$

which is exactly (4.9). □

At this point, it should be pointed out that there can be many different proofs of a claim. Some may be easier, some more complicated. For example, if we just wanted to validate the present statement, that is, x_{pm} as given in (4.9) expresses the roots of a quadratic function (4.7), it is enough to proceed as follows[2]:

Alternative proof of the formula for the roots of a quadratic function. The validity of (4.9) can be easily verified by a simple substitution. Let us take x_+ and show that it is a root of (4.7).

$$\begin{aligned} ax_+^2 + bx_+ + c = a \cdot \frac{1}{4a^2}\left(- b + \sqrt{b^2 - 4ac}\right)^2 + \frac{b}{2a}\left(- b + \sqrt{b^2 - 4ac}\right) + c = \\ = \frac{1}{4a}\left(b^2 - 2b\sqrt{b^2 - 4ac} + b^2 - 4ac\right) - \frac{b^2}{2a} + \frac{b}{2a}\sqrt{b^2 - 4ac} + c = 0 \end{aligned}$$

Thus x_+ is indeed a root! Analogously, it can be verified that x_- is a root of (4.7), too. □

Question 4.4: Let as take $a > b > 0$. The numbers a and b are said to be in golden ratio[3], if the ratio $\frac{a+b}{b}$ is the same as $\frac{a}{b}$. What is then the value of $\varphi = \frac{a}{b}$?

[2] Of course, to do this, we should get that formula for the roots from someone, or we could guess it, by some ingenious idea.

[3] The value of this ratio is also sometimes called the golden section.

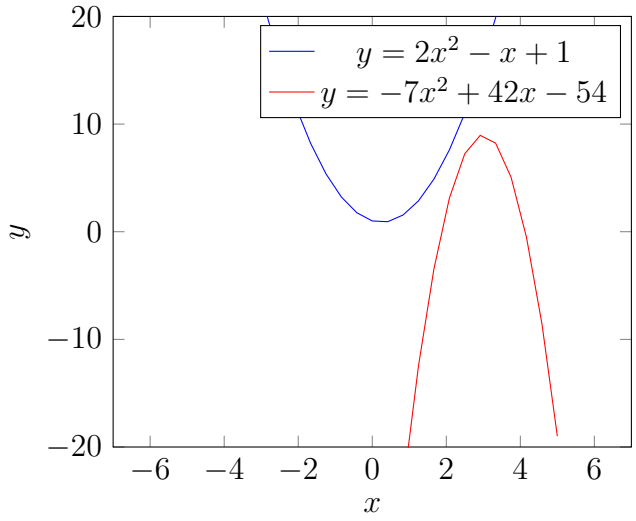


Figure 4.4: Graphs of two quadratic functions.

4.6 Polynomial function

It is certainly well known to the reader how to define the integer **power** of a real number a. Let us recall it here. For a natural number n we set

$$a^n := \underbrace{a \cdot a \cdots a}_{n \text{ times}} \tag{4.10}$$

and for $n = 0$, $a^0 := 1$ (in the context of this section, even in the case $a = 0$). For negative integers n and non vanishing a we define $a^n := \frac{1}{a^{-n}}$. The number $-n$ is then positive so we can use it in the denominator (4.10). For examples, it holds

$$\pi^0 = 1, \quad 2^4 = 2 \cdot 2 \cdot 2 \cdot 2 = 16, \quad 3^{-2} = \frac{1}{9}, \quad 0^0 = 1.$$

According to this definition of power, it is obvious that for every real non-zero a and integer k and n we have the important relationships (think!)

$$a^k \cdot a^n = a^{k+n} \quad \text{a} \quad \left(a^k\right)^n = a^{kn}. \tag{4.11}$$

The „power“ operation with $a > 0$ can be defined not only for integer coefficients. However, at this point it is not clear how to define (let alone calculate) the value of an expression such as for example 3^π or $1.2^{2.8}$. This issue is discussed in more detail in BIE-ZMA.

The generalizations of linear and quadratic functions are polynomials. We call **polynomial function** each function of the form

$$f(x) = \sum_{k=0}^{n} a_k x^k, \quad x \in D_f = \mathbb{R}.$$

If $a_n \neq 0$, we say that n is the **degree**. (or order) of f. The real constants $a_0, a_1, \ldots, a_n$ determine the function f as in previous cases the constants a, b, c did for the linear, resp. quadratic, function. These constants are often called polynomial coefficients. To emphasize

the field in which we work, we sometimes speak of the functions introduced above as *real polynomials*.

Of course, polynomial functions include both linear and quadratic functions. A common feature of polynomials is that only adding and multiplying operations are needed to calculate their functional values. In this sense, they are indeed one of the simplest (elementary) functions. In addition, these operations can be cheap on CPU, resp. FPU, and therefore the evaluation of polynomial functional values is easy.

The domain of any polynomial is the whole real line, $D_f = \mathbb{R}$. If the degree of the polynomial is odd, then its image set is $\mathbb{R}$. However, if the polynomial degree is even, then only a portion of the real axis contains the image set (in particular a certain interval or a point in the case of a constant polynomial).

Finding the roots of polynomials is generally a complicated task. Explicit formulas like for example (4.9), are known only for polynomials of degree 1, 2, 3 and 4. For higher degree polynomials, not only formulas for the roots are unknown, it is also *proven* that they do not exist. Let us emphasize this fact once more. If a polynomial of degree at least five is given, then the formula to find its roots does not exist and will never exist. When searching for roots then we have to resort to numerical methods[4].

Question 4.5: Which of the following functions is a polynomial?

1. $f(x) = x^2 + 2x + 3 + \frac{4}{x}$,
2. $f(x) = x \sin(2) - x^3$,
3. $f(x) = e^{2\ln(1+x^2)}$,
4. $f(x) = \frac{x^3+x}{x^2+1}$

The only high school „method“ to search for the roots of a polynomial $P(x)$ of degree greater than two[5] consists in repeating the following steps

1. guess one root, let us call it λ,
2. find (for example by the polynomial division) **the root factor**, i.e. factorize $P(x) = (x - \lambda)Q(x)$, where the polynomial $Q(x)$ is of one degree lower than $P(x)$,
3. return to the first point, but now guess the root of the polynomial $Q(x)$.

This process is repeated until we reach a polynomial of the degree two, for which we can find the roots by using the formula (4.9).

It is advisable to realize that this procedure is *not* an algorithm solving the task of finding the roots of a given polynomial. The first task is an esoteric step leaning on randomness. For example, try applying the procedure to the following polynomial (still of quite small degree):

$$12\,x^6 - x^5 + 57\,x^4 - 10\,x^3 - 9738\,x^2 + 759\,x + 47817.$$

At this point we advise the reader to review the polynomial division algorithm. This algorithm finds use not only in the task of finding the roots of polynomials, but also finds very important applications in computer security and encryption.

[4] See, for example, the bisection method or Newton's method discussed in BIE-ZMA.

[5] We can find the roots of polynomial of degree one and two easily.

