Transition to Advanced Mathematics

MTMM.00.342

Terje Hõim
Johann Langemets

Fall 2019

Contents

***

1

Introduction

***

Mathematics is the language in which
God has written the universe –
G. Galilei

So far your main contact with mathematics has probably involved solving exercises by using some well-known schemes and techniques. For example, you have learned how to solve algebraic equations, systems of equations and how to simplify expressions or check if trigonometric relations are true. By using certain rules and simplifications, you have learned to find the derivative and integral of a function and used them to examine the function or to compute areas and volumes. Usually, to be able to solve such problems, you just needed to practise enough.

All these methods and results that you learned in school mathematics were discovered by other people long time ago and shown to be true over the centuries. Of course, for you that mathematics was new and just like everything new, you have learned a lot and worked hard to understand it. And learning new things could and should be interesting. Do you agree? It would be very interesting to discover something new in mathematics that we did not know before and to show that this new result holds true. But how is that done? How do people come up with new results? How are new relations and methods discovered? One way is to look at different examples and find a common property between these examples. By relying on examples a new hypothesis is phrased, i.e., a new claim that is believed to be true. The first step, however, is to convince ourselves that what we claim is actually true. In mathematics convincing actually means constructing a proof. Since besides ourselves we also need to convince everyone else that our result

is true, then our proof must be very clear and logical, so that the people who know the respective mathematical methods, believe us. Here we should also mention that in mathematics if a claim has a correct proof, then no one questions that this result is correct. Therefore if your result is proved – then it is true. End of discussion. There are no other alternatives. And that is how mathematics is different from all other disciplines.

1.1 The goal of the course

This course is quite different from all other courses you have taken so far. Our main goal is to develop the skill of constructing and writing mathematical proofs so that the proofs you write would be clear and understandable to others as well. In addition to learning new mathematical content we also concentrate on the process of mathematical thinking and try to developing it. Therefore, together we will go through a process that transforms you from person who uses mathematics to a person who also understands it more thoroughly. Maybe this will be your first step on a road, where you will one day create new mathematics and new knowledge. All of that is obtainable, if only you want it. A big part of mathematics that you will see in your future courses is based on knowledge that you learn in this course. The more thoroughly you study the materials and develop the process of mathematical thinking, the easier it will be for you to understand mathematics in the future. In reality, it is true that it is more enjoyable to learn a subject, if you can also understand it. But to achieve that you need to work hard. Too often we hear adults or children claim that they are not good at mathematics. However, this is a false alibi they hide behind. Mathematics is a skill that can be learned, just like every other subject in school. Sometimes we also hear people claim that despite the fact that they are good at mathematics and that they like mathematics, they can not write proofs. That is no argument either, because it takes a lot of confidence and hard work to understand a proof. Getting a good grade for a test or exam without studying and working hard is definitely not something to be proud of. Much more admirable is, if you can say that you have a good mathematical preparation.

1.2 Mathematics as a language

Just like every other language, mathematics helps us to describe the world and therefore, mathematics allows people who understand it to communicate and exchange information. However, mathematics is a bit different from other languages, because usually in a language one word can have more than one meaning, but mathematics describes objects much more specifically and unambiguously. Additionally, mathematicians use a particular vocabulary to describe concepts and you are already familiar with that from school, but we will keep developing it throughout this course. Soon you will notice that mathematics is much more difficult to study, if you can not understand its language.

Mathematicians are like Frenchmen: whatever you say to them they translate into their own language and forthwith it is something entirely different. (Johann Wolfgang von Goethe)

1.3 Why study mathematics?

Mathematics develops thinking that we need in almost all fields of study. For example, when working as a lawyer mathematics help you to formulate and build your arguments better and find mistakes in others arguments. When working as a doctor, knowing statistics helps to understand the real meaning of slogans made by pharmaceutical companies or to understand, what does it really mean if one or other gene increases the risk of getting a disease. Architects and engineers must know how to draw figures and understand the information they contain, how to calculate the sizes of rooms and areas or know how to find a load-bearing capacity of a beam. The computer was invented by mathematicians and maybe you do not know it yet, but computers only understand an algorithmic language that is based on math. That means if you want a computer to do something for you, you need to say that to it precisely and correctly – mathematically. Additionally, mathematics has a big influence on arts, poetry and music. Artists and architects often use the proportion of the golden section, musical sounds consist of harmonic oscillation and the authors of books „Alice in Wonderland" and „Winnie the Pooh" also have a mathematical education. In these books there are also many fun word plays. For example, Lewis Carroll lists four branches of arithmetic—ambition, distraction, uglification, and derision.