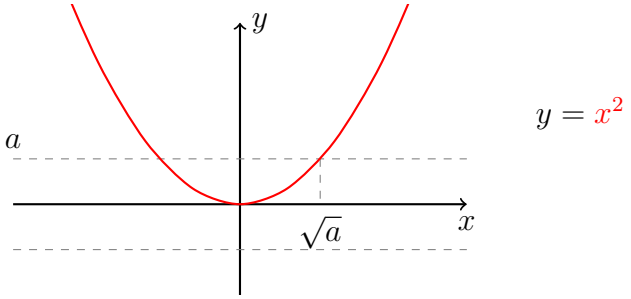


Figure 4.5: Construction of the square root of a number a.

Question 4.6: Find the roots of the following polynomials.

1. $x^2 + x - 12$,
2. $x^3 - 2x^2 - 5x + 6$,
3. $x^3 + 2x^2 - 4x - 8$.

4.7 Roots

Let us now consider a real number a and a natural number n. We use powers with natural exponents to define **natural roots** as a certain (see below) real solution of the equation $x^n = a$. We then symbolically denote this solution in the following two ways

$$a^{\frac{1}{n}} = \sqrt[n]{a}, \quad n \in \mathbb{N}.$$

It is necessary to distinguish between the cases of odd and even n and to consider whether such a construction makes sense or not.

Even roots

If it is $n = 2k$, $k \in \mathbb{N}$, thus n is *even*, then $x^n \geq 0$ for every $x \in \mathbb{R}$. This means that the equation $x^n = a$ has a real solution only for $a \geq 0$. This situation is shown in figure 4.5 for $n = 2$. For $a > 0$ the solutions of such equation are actullay two, since $x^{2k} = (-x)^{2k}$.

We define the **even root** $\sqrt[2k]{a}$ as the non-negative solution of the equation $x^{2k} = a$. Therefore, for example, $\sqrt{x^2}$ is $|x|$ and not x. For $a = 0$ the solution is just one and it is $\sqrt[2k]{0} = 0$.

From the above discussion, it is clear that the domain and the image set of the function $f(x) = \sqrt[2k]{x}$ are both given by the set $[0, +\infty)$. Furthermore, the following equality applies

$$\sqrt[2k]{x^{2k}} = \left(\sqrt[2k]{x}\right)^{2k} = x \quad \text{for every } x \geq 0.$$

In other words, $\sqrt[2k]{x}$ is the inverse function of x^{2k} restricted to the set $[0, +\infty)$. See picture 4.6 for $k = 1$. This will be discussed in more detail in BIE-ZMA.

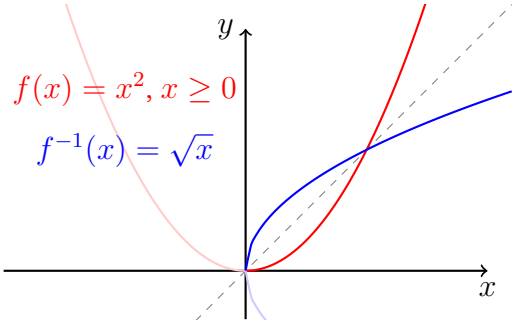


Figure 4.6: Square power and square root.

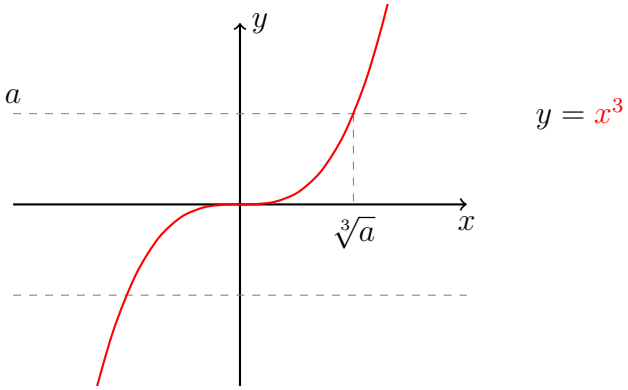


Figure 4.7: Construction of the cubic root of the number a.

Odd roots

If it is $n = 2k - 1, k \in \mathbb{N}$, thus n is *odd*, then the equation $x^{2k-1} = a$ has only one solution, that we call **odd power** of a and we denote it as $\sqrt[2k-1]{a}$. For example, $\sqrt[3]{-8} = -2$. See picture 4.7 for the case $n = 3$.

The domain and image set of an odd root are both given by the whole real line $\mathbb{R}$. An odd power and the corresponding odd root are inverse to each other, namely it holds

$$\sqrt[2k-1]{x^{2k-1}} = \left(\sqrt[2k-1]{x}\right)^{2k-1} = x \quad \text{for every } x \in \mathbb{R}.$$

For illustration in the case $k = 2$, see picture 4.8.

4.8 Rational function

We call **rational function** any function of the form

$$f(x) = \frac{P(x)}{Q(x)},$$

where P and Q are polynomials. Generally speaking, the domain of such a function is given by the set of all real numbers that does not contain roots of the polynomial Q, i.e.

$$D_f = \{x \in \mathbb{R} \mid Q(x) \neq 0\}.$$

Rational functions include linear, quadratic and all polynomial functions. Simply, you just have to set $Q(x) = 1$, for $x \in \mathbb{R}$ and P to be any polynomial.

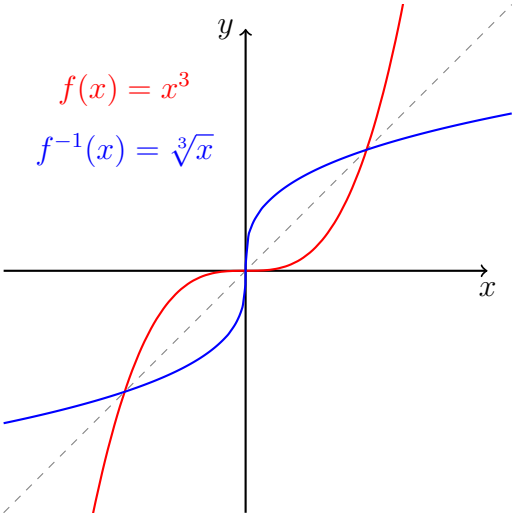


Figure 4.8: Cubic power and cubic root.

It is no longer easy to say something about the image set, so we will not dicuss this question. However, let us at least show a few examples illustrating that there can be very diverse situations (see picture 4.9).

4.9 Trigonometric functions

As **trigonometric functions** we name the functions sine (sin), cosine (cos), tangent (tg) and cotangent (cotg). Furthermore, in this chapter we will mention theirs *appropriately chosen* inverse functions, which are the functions arcsine (arcsin), arccosine (arccos) and arctangent (arctg).

The functions sine and cosine are defined by using the following geometric construction or algorithm. The input is the angle $alpha$ and the output is given by $\sin(\alpha)$ and $\cos(\alpha)$. While reading the algorithm, it is advisable to look at the picture 4.10.

1. Consider an orthogonal coordinate system with coordinate axis x and y and construct a unit circle K (i.e. a **unit circle** with radius 1 in the given axes units) and center point at the origin $(0, 0)$.

2. Clockwise from the positive direction of the x axes we measure the angle[6] α. One side of this angle is the positive x axis and we denote the other side by p.

3. Let A be the point at the intersection of p and K. Then we construct the point P as the intersection with the y axis of the line passing through A and parallel to x. In this way, we obtain the rectangular triangle OPA.

4. The length of the (oriented) side OP represents $\cos(\alpha)$ and the other (oriented) side PA represents $\sin(\alpha)$.

Of course, the accuracy of the result depends on the accuracy of our drawing tools. Infinite accuracy can only be achieved with infinitely accurate tools (here ruler, compass and

[6] the angle is measured in radians

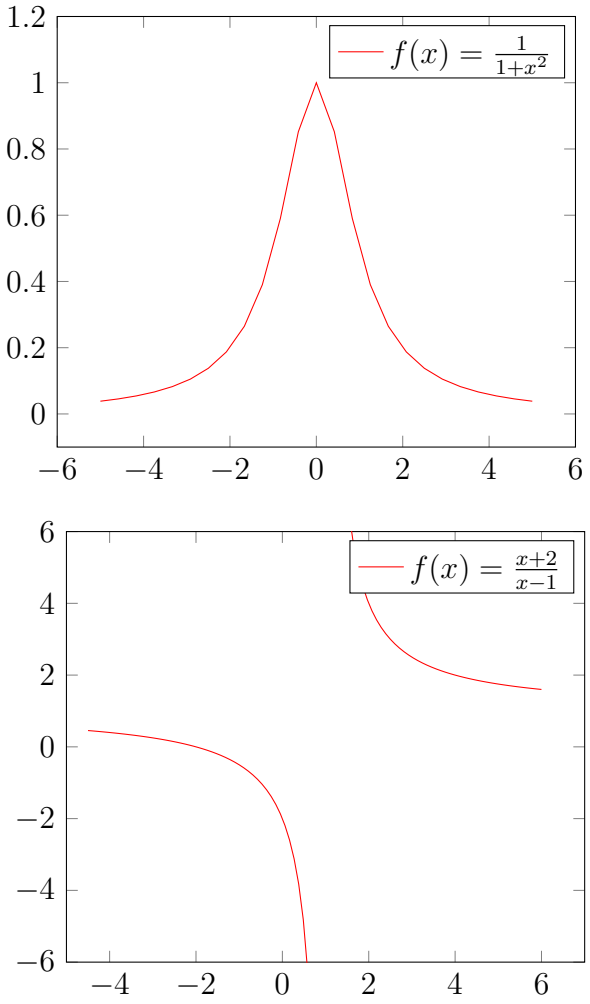


Figure 4.9: Examples of rational functions.

protractor). Obviously, this „calculation method“ is not very practical. In the course BIE-ZMA we will show how to effectively evaluate functional values of (not only) these functions.

The basic values of the sine and cosine functions are summarized in the following table and you can remind yourself of their graphs in figure 4.11.

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

From the construction of sine and cosine, it follows immediately the following equality

$$\sin^2(\alpha) + \cos^2(\alpha) = 1, \quad \alpha \in \mathbb{R}. \tag{4.12}$$

This equation is a consequence of the Pitagora's theorem applied to the triangle OPA with hypotenuse of lenght 1 and sides of lenght $\sin(\alpha)$ and $\cos(\alpha)$ (see the construction above and picture 4.10). Furthermore, it is evident from the construction that the sine function is odd and the cosine function is even, i.e.

$$\sin(-\alpha) = -\sin(\alpha) \quad \text{a} \quad \cos(-\alpha) = \cos(\alpha), \quad \alpha \in \mathbb{R}.$$

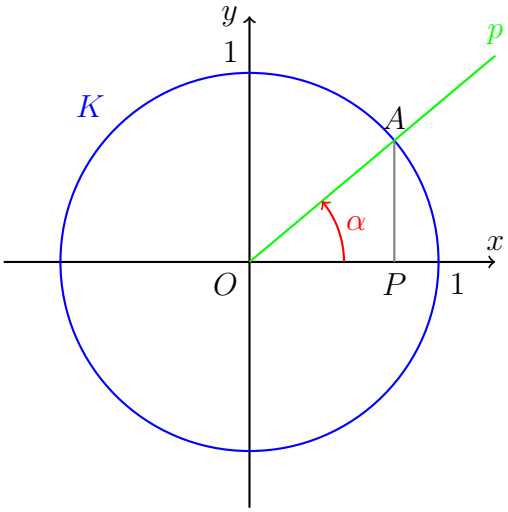


Figure 4.10: Geometric construction of the functions sine and cosine.

For the domain of these function we have

$$D_{\sin} = D_{\cos} = \mathbb{R}.$$

Their image set is

$$H_{\sin} = H_{\cos} = [-1, 1].$$

To conclude, both functions are **periodic** with period 2π, both functions are well defined on $\mathbb{R}$ and for every $x \in \mathbb{R}$ the equality $\sin(x + 2\pi) = \sin(x)$ and $\cos(x + 2\pi) = \cos(x)$ holds.

Very useful are the so-called **addition formulas** for the functions sine and cosine: for any real α and β, it holds

$$\sin(\alpha + \beta) = \sin(\alpha)\cos(\beta) + \cos(\alpha)\sin(\beta) \tag{4.13}$$

and

$$\cos(\alpha + \beta) = \cos(\alpha)\cos(\beta) - \sin(\alpha)\sin(\beta). \tag{4.14}$$

These formulas could be most easily derived using the property of multiplication of complex numbers by their goniometric expression.

By using the fact that sine is and odd function and cosine is an even function, from formulas (4.13) a (4.14) we immediately get analogous formulas for the difference of angles:

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

Similar formulas can be derived for both the tangent and cotangent functions. The meaning of these formulas and their use is obvious: if we have information about the values of $\sin\alpha$ and $\cos\beta$, then they allow us to get information for example on the value of $\sin(\alpha + \beta)$.

From formulas (4.13) and (4.14), we obtain the **double-angle formulas**, which are very often used:

$$\sin(2\alpha) = 2\sin(\alpha)\cos(\alpha),$$

and

$$\cos(2\alpha) = \cos^2(\alpha) - \sin^2(\alpha). \tag{4.15}$$

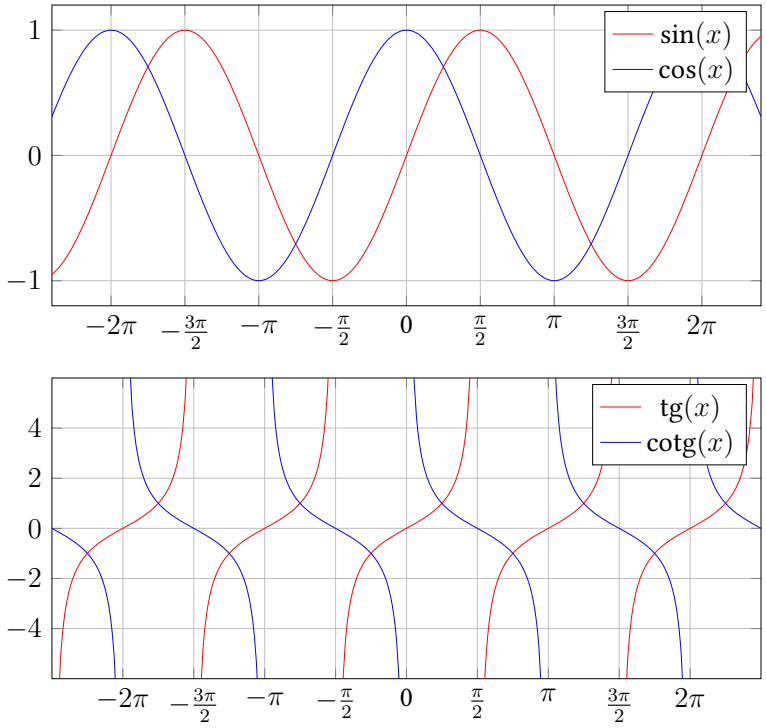


Figure 4.11: The trigonometric functions sin, cos, tg and cotg.