Mathematics helps to understand and describe the world around us. According to one of the greatest physicist of the 20th century – Richard Feynman – knowing mathematics is absolutely necessary to describe the nature. Mathematical biology, mathematical physics and other fields that use mathematics have not been created by coincidence but from the need to describe the processes happening around us. The examples we brought here are of course not the only ones that require mathematics – a little wrestling with mathematics is a good preparation for the whole life.

1.4 How to study mathematics?

Studying mathematics is not easy. There is no recipe for studying mathematics in such a way that is is interesting and that guarantees good results. However, we can give a few suggestions. First of all, be in loop with what is happening in lectures and practical lessons. That means showing up and being prepared for every lesson. After every lecture go through the material and rewrite the most important parts or fill in the gaps in the materials. If something was unclear, then ask from your lecturer or classmate right away! It would be good, if you have a buddy with whom you regularly discuss the lecture materials. Read the lecture notes carefully and keep a paper and a pencil nearby. When reading one chapter try to find what is the most important part of it. Solve independently all the example exercises and solve all the homework. Be sure that you always understand what you are writing! Additionally, solve exercises that are not homework. It is even better, if you can come up with an exercise by yourself or even write a test for yourself for preparation (why not to do that in other subjects as well). By doing that you will surprise yourself with how skillful you can be! Creativity is very important in mathematics. By discovering and creating you do not only develop your mathematical skills, but you also might contribute to the development of the field of mathematics. If you have found the first mushroom or made your first discovery, then look around: they grow in clusters. We

can not emphasize it enough – studying mathematics takes confidence, believing in yourself and lots of effort!

A guy decided to go to the clinic for a brain transplant to enlarge his brain. The secretary explains to him that currently they have only three kind of brains. Brains of doctors cost 20 dollars an ounce, brains of lawyers cost 30 dollars an ounce and brains of mathematicians cost 1000 dollars an ounce. "1000 dollars for an ounce!" yelled the guy. "Why are they so expensive?" "Because we need a lot of mathematicians to get one ounce."

1.5 Mathematical view of the world

A view of the world is a system of knowledge that helps people to understand the world around them and relate to it. A view of the world is all the systematized info that a person knows about the respective world and that evolves from all the experiences, knowledge, tenets and beliefs of that person. In mathematics, the view of the world evolves from axioms and proofs of theorems. We should also mention that people from different time periods and different cultures can have a very different view of the world. Nowadays, the scientific view of the world is important – it relies on globally accepted truths. Even though the societal view of the world is in constant changing, the mathematical view of the world is quite definite, because of its axioms and strict logical structure. Mathematical view of the world means to us a context of mathematical knowledge into which we add new knowledge that fits well.

1.6 Symbols and correct mathematical writing

Even though mathematics is a subject orientated around symbols, mathematical texts also contain words. Next we will take a look at some recommendations for writing a mathematical text:

1. **Do not begin a sentence with a symbol, formula or expression.** Writing a mathematical text follows the same rules as writing a regular text. For example, a sentence always begins with a capital letter. If a sentence begins with an equation or symbol, then it seems incomplete, because the capital letter is missing. Also, it is easier to read a sentence that starts with a word.

   Example. Instead of writing: $x^2 - 6x + 8 = 0$ *has two different real solutions.*

   Write: *Equation* $x^2 - 6x + 8 = 0$ *has two different real solutions.*

2. **Separate the symbols from different listings by a word.** It is not advisable to write two mathematical expressions or symbols next to each other if they do not belong to same listing. To make it easier to read and understand the sentence, such symbols should be separated by a suitable word.

   Example. Sentence: *Additionally to number* a*,* b *is also a solution of the equation* $(x - a)(x - b) = 0$.

   It would be a lot clearer to write: *Additionally to number* a*, the number* b *is also a solution of the equation* $(x - a)(x - b) = 0$.