By using the relationships (4.12) and (4.15), we immediately derive formulas for the sine and cosine of half angle,

$$\cos^2(\alpha/2) = \frac{1}{2}\big(1+\cos(\alpha)\big), \quad \big|\cos(\alpha/2)\big| = \sqrt{\frac{1}{2}\big(1+\cos(\alpha)\big)},$$
$$\sin^2(\alpha/2) = \frac{1}{2}\big(1-\cos(\alpha)\big), \quad \big|\sin(\alpha/2)\big| = \sqrt{\frac{1}{2}\big(1-\cos(\alpha)\big)}.$$

If we want to get rid of absolute values in these formulas, we have to decide the sign of expressions based on the angle α, more precisely to which of the four quadrants in the Cartesian plane it belongs.

Through the functions sin and cos we define the functions tangent tg and cotangent cotg as

$$\operatorname{tg}\alpha := \frac{\sin\alpha}{\cos\alpha}, \quad \alpha \in D_{\operatorname{tg}} = \mathbb{R} \setminus \Big\{\frac{\pi}{2} + k\pi \,\Big|\, k \in \mathbb{Z}\Big\},$$
$$\operatorname{cotg}\alpha := \frac{\cos\alpha}{\sin\alpha}, \quad \alpha \in D_{\operatorname{cotg}} = \mathbb{R} \setminus \big\{k\pi \,\big|\, k \in \mathbb{Z}\big\}.$$

Their image set is the whole $\mathbb{R}$. For the sake of clarity, we present their graphs in picture 4.11.

Neither of the previously introduced trigonometric functions is injective on its domain. If you choose any y in the image set of sin, there exists infinite x in the domain of sin such that $\sin(x) = y$ (see picture 4.11). Therefore, for any given $y \in H_{\sin}$, it cannot be unambiguously specified $x \in D_{\sin}$ satisfying $y = \sin(x)$. The same observation applies to cos, tg and cotg. Trigonometric functions are not injective on their natural domain and therefore can not have inverse functions... unless we restrict them appropriately, that is, we reduce their domain. In accordance with the established convention, we define

- **arcsine**, arcsin, as the inverse function of sin restricted on the interval $[-\frac{\pi}{2}, \frac{\pi}{2}]$,

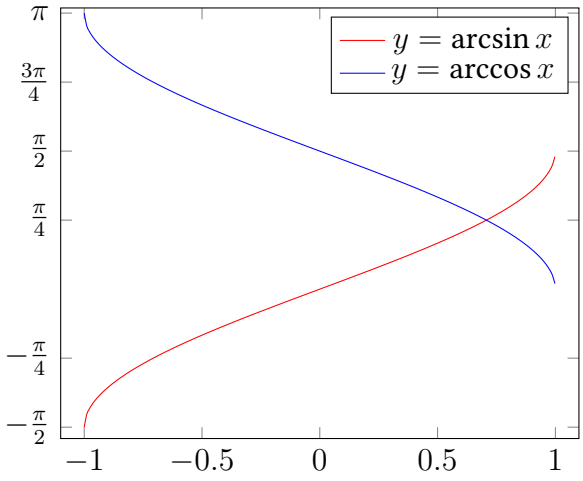


Figure 4.12: Graph of the functions arcsin and arccos.

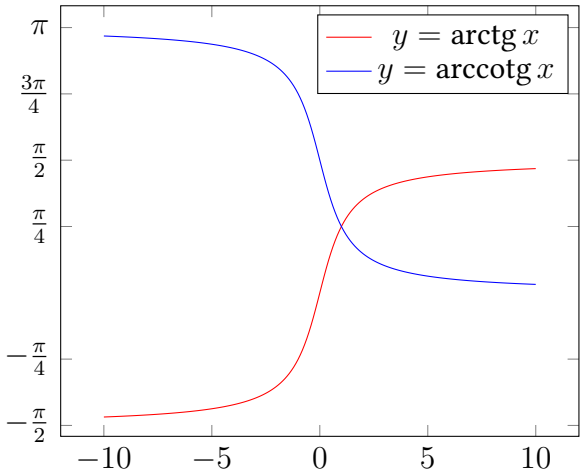


Figure 4.13: Graph of the functions $\operatorname{arctg} x$ and $\operatorname{arccotg} x$.

- **arccosine**, arccos, as the inverse function of cos restricted on the interval $[0, \pi]$,
- **arctangent**, arctg, as the inverse function of tg restricted on the interval $(-\frac{\pi}{2}, \frac{\pi}{2})$,
- **arccotangent**, arccotg, as the inverse function of cotg restricted on the interval $(0, \pi)$.

Question 4.7: From the geometric definition of the functions sin and cos derive the values of $\sin \frac{\pi}{3}$ and $\cos \frac{\pi}{3}$.

Question 4.8: From the geometric definition of the functions sin and cos derive the values of $\sin \frac{\pi}{4}$ and $\cos \frac{\pi}{4}$.

Question 4.9: Without using a calculator (it would not give the result exactly) find the value of the following expressions.

1. $\arcsin \sin \dfrac{9\pi}{4}$,
2. $\sin \dfrac{7\pi}{4}$.

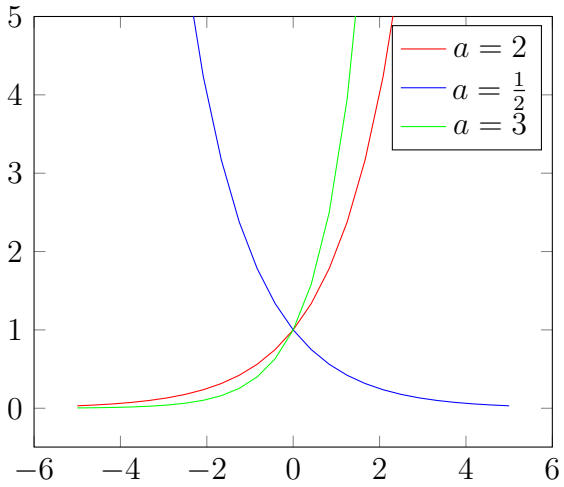


Figure 4.14: Exponential functions.

Question 4.10: Derive the addition formula for the function tg, i.e. express $\mathrm{tg}(x+y)$ by using $\mathrm{tg}(x)$ and $\mathrm{tg}(y)$.

4.10 Exponantiation and logarithm

For $0 < a \neq 1$ the function[7]

$$f(x) = a^x, \quad x \in D_f = \mathbb{R},$$

is called **exponentiation of base** a. This function extends the operation of elevation to power to non-integer exponents. For any real numbers x and y, it applies the well known equality

$$a^x \cdot a^y = a^{x+y} \quad \text{a} \quad \left(a^x\right)^y = a^{xy}.$$

In figure 4.14 the graph of the function f is shown for different bases a.

In general, for $a > 1$ f is strictly increasing (i.e. $f(x) < f(y)$ for any $x < y$), $D_f = \mathbb{R}$ and $H_f = (0, +\infty)$. For $a < 1$, f is strictly decreasing (i.e. $f(x) > f(y)$ for any $x < y$), $D_f = \mathbb{R}$ and $H_f = (0, +\infty)$.

Logarithm

The **logarithm** is the inverse function of the exponentiation (only in the case of base different from one, otherwise the exponential function is not injective). More specifically, from the graph of the exponential function $f(x) = a^x$, $a \neq 1$, we see that for every real number y there exists a real x such that $a^x = y$. We say that a function with such a property is injective (in this case on the whole $\mathbb{R}$) and therefore invertible on its image set. The inverse function of the exponentiation of base a, $0 < a \neq 1$, is said **logarithm of base** a and we denote it as $\log_a$. The domain of the exponentiation is the whole $\mathbb{R}$ and its image set is the interval

[7] We will see in the course BIE-ZMA the definition of the generic power, ie a^x, for positive a and real x. In secondary schools, the concept is axiomatic.

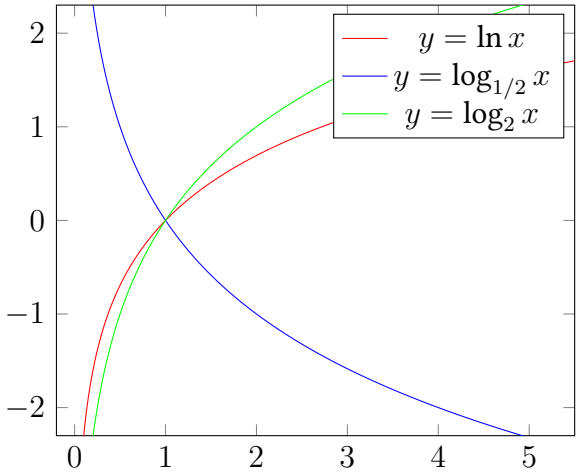


Figure 4.15: Graph of some logarithmic functions with different bases.

$(0, +\infty)$. From this it follows that the domain of the logarithm, since it the function inverse of the exponentiation, is $D_{\log_a} = (0, +\infty)$ and its image set is $H_{\log_a} = \mathbb{R}$.

The reader has certainly already indirectly encountered logarithms through applications. For example the Richter scale (that measures the intensity of earthquakes) or the decibel scale (measuring the intensity of sound) are logarithmic.

Important properties of the logarithm can be derived from properties of the exponentiation:

$$a^{\log_a x} = x, \quad x > 0, \tag{4.16}$$

$$\log_a a^x = x, \quad x \in \mathbb{R}, \tag{4.17}$$

$$\log_a xy = \log_a x + \log_a y, \quad x, y > 0, \tag{4.18}$$

$$\log_a x^y = y \log_a x, \quad x > 0 \text{ a } y \in \mathbb{R}. \tag{4.19}$$

Indeed, the first two equalities, (4.16) and (4.17), are merely an expression of the inverse relationship between the exponential and the logarithm, thus they apply by definition. Let us prove the equality (4.18). For positive x, y there exist real u, v such that

$$x = a^u \quad \text{a} \quad y = a^v.$$

From this we have

$$xy = a^u \cdot a^v = a^{u+v}.$$

Thus

$$\log_a xy = u + v = \log_a x + \log_a y.$$

In a similar way, the property (4.19) can be proven.

Remark 4.3: The reader is certainly familiar with the operation called *remove the logarithm*. That is, saying the following: if

$$\log_a x = \log_a y,$$

for some $x, y > 0$ and $0 < a \neq 1$, then

$$x = y.$$

This operation is no magic. It is just about using the injectivity of the function $\log_a$. The same can be done with any injective function!

Question 4.11: Which is the domain of the function $f(x) = \log_a x^2$?

5 Analytical geometry

Let no one ignorant of geometry enter here.

Inscription above the entrance to Platonic Academy

5.1 Basic notions

We will recall how geometric objects in a plane can be described using equations. These concepts are very useful because, as everyone knows, the output periphery of an overwhelming number of electronic devices are two-dimensional (monitors, paper, projectors, etc.).

Consider an orthogonal coordinate system with axes x, y and origin O in a plane. A point in this plane is described by two numbers called **coordinates**. For example, if a point A has coordinates $(1, 2)$, we write[1] $A = (1, 2)$, or, using square brackets, $A = [1, 2]$. The point A lies at the intersection of a line parallel to the y-axis which cuts the x-axis at number 1 and a line parallel to the x-axis which cuts the y-axis at number 2. The situation is shown in detail in Figure 5.1.

Another important geometric object is the **vector**. We will denote vectors by lower case letters with arrows, e.g. $\vec{a}$, $\vec{b}$, $\vec{c}$. We understand a vector as a pair of numbers[2] giving

[1] We do not use expressions such as $A[1, 2]$ to denote point coordinates. This notation rather evokes the feeling in the reader that A is a function of two variables. In addition, it is dangerously similar to Mathematica syntax.

[2] We will write vectors as rows although it would be more correct to write them as columns. You will learn more about this topic in BIE-LIN.

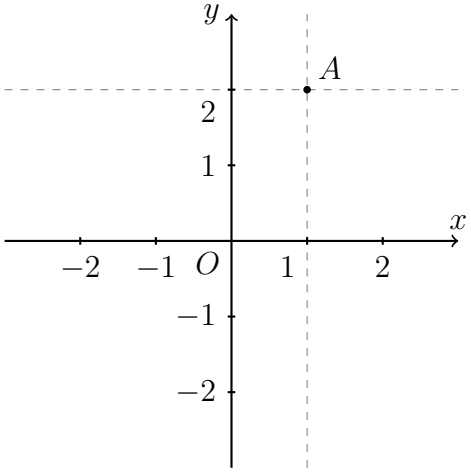
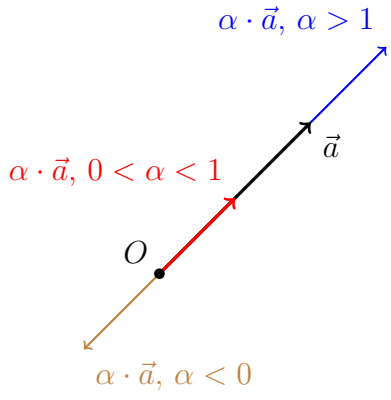
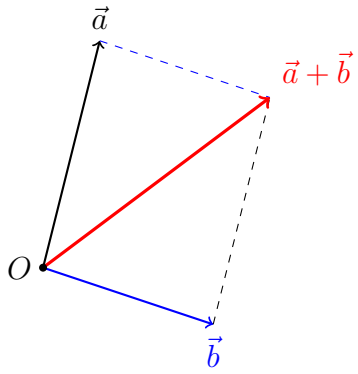


Figure 5.1: Orthogonal coordinate system and point $A = (1, 2)$.