3. **Do not unite word and symbols with each other.**

   Example. Instead of writing: *Every integer* ≥ 2 *is either a prime number or composite number.*

   Write: *Every integer that is bigger or equal to two is either a prime number or a composite number.*

4. **Write the number with words, if that number describes a noun, if that number is small or easy to write in words. To describe a numerical value use numbers.**

   Example. A million Estonians can not all be wrong at the same time.
   There are 100 positive numbers that are smaller than the number 101.
   You can give me one ticket!

5. **Make sure that commas and periods after the equations are in the correct place.**

6. **Avoid the symbols** $\Rightarrow$, $\forall$, $\exists$, $\therefore$ **in professional mathematical writings, except for writing operations of mathematical logic.** The given symbols are short from following expressions: $\Rightarrow$ *concludes*, $\forall$ *for every*, $\exists$ *exists*, $\therefore$ *therefore*. Knowing these symbols is useful for taking notes in a lecture or for sketching the first versions of a proof of a theorem. However, many mathematicians avoid these symbols in their final professional writings.

Exercise 1.1. Rewrite the following sentences in the correct way. Which rule has been broken?

(a) Let x be a positive real number. x can be ≤ -1. $x = 0$ is also suitable.

(b) There are 3 types of people those who can not calculate and these who can.

(c) To solve the equation $x^2 = 36$ we need to $\sqrt{}$ both sides.

(d) $f(x) = x^2$ and $g(x) = 3x + 4$ means $f(x) = g(x) = x = 4$.

2

Concept, definition, theorem, assumption and conclusion

***

The whole is greater than the sum of its parts – Aristotle

2.1 Concept

We have studied mathematics in school for years and therefore we have already seen many concepts. For example, we are familiar with basic geometry concepts like point, line, plane, triangle, vector, cuboid, cube as well as with concepts from other fields of mathematics. To understand and use our knowledge we need to know the concepts well. For example, you can definitely understand the sentence "The derivative of an exponential function is equal to itself", because you know the concepts of exponential function and derivative. However, you probably do not understand the sentence "For every non-empty set there exists a bijection between the set of all equivalence relations and the set of all partitions of that set", because you might not know the concepts of equivalence relation, partitions or bijection.

Just like we do when thinking, we also generalize and restrict concepts in mathematics. We say we are **generalizing** a concept if we proceed from a less general concept to more general concept. We say we are **restricting** a concept if we proceed from a more general concept to a less general concept. Such series of concepts, where the concepts are deduced from each other by

generalizing or restricting are called ladders. For example, in mathematics we have the following ladder: quadrangle, convex quadrangle, parallelogram, rectangle, square.

Exercise 2.1. Generalize and restrict the following concepts:

(a) triangle;

(b) geometry;

(c) rational number;

(d) root;

2.2 Definitions

If we use a concept, we also want to explain the meaning of that concept to others and to do so we can list all the properties the concept has. For example, we can describe parallelogram as follows: "Parallelogram is a planar figure; polygon; it has four sides and four angles; its opposite sides are parallel and equal; its diagonals divide each other to two equal parts; the sum of its interior angles is 360°; the area of parallelogram is the product of the base and height." However, that way of describing is not optimal, because some of the properties we listed can be concluded from others. To determine the parallelogram in a short and exact way, we need to define it. For example, we can define it as follows: "A quadrangle is called a parallelogram if its opposite sides are parallel".

Determining a concept through easier and well-known concepts is called **defining** a concept and the specification itself is called a **definition**.

Definition must give an exact and short answer to the question "What is called . . . ?" or "What is . . . ?". Definition is exact if it obeys the following rules. Knowing the rules and obeying them helps us to avoid incorrect definitions.

1. **Definition must contain exactly that many properties** it takes to determine the exact volume we want to define. Definition „Triangle is a polygon“ is too wide, however, definition „Triangle is a polygon that has three sides with equal lengths" is too narrow. (Explain why.) In a too narrow definition there are more conditions than necessary.

2. **It is not allowed to define a concept by using the concept itself**, one of its synonyms or a concept that is only understandable through the concept we define. Therefore, a definition can not contain a circle. If this rule is not followed, we will get a **tautology**, a mistake "idem per idem," that means repeatedly using one word in a definition.

3. **Definition must be affirmative if possible**, because when we use negation the content of the definition is unclear. For example, "point is something that does not have portions nor size" or "triangle does not have four sides" do not explain the content of respective concepts. Using negation in a definition is allowed only if the concept we want to define is a negation by content.

4. **Definition must be clear and understandable**, that means definition can not contain ambiguous, metaphorical and obscure expressions. Expressions such as "lion is the king of the jungle" are not definitions but they can be useful when explaining the content of the concept. Also the famous definition of a country given by Hegel; "Country is the political exposition of the world spirit", is incorrect for the same reason.

Therefore, a definition must determine the concept fully. When defining we show to which set the object belongs and then add the condition that separates that object from other elements of that set. For example, when defining a parallelogram we note that it belongs to the set of quadrangles and add a property that distinguishes it from other quadrangles.

The concept that determines the set that contains the object we are defining is called **genus**. The condition that separates that object from other objects in that set is called **specific difference**.

Often it is possible to define a concept in more than one way. For example when we are defining a parallelogram, we can choose for its genus a polygon or even a planar figure. However, when making these changes we also need to change the specific difference. Even if we have chosen quadrangle for the genus, we can still choose the specific difference in many ways. For example, we can choose the equality of opposite sides or the parallelism of opposite sides.

Concepts that we use to define another concepts must be known beforehand. Therefore, these concepts must be defined before. That is how the ladders of concepts are created. These ladders start with concepts that are not defined and that form the basis for defining other concepts. These concepts are called **primitive notions**. In mathematics the primitive notions are for example point, line, plane, space, set, number, size and many more.

In a girls baseball game are three judges - one engineer, one physicist and one mathematician. The last player of the team reaches the tile the same time as the ball, but all three judges decide that the player is out from the game. The angry father asks why judges decided that way. The engineer says, "She is out from the game because I trust only things that have really happened." Physicist says, "She is out because I trust and confirm only what I can see." The mathematician answers, "She is out because I say so." (Can you comment the mathematician point of view?)

2.3 Classification

Classification means unfolding the content of the concept fully and properly. For example, triangles can be divided into obtuse, acute and right angled triangles. Classifying by sides we can divide triangles into equilateral, isosceles and scalene triangles. Classification must have exactly one base, that means the base of a classification must be same in entire classification, in that case it is clear and consistent and the members of the classification exclude each other. Otherwise one object could be part of two or more parts of the classification. Classification must also be continuous, that means there can not be a leap in the classification.

2.4 Theorem and proof

In mathematics, if we want to make sure that something is true, we do not conduct experiments nor carry out measurements – we use proofs instead. **Theorem** (Greek theóréma – speculation, proposition to be proved) is a sentence we need to prove by using axioms, and previously proven propositions. A proposition that we do not prove by other propositions is called an **axiom** (Greek axióma) or a **postulate** (Latin postulátum). Following sentences are examples of axioms:

(a) Every natural number is directly followed by exactly one natural number.

(b) Through any two different points, there is exactly one line.

(c) For every two points A and B the equality $\overline{AB} = \overline{BA}$ is true.

(d) **Parallel postulate**: in a plane, given a line and a point not on it, at most one line parallel to the given line can be drawn through the point.

Rest of the formulas and results are presented as sentences that are called theorems. Whether a theorem is true or false can be concluded from the axioms. Since axioms are not proven, then we might wonder, why are they true. We decide if axioms are true by applying the theorems we proved from them: every theory is confirmed by practice. Axioms are actually only hypothesis.

Theorems are usually in the form: *"If A, then B"*. The part A of the theorem that is connected with the word "if", is called an **assumption** and the part B that is connected with the word "then" is called a **conclusion**. In the assumption we determine which objects are subject to the theorem, that means what we have been given or what we already know. In the conclusion, we state what we can conclude from the assumption, i.e. what want to prove.

Example 2.2. "If two vectors are orthogonal, then their scalar product is zero." The assumption of that theorem is that two vectors are orthogonal and the conclusion is that their scalar product is zero.