(a)



(b)

Figure 5.2: Geometric interpretation of scalar multiplication (a) and vector addition (b).

a direction; if we have a vector $\vec{a} = (a_1, a_2)$ then the numbers a_1 and a_2 are called **vector components** of $\vec{a}$. We can add vectors and multiply them by a number using the rules

$$\alpha \cdot (a_1, a_2) := (\alpha a_1, \alpha a_2), \quad (a_1, a_2) + (b_1, b_2) := (a_1 + b_1, a_2 + b_2). \tag{5.1}$$

For obvious reasons we sometimes say that vector addition and scalar multiplication (multiplication of a vector by a number) defined in (5.1) are done „componentwise“. Equality of vectors is defined intuitively. We say that two vectors $\vec{a} = (a_1, a_2)$ and $\vec{b} = (b_1, b_2)$ are equal if their components are equal, i.e. if $a_1 = b_1$ and $a_2 = b_2$, and we write $\vec{a} = \vec{b}$. Geometric interpretation of vector addition and scalar multiplication is shown in Figure 5.2.

We can multiply a vector by a number. Can we also multiply two vectors? For that purpose we define **scalar product** [3]. Standard[4] scalar product of two vectors $\vec{a} = (a_1, a_2)$ and $\vec{b} = (b_1, b_2)$ is defined by this rule

$$\vec{a} \cdot \vec{b} := a_1 b_1 + a_2 b_2.$$

[3] You are certainly also familiar with the *vector product*, which assigns to a couple of three-dimensional vectors another three-dimensional vector. However, as this chapter concerns only planar objects we will not discuss this operation in more detail here.

[4] There are more ways, even infinitely many, of defining scalar product. You will find out more about this topic in BIE-LIN.

The product is called *scalar*, because the result is not a vector but a number (a scalar). Furthermore, scalar product is related to the angle between vectors. The angle between two vectors $\vec{a}$ and $\vec{b}$ is $\alpha \in \langle 0, \pi)$, if and only if

$$\cos\alpha = \frac{\vec{a} \cdot \vec{b}}{\|\vec{a}\| \, \|\vec{b}\|}.$$

Length of a vector $\vec{a} = (a_1, a_2)$ is defined by the Pythagoras' theorem. It is denoted by $\|\vec{a}\|$ and computed as

$$\|\vec{a}\| := \sqrt{a_1^2 + a_2^2} \quad \text{for } \vec{a} = (a_1, a_2).$$

Note that the length can be also expressed using scalar product as $\|\vec{a}\| = \sqrt{\vec{a} \cdot \vec{a}}$.

You will study these and other geometric objects in the BIE-LIN course, for more than two dimensions as well.

5.2 The line

The simplest geometric structure (apart from the point) is the **line**. To describe a line p completely we need to know a point A which is contained by the line and a direction of the line, i.e. a non-zero vector $\vec{a}$. The line p then consists of all points with coordinates

$$(x, y) = A + t \cdot \vec{a}, \quad t \in \mathbb{R}. \tag{5.2}$$

The number t is called a parameter as it parametrises the points on the line. Note that if we bound the set of possible values of t we get only parts of the line. For instance, for $t \in \langle 0, +\infty)$ we get a ray with the initial point A and direction $\vec{a}$, whereas for $t \in \langle 0, 1\rangle$ we get a line segment with A and $A + \vec{a}$ as its end points. This way of describing a line, i.e. by an equation (5.2), is often called the **parametric equation of a line**.

An alternative way of describing a line is this. A line consists of all points with coordinates (x, y) which satisfy the **linear equation of a line**

$$ax + by + c = 0. \tag{5.3}$$

Constants a, b, c are parameters of the line. In equation (5.3), the symbols x and y represent unknowns. A point (α, β) is contained in the given line if and only if after substituting α for x and β for y into (5.3) we get a valid equality ($0 = 0$). Let's analyze in more detail the line p described by equation

$$x - 2y + 1 = 0. \tag{5.4}$$

The point $(1, 2)$ does not lie on p because after substituting to (5.4) we get $-2 = 0$ which is not true. On the contrary, $(-1, 0)$ and $(0, 1/2)$ after substituting give $0 = 0$ and so they do lie on the line. Two points are sufficient to plot a line.

We assume that the reader knows how to convert a parametric equation of a line to its linear equation and vice versa.

Question 5.1: Convert the parametric equation of a line into a linear equation: $(x, y) = (1, 2) + (2t, -t)$, $t \in \mathbb{R}$.

Question 5.2: Convert the linear equation into a parametric equation for $3x - 2y + 1 = 0$.

Question 5.3: Construct a linear equation of a line containing points $(1, -3)$ and $(2, 4)$.

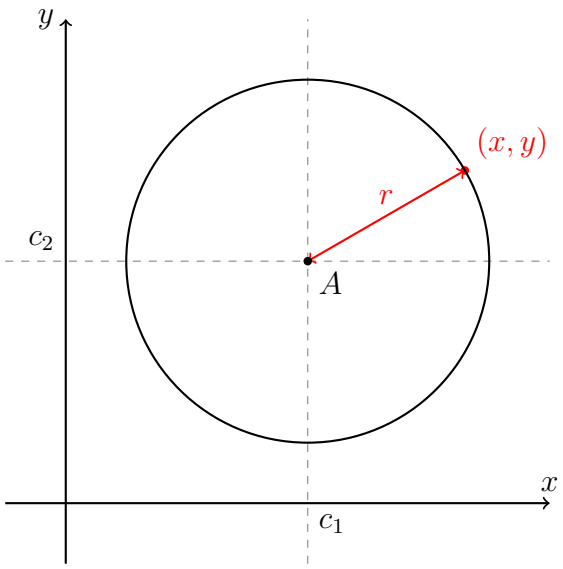


Figure 5.3: Circle with centre at point $(c_1, c_2) \in \mathbb{R}^2$ and radius $r > 0$.

5.3 The circle and the ellipse

The **equation of a circle** can be formed easily if we recall the **Pythagoras' theorem**. again. A circle with centre at point $C = (c_1, c_2)$ and radius $r > 0$ is the set of all points (x, y) whose distance from C is equal to r. Hence

$$(x - c_1)^2 + (y - c_2)^2 = r^2$$

This situation is shown in Figure 5.3.

The **equation of an ellipse** is given by

$$\frac{(x - c_1)^2}{a^2} + \frac{(y - c_2)^2}{b^2} = 1,$$

where a and b are positive parameters and $A = (c_1, c_2)$ is the centre of the ellipse. The parameters a and b define the length of the semi-major axis and the semi-minor axis. If $a = b$ then we get a circle. A typical ellipse is depicted in Figure 5.4.

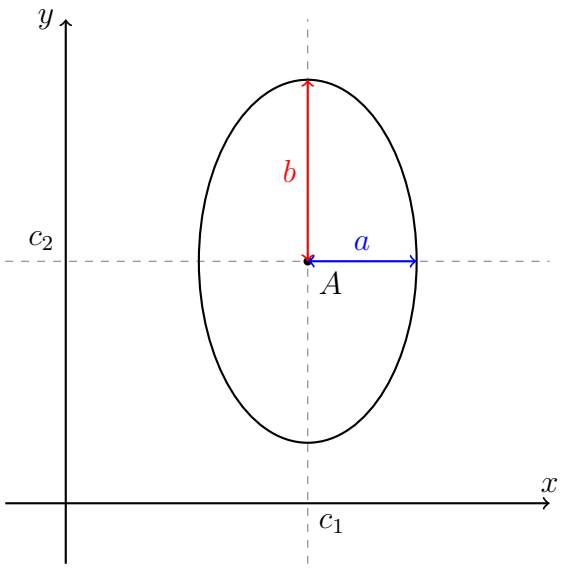


Figure 5.4: Ellipse with centre at $(c_1, c_2) \in \mathbb{R}^2$, semi-major axis b and semi-minor axis a, $0 < a < b$.