Sometimes it is shorter to write theorems as simple sentences. For example, we can rephrase the statement "The sum of supplementary angles is 180°" as "If angles are supplementary, then their sum is 180°."
Proving a theorem means showing that from the assumption A we can conclude the conclusion B; in short $A \Rightarrow B$. When proving we use axioms and previously proven theorems.

Proving statements in mathematics is much more strict than in other disciplines. For example, if we claim that "In July the weather is hot in Tartu", then based on our experiences from the past few years we can say whether it is true or not. However, does that also mean that the whether is hot every day of July of every year? Of course not! It is not smart to make such a universal claim about weather. Physicists say that "If we let go of an object close to the ground, then it will fall with acceleration of 9.8 m/s^2*" That sentence is more likely to be correct than the sentence about weather in Tartu, but that rule of physics is not absolutely true either. First of all, the number 9.8 has been rounded. Secondly, the word "close" is very unclear. When we think about the whole galaxy, then Moon is close to Earth as well, but that is not the same*

"close" we had in mind when making the statement. We could clarify that by saying "close" we mean "100 meters or less from the ground," but even that clarification leaves us with a problem. The gravitational force is a bit smaller for objects that are 100 meters above the ground than the gravitational force is for objects on the ground. And the gravity on the ground is not always the same either: the gravity on top of the mount Everest is weaker than the gravity on the sea level.

Since theorems are proved by logical discussion, then we also need to examine logic – the study of "right thinking". In logic we also allocate axioms – the fundamental laws of right thinking.

Therefore, most sentences that we use in every day life and believe to be true might not be absolutely and universally true. However, in mathematics the word "true" means that something is absolutely true without any conditions or counterexamples.

For example, let us take a look at the Pythagorean theorem that clams that if a and b are the two legs of a right angled triangle and c is the hypotenuse of the same triangle, then the equality $a^2 + b^2 = c^2$ holds. Of course, that statement is true with no exceptions! We know it because Pythagorean theorem has a proof (actually many different proofs). Of course, we can ask and wonder if it indeed is true by drawing a right angled triangle and measuring its sides with accuracy of $\frac{1}{1000}$ mm. It turns out that Pythagorean theorem is not true for our drawing, because the triangle we drew is not an exact right angled triangle! Drawing is an important tool in mathematics that helps us to understand concepts, but it is actually nothing more than a sketch, i.e., ink on the paper. The "real" right angled triangle can exist only in our minds.

An engineer, physicist and mathematician are travelling by train through Scotland. Suddenly they notice a black sheep on the side of a mountain. "Look," the engineer shouts. "In this part of Scotland all the sheep are black!" "Indeed," snaps the physicist. „You should not make such conclusions. All we know is that some sheep in this part of Scotland are black." „Well, they are black on one side indeed," mumbles the mathematician.

By switching in a theorem "If A, then B" the assumption and the conclusion we get a sentence "If B, then A." That sentence is called the **converse** of the given theorem. Even if the sentence is true, its converse might not be.

Example 2.3. Proposition "If a number ends with zero, then it is divisible by five." is true. The converse of that proposition „If a number is divisible by five, then it ends with zero" is not true.

Therefore, from the fact that the theorem is true we can not conclude that its converse is true. If the converse of the theorem is true, then it is called a **biconditional theorem**.

By replacing in a theorem "If A, then B" the assumption and conclusion with their negations (symbols $\neg A$ and $\neg B$), we get the proposition "If $\neg A$, then $\neg B$." That sentence is called the **inverse** of the given theorem. Again, from the theorem being true we can not conclude that its inverse is true.

Example 2.4. Proposition "If a figure is a triangle, then it is polygon" is true. The inverse of that proposition is "If a figure is not a triangle, then it is not a polygon." That sentence is not true, for example quadrangle is not a triangle but it is a polygon. The inverse of the theorem "If a number is divisible by nine, then its cross sum is divisible by nine" is "If a number is not divisible by nine, then its cross sum is not divisible by nine." Both of these sentences are true.

If in the theorem "If A, then B" we switch the assumption and the conclusion and replace them by their negations, we will get a sentence "If $\neg B$, then $\neg A$." That sentence is called the **contrapositive** of the given theorem. If the theorem is true we can conclude that the contrapositive of the theorem is also true and vice versa. By using symbols: If A, then $B \Leftrightarrow$ If $\neg B$, then $\neg A$. It is also said that these sentences are logically equivalent.

We will take a closer look at propositions and their converses, inverses and contrapositives in the next chapter.

In a theorem the conclusion is concluded from the assumption. In that case we say that the assumption is **sufficient** to prove the theorem. If the converse of that theorem is true is, then the assumption is concluded from the conclusion. In that case we say that the assumption is a **necessary** condition for conclusion. If both the theorem and its converse are true, then usually they are put together in a one sentence by using the expression "is necessary and sufficient," or "if and only if".

Example 2.5. "For a number to be divisible by five it is necessary and sufficient that the number ends with zero or five." "A number is divisible by five if and only if it ends with zero or five."

These sentences present so called necessary and sufficient conditions. Since at the same time both $A \Rightarrow B$ and $B \Rightarrow A$ are true we can denote that by: $A \Leftrightarrow B$. When proving necessary and sufficient conditions we usually prove both the necessity and the sufficiency separately.

If the specific difference in the definition of the concept is a necessary and sufficient condition to determine that the element of the genus set is the defined object then we can rephrase that theorem into a new definition of that concept. The previous definition of the concept is then a theorem that has a necessary and sufficient condition.

Example 2.6. Definition. A quadrangle if is called a parallelogram if its diagonals bisect each other. **Theorem**. A quadrangle is a parallelogram if and only if its opposite sides are parallel.

Symbols □ and ■ denote the end of the proof.

Some theorems are more interesting and important than others. Therefore, mathematicians often use alternative expressions instead of the word "theorem". Word "theorem" is used only for the most important and most general results. Otherwise the following words are used in academic texts:

- **Proposition** is a less important theorem.

- **Lemma** is a less important theorem, its goal is to present an independent result that is used to prove a more important theorem. Some theorems have very long and complicated proofs, that are divided into smaller parts. A lemma can be one of these parts or a tool that is used to prove a more complicated theorem.
- **Corollary** is a result that has a short and easy proof that uses the previously proven theorem.

In some texts the following expressions are also used to present smaller theorems:

- **Claim** is similar to lemma, that means it is part of a longer proof of a theorem and it helps to organize the necessary steps.
- **Result** is very modest and general name for a theorem. All important and less important theorems can be called results.
- **Fact** is a result that has little importance.

2.5 Quantifiers

In the next chapter we will see how mathematicians use specific logical operations. In this introductory chapter we will get acquainted with **quantifiers** and the according symbols.

In many mathematical sentences (theorems) we use words "for all", "for every", "there exists", "at least one". For example, "All numbers are divisible by two", "There exist linear functions", "At least one prime number is even" and so on.

Some of these sentences are true, some are false. When writing these sentences we use two symbols that are called **quantifiers**. One of them is $\exists$ (we say "exists") and the second one is $\forall$ (we say "for all" or "for every"). These symbols represent the inverted first letters of German words "Existieren" and "Alle". After the quantifier we always need to write the variable to which the quantifier is applied to.

How do we use these symbols? For example, writing $\forall x \in \mathbb{R},\ x^2 + 1 > 0$ means that $x^2 + 1$ is bigger than zero for every real number x. That sentence has a general form $\forall x\ P(x)$ that can be written as follows: „For any object x (from the given set of objects) the statement $P(x)$ is true.“

Writing $\exists x,\ x^3 - 27 = 0$ means "there exists x such that $x^3 - 27 = 0$ is true." The general form $\exists x\ P(x)$ represents here "there exists x such that $P(x)$ is true" that means "at least one object has the property P". The word “exist” here does not mean that there exists exactly one object that satisfies the condition, but that there exists at least one object (i.e., there might exist many), that satisfies the given condition.

If we use the quantifier “for all” in the sentence, then we are claiming that something is true for all objects from the given set and therefore we need to prove this claim in general. However, to

disprove the claim it suffices to find one counterexample. For example, Pierre Fermat' presented a hypothesis that for every natural number n the number $2^{2^n}+1$ is prime. Hypothesis is true for $n = 0, 1, 2, 3$ and 4 but Leonhard Euler showed that when $n = 5$, then the number is divisible by 641. With that the hypothesis was disproved.

Quantifiers $\forall$ and $\exists$ can be combined with each other. For example, $\forall x \in \mathbb{R}\ \exists y \in \mathbb{R},\ x < y$ denotes the sentence "for every real number x there exists a real number y such that $x < y$" which we know is true. If we change the order of the quantifiers in the previous sentence, we will get a false sentence $\exists x \in \mathbb{R}\ \forall y \in \mathbb{R},\ x < y$, that means "there exists a real number x such that $x < y$ for every real number y". Find a counterexample for the last sentence!

Also, it is possible to apply the quantifiers to more than one variable. For example, $\exists x, y,\ x+y = 5$ denotes the sentence "there exist numbers x and y for which $x + y = 5$ is true". By switching the quantifier, we will get a false sentence $\forall x, y,\ x+y = 5$, i.e., „$x+y = 5$ is true for all numbers x and y". Similarly we can form sentences $\forall x\ \exists y,\ x + y = 5$ and $\exists x\ \forall y,\ x + y = 5$. Again one of these is true (which one?) and one false. Therefore, usually sentences

$$\forall x\ \exists y,\ P(x, y) \text{ and } \exists x\ \forall y,\ P(x, y)$$

are not equivalent.

2.6 Negating sentences that contain quantifiers

Let us consider the following sentences:

- „There does not exist an integer that is even and odd at the same time."
- „Not all natural numbers are prime numbers."

We can write these sentences by using quantifiers:

- $\neg(\exists x \in \mathbb{Z}$, x is even and x is odd).
- $\neg(\forall x \in \mathbb{N}$, x is prime).

We can rephrase the first sentence in the following way: "All integers are not even and odd at the same time" or by using symbols $\forall x \in \mathbb{Z}$, $\neg(x$ is even and x is odd). In the same way we can rephrase the second sentence: „There exists a natural number that is not a prime number" or by using quantifiers $\exists x \in \mathbb{N}$, $\neg(x$ is a prime number).
Therefore, to claim that $\exists x\ P(x)$ is not true we actually claim that $\forall x\ (\neg P(x))$ is true.

Example 2.7.

1. Let us examine the sentence "There exists a real number x such that $x^2 = 3$." By denoting $P(x) : x^2 = 3$, we can write that sentence in the form $\exists x \in \mathbb{R},\ P(x)$. That is a true sentence because for example $x = \sqrt{3}$ satisfies the given condition. Its negation is the sentence "$x^2 \neq 3$ for every real number x" that is false.

2. Let us now take a look at the sentence „For every two real numbers x and y the inequality $x^2 + y^2 \geq 0$ is true“ or by using symbols $\forall x \in \mathbb{R},\ \forall y \in \mathbb{R},\ P(x, y)$, where $P(x, y)$ denotes the claim $x^2 + y^2 \geq 0$. This is a true sentence. Its negation is „There exist real numbers x and y such that $x^2 + y^2 < 0$“ is clearly false.

3. Proposition "For every positive rational number a there exists a positive rational number b such that $ab = 1$". Let us formulate its negation: "There exists a positive rational number a such that for every positive rational number b the condition $ab \neq 1$ is true". This is a false sentence. Why?

To sum up, we use the following rules to form the negations of sentences that contain quantifiers:

$$\neg(\forall x\ P(x)) \equiv \exists x(\neg P(x)), \quad \neg(\exists x\ P(x)) \equiv \forall x(\neg P(x))$$

$$\neg(\forall x\ \exists y,\ P(x, y)) \equiv \exists x\ \forall y\ (\neg P(x, y)), \quad \neg(\exists x\ \forall y\ P(x, y)) \equiv \forall x\ \exists y\ (\neg P(x, y))$$

In the next chapter we will discuss whether the sentences formed in such way are true or not and how to form negations of more complicated sentences that contain quantifiers.

3

Propositional calculus

***

To err is human, but to persist in error (out of pride) is diabolical. – Seneca

3.1 Mathematical logic

Logic (in Greek, *logiké techne* — the art of thinking, logos – the word, the concept, the mind) is a science of right thinking, its forms and structures.