6 Warning

The BIE-ZMA course is taught at the Faculty of Information Technology, therefore many students have a warm relationship to the various computer algebraic systems (CAS), be it particular programs (Mathematica, Maple, Matlab, Sage, Maxima,...) or on-line applications (WolframAlpha, CoCalc). We would like to point out here that although we generally welcome the use of these systems, users that are not familiar with various parts of mathematics may find the outputs and behaviour of such systems confusing.

We will mention some of the classic traps.

6.1 Smart calculators are too smart

How come that $\ln(-1)$ or $\sin(\mathrm{i})$ are evaluated and do not return an error?

Virtually all elementary functions can be extended almost to the entire set of complex numbers. And indeed, $\ln(-1) = \mathrm{i}\pi$ and $\sin(\mathrm{i}) = \mathrm{i}\sinh(1)$. There is not enough time to study the calculus of complex numbers in BIE-ZMA. However, we will at least mention how to define e^z for any complex number z.

Mathematica, for example, works implicitly in „complex mode“. This may be very confusing for an uneducated user.

How come that $\sqrt[3]{-1}$ is evaluated as $\frac{1}{2} + \frac{\sqrt{3}}{2}\mathrm{i}$ and not as -1?

If you are curious you can easily verify that this answer is not wrong:

$$\left(\frac{1}{2} + \frac{\sqrt{3}}{2}\mathrm{i}\right)^3 = \left(\underbrace{\frac{1}{4} + \frac{\sqrt{3}}{2}\mathrm{i} - \frac{3}{4}}_{-\frac{1}{2}+\frac{\sqrt{3}}{2}\mathrm{i}}\right) \cdot \left(\frac{1}{2} + \frac{\sqrt{3}}{2}\mathrm{i}\right) =$$
$$= -\frac{3}{4} - \frac{1}{4} = -1.$$

The „problem“ is that in complex numbers there are in total three solutions to the equation

$$z^3 = -1, \quad z \in \mathbb{C}.$$

The one solution that we got is what we call principal solution – the solution with the least „argument“. We repeat again the calculus of complex numbers is not part of the BIE-ZMA course.

Equality in CAS Mathematica

In CAS Mathematica there are several symbols for equality with the following meaning:

- Symbol == denotes logical equality (comparison, writing equations).
- Symbol = denotes assignment.
- Symbol := denotes „delayed evaluation“.

We will demonstrate the various meanings using the example below. The output of this piece of code

```
a = 4;
b = a;
Print[b]
a = 2;
Print[b]
```

is

```
4
4
```

On the other hand, the cell containing

```
a = 4;
b := a;
Print[b]
a = 2;
Print[b]
```

results in the output

```
4
2
```

6.2 Frequently asked questions

Here you will find an overview of most frequent questions, problems and mistakes which students meet especially at the beginning of the course and which can already be discussed now.

We did/called/denoted it differently at high school

It is possible and it is also quite all right. However, you cannot expect that all people around the world will comply with the approach you were taught at high school. Different people may use different conventions and may have very good reasons for doing so.

If you use some materials to study it is a good idea to first make yourself familiar with the language which is used in the text. For example, the BIE-ZMA course material starts with

a list of symbols and ends with a list of names which helps readers to find definitions they need quickly.

We can demonstrate this situation on the names used in connection with monotonous functions and sequences (increasing, strictly increasing, non-increasing, etc.). There are a lot of different nomenclatures. However, we will only use one set of names to avoid misunderstanding. See lectures and lecture notes.

This remark does not only apply to mathematics but it is generally valid.

Inclusion

Not only in BIE-ZMA, the symbol $\subset$ is used to denote inclusion and we do not distinguish between a subset and a proper subset. I.e., the inclusion $A \subset B$ holds if and only if every element of the set A is also an element of the set B. In particular, for any set A we have that $A \subset A$. We can make do with this one notion without a problem throughout the whole course.

Texts which do distinguish between subsets and proper subsets usually use special symbols $A \subseteq B$ and $A \subsetneq B$ for that end.

Domains of trigonometric functions

The functions sin, cos, tg are not injective and therefore they do not have inverses. However, we can restrict them to sets on which they are injective and then construct inverse functions on such sets. There are infinitely many ways of rectricting these functions in such a way. The *standard* choice is the following:

$$\begin{aligned}
\operatorname{arcsin} &= \left(\sin\Big|_{\langle -\pi/2,\pi/2\rangle}\right)^{-1},\\
\operatorname{arccos} &= \left(\cos\Big|_{\langle 0,\pi\rangle}\right)^{-1},\\
\operatorname{arctg} &= \left(\operatorname{tg}\Big|_{(-\pi/2,\pi/2)}\right)^{-1}.
\end{aligned}$$

Hence we have that

$$\begin{aligned}
D_{\arcsin} &= \langle -1,1\rangle, \quad H_{\arcsin} = \langle -\pi/2,\pi/2\rangle,\\
D_{\arccos} &= \langle -1,1\rangle, \quad H_{\arccos} = \langle 0,\pi\rangle,\\
D_{\operatorname{arctg}} &= \mathbb{R}, \qquad\quad H_{\operatorname{arctg}} = (-\pi/2,\pi/2).
\end{aligned}$$

Zero to the power of zero

The algebraic expression 0^0 is defined as 1. Zero in the exponent denotes an empty multiplication (there are no numbers to be multiplied) and so the result is the identity element for multiplication which is 1. Similarly, the empty sum evaluates to 0, the identity element for addition.

Necessary condition, direction of an implication

If an implication $A \Rightarrow B$ is true then we often call B a *necessary condition* for A. If B is not true then A cannot be true either (because if A were true then so would be B).

7 List of the used symbols

The table below is compatible with the notation used in the lectures and exercises of BIE-ZMA.

Symbol	Meaning
$=$	symbol of equality
$:=$	equality by definition, the expression on the left is defined on the right
$a \leq b$	a is less than or equal to b
$a \geq b$	a is greater than or equal to b
$a < b$	a is less than b
$a > b$	a is greater than b
$\mathbb{N} = \{1, 2, \ldots\}$	set of natural numbers
$\mathbb{N}_0 = \{0, 1, 2, \ldots\}$	set of natural number plus 0
$\mathbb{Z}$	set of integer numbers
$\mathbb{Q}$	set of rational numbers
$\mathbb{R}$	set of real numbers
$\mathbb{C}$	set of complex numbers
Re z	real part of the complex number z
Im z	imaginary part of the complex number z
(a, b)	open interval, or an ordered pair or point in a plane
$[a, b]$	closed interval
$A \subset B$	A is a subset of B, it admits $A = B$
$A \cup B$	union of the sets A and B
$A \cap B$	intersection of the sets A and B
$A \setminus B$	set difference
$A \times B$	Cartesian product of the sets A and B
$\lvert A \rvert$	number of elements of the set A
$x \in A$	x is an element of the set A
$x \notin A$	x is not an element of the set A
$\wedge$	conjunction
$\vee$	disjunction
$\Rightarrow$	implication
$\Leftrightarrow$	equivalence
$\forall$	universal quantifier
$\exists$	existential quantifier
D_f nebo $D(f)$	domain of a function f
H_f nebo $H(f)$	image set of a function f
e	Euler's number
π	Ludolph's number

Symbol	Meaning
i	imaginary unit
sin	function sine
cos	function cosine
tg	function tangent
cotg	function cotangent
arcsin	function arcsine
arccos	function arccosine
arctg	function arctangent
$\log_a$	logarithm of base a, $0 < a \neq 1$
ln	natural logarithm, i.e. $\log_e$
log	decimal logarithm, i.e. $\log_{10}$
$\lfloor x \rfloor$	lower integer part of the real number x
$\lceil x \rceil$	upper integer part of the real number x
$\lvert x \rvert$	absolute value of the number x
$n!$	factorial of the number n
$\binom{n}{k}$	binomial coefficient

The following table lists frequently used Greek letters with their name.