Aristotle (384–322 B.C.) was an ancient Greek philosopher who is considered the "Father of Western Philosophy". Of course some logical rules were known and used before Aristotle, but he was the first who established logic as a systematic science. The word "logic" also originates from the Greek language, but Aristotle himself did not call his work by that name. The Aristotelian logic and its further developments are also known as traditional logic. In the second half of the 19th century, mathematicians started developing the contemporary logic that has more logical rules than the Aristotelian logic. Contemporary logic is also known as mathematical logic.

Mathematical logic is a branch of logic, where mathematical methods are used to solve logical problems. By describing the concepts and statements of some field the formal language is created that is precise and plain enough to be used for mathematical research. At the same time there is a clear difference between the syntactic aspects that treat objects as sequences of

symbols constructed by certain rules, and the semantic aspects that give the syntactic objects an interpretation, i.e., "meaning". Nowadays mathematical logic is divided into many branches. Since the formal languages of logic have turned out to be very suitable for writing and analyzing computer programs, the development of mathematical logic is strongly connected with the field of computer science.

The foundation of traditional logic are the **laws of thought** that are also called axioms of logic. Laws of thought are laws which our mind must follow to be logical and true. Aristotle phrased three laws of thought: the law of identity, the law of non-contradiction and the law of excluded middle. **W. G. Leibniz** (1646 – 1716) added a fourth law – Leibniz's law.

1. **The law of identity** claims that every concept or claim must stay the same in one discussion. Breaking that law causes vain arguments and we have an Estonian saying about that: "One is talking about the fence and other about the hole in the fence." In mathematics it is important to make sure that the content of the concepts we use in discussions do not change during the discussion and therefore, we are using the concept in only one meaning. We need to avoid the everyday language as much as possible, because it is often ambiguous.
2. **The law of non-contradiction** says that two propositions that are negating each other can not both be true. For example, the discriminant of a quadratic equation with fixed coefficients can not be both negative and nonnegative or one and the same natural number can not be a prime number and a composite number at the same time. If we have reached a point in our discussion where two contradictory propositions are both true then obviously there is a mistake in our discussion. If the mistake is simple, then we can correct it easily. However, if the mistake is more complicated and hidden, then the cause of mistake might keep mathematicians and philosophers busy for decades or even centuries. Such mistakes are called paradoxes or antinomies.
3. **The law of excluded middle** says that one of two contradictory propositions is true and the other is false; there is no third option. Therefore, two numbers can be equal or not equal; animals can be vertebrate or invertebrates, there is no third option (tetrium non datur).
4. **The Leibniz's law** declares that every decision and thought must have a solid base, that means every statement needs to be justified by some other statement that we know to be true. For example, if we claim that the median of the trapezoid is parallel to its bases and equal to half of the sum of its bases, then we need to justify it by proof.

The base of mathematical logic consists of propositional calculus and predicate calculus. The goal of propositional calculus is to examine what happens when we combine propositions into compound propositions, for example, how does the truth value of the compound proposition depends on the truth values of the component propositions. Predicate calculus is a generalization of propositional calculus, where instead of examining propositions with fixed truth values, we examine propositions for which truth values might depend on the value of the arguments (for example propositions "$2x + 3 = 11$" and "x is prime number").

3.2 Basic concepts of propositional calculus

In propositional calculus the main object of interest is a proposition that can originate from any field. However, not every linguistically correct sentence is a proposition. In mathematical logic an expression is called a **proposition** if we can discuss whether its content is or is not in correspondence with reality. If its content corresponds to reality then that proposition is called **true**. However, if the content does not correspond to reality, then that proposition is called **false**. Therefore, it is important that for every proposition we can determine its **truth value** which shows whether the proposition corresponds to reality or not. Let us assume that

- every proposition is either true or false (the law of excluded middle);
- no proposition is both true and false (the law of non-contradiction).

Therefore, we examine only the propositions that claim something and each claim they make has a unique truth value.

For example, propositions "Abruka is an Estonian island" and "Number 19 is a prime number" are true, but propositions "Horse is a bird", "Moon is a big yellow cheesecake" and "$25 > 50$" are false. However, we can not determine if sentences "Do you have an iPad?", "Good day!" and "$x > 