Greek letter	Upper case	Name	LaTeX
α		alpha	alpha
β		beta	beta
γ	Γ	gamma	gamma
δ	Δ	delta	delta
ϵ		epsilon	epsilon
ζ		zeta	zeta
η		eta	eta
θ	Θ	theta	theta
κ		kappa	kappa
λ	Λ	lambda	lambda
μ		mu	mu
ν		nu	nu
ξ	Ξ	xi	xi
π	Π	pi	pi
ρ		rho	rho
σ	Σ	sigma	sigma
τ		tau	tau
φ	Φ	phi	varphi
χ		chi	chi
ψ	Ψ	psi	psi
ω	Ω	omega	omega

Answers to some questions

2.1 The numbers $\frac{3}{4}$ and $\sin\frac{\pi}{6} = \frac{1}{2}$ are rational, $\frac{\pi}{2}$ and $\sin\frac{\pi}{4} = \frac{\sqrt{2}}{2}$ are irrational.

2.2 1. non-coprime (both can be divided by 7), 2. neither coprime nor non-coprime, it is not a pair of integers, 3. coprime (both are prime numbers).

2.3 $\sum_{j=1}^{n}(2j-1) = n^2$. The proof by mathematical induction is easy and left to the reader.

3.1 $A \setminus B = (1,2)$, $B \setminus A = \rangle 3,4)$

3.2 From ijk $= -1$ by multiplying with k from the right we have $-$ij $= -k$ and so ij $= k$. Similarly, from ijk $= -1$ by multiplying with i from the left and then with j from the left we get $-$k $=$ ji.

3.3 a) Re $z = 10$, Im $z = -5$, b) Re $z = 3$, Im $z = -4$, c) Re $z = -1$, Im $z = 1$, d) Re $z = \frac{2}{5}$, Im $z = -\frac{1}{5}$.

3.4 a) bounded, b) bounded from below, c) not bounded from above or below, d) bounded.

3.5 a) min $A = -1$, max $A = 3$, b) has no minimum, max $B = a$, c) min $C = -1$, max $C = 1$, d) min $D = -1$, has no maximum, e) has no maximum neither minimum.

3.6 The claim is not true, for instance consider $(0,1)$.

3.7 Yes, if $q = 1$ then $\displaystyle\sum_{k=1}^{n} q^{k-1} = n$.

3.8 5, -6.

3.9 None, all expressions are ambiguous.

4.1 The statement is not true, consider any negative number x. For every real number x it holds $\sqrt{x^2} = |x|$.

4.2 It is not. For example, any straight line parallel to the y axis is not a function, it can not be expressed by the equation $y = ax + b$ with real $a,\ b$.

4.3 No. The linear fuction $f(x) = 0$ coincides with the x axis and thus the number of intersections is infinite.

4.4 $\varphi = \dfrac{1+\sqrt{5}}{2}$.

4.5 1. no, 2. yes, 3. yes, 4. yes.

4.6 1. 3 a -4, 2. 1, -2 a 3, 3. -2 a 2.

4.9 1. $\frac{\pi}{4}$, 2. $-\frac{1}{\sqrt{2}}$.

4.11 $\mathbb{R} \setminus \{0\}$.

5.1 $x + 2y - 5 = 0$.

5.2 $(x, y) = (-1, -1) + t \cdot (2, 3)$.

5.3 $7x - y - 10 = 0$.

Bibliography

[1] Berry A. Cipra. The best of the 20th century: Editors name top 10 algorithms. *SIAM News*, 33(4).

[2] Confuted. Using quaternion to perform 3d rotations.

[3] Keith Devlin. *The Man of Numbers*. Bloomsbury, 2011.

[4] Nist digital library of mathematical functions. http://dlmf.nist.gov/, Release 1.0.15 of 2017-06-01. F. W. J. Olver, A. B. Olde Daalhuis, D. W. Lozier, B. I. Schneider, R. F. Boisvert, C. W. Clark, B. R. Miller and B. V. Saunders, eds.

[5] Eric Weisstein. Euler-mascheroni constant.

Index

assignment, 12
assumption, 11

bound
    lower, 28
    upper, 28

circle
    unit, 47
claim, 11
    obvious, 11
coefficient
    binomial, 32
complement, 18
condition
    necessary, 27
    sufficient, 27
conjunction, 26
connectives
    logical, 26
corollary, 4
counterexample, 10, 11

definition, 3
difference, 18
discriminant, 42
disjunction, 26
domain, 36

equality, 12, 13
    set, 17
equation, 13
    of a circle, 57
    of a line, 56
    of an ellipse, 57
equivalence, 26

factor
    root, 44
factorial, 31
field, 20
formulas
    addition, 49
    double-angle, 49
function, 35
    affine, 41
    arccosine, 51
    arccotangent, 51
    arcsine, 50
    arctangent, 51
    constant, 41
    decreasing, 37
    exponentiation, 52
    graph, 36
    increasing, 37
    injective, 37
    linear, 39
    logarithm
      of specified base, 52
    monotonic, 37
    periodic, 49
    quadratic, 41
    rational, 46
    stricly increasing, 37
    strictly decreasing, 37
    trigonometric, 47

image, 35
image set, 36
implication, 26
index
    lower, 16
    summation, 14, 27
    upper, 16
inequality
    triangular, 39
intersection, 17

interval, 25

law
  associative, 20
  distributive, 20
lemma, 4
line, 56
  number, 22
  parametric equations, 56
logaritmus, 52

maximum
  of a set, 25
minimum
  of a set, 25

natural domain, 36
negation, 26
number
  coprime, 6
  irrational, 5
  non-coprime, 6
  rational, 5
numbers
  integers, 19
  natural, 18
  rational, 19

parabola, 41
part
  lower integer, 39
  upper integer, 39
point
  coordinates, 54
polynomial, 43
  degree, 43
power, 43
pre-image, 35
product
  cartesian, 18
  scalar, 55
proof, 4, 5
  by contradiction, 6
proposition, 26

quantifier, 26
  existential, 27
  universal, 27

root, 45
  even, 45
  odd, 46

set, 16
  bounded, 25
  bounded from above, 25
  bounded from below, 25
  empty, 16
solution, 13
squaring, 41

theorem, 4
  binomial, 7
  Pythagoras', 57
triangle
  Pascal's, 32

union, 17
unknown, 13

value
  absolute, 38
  of a function, 35
vector, 54
  components, 55
  length, 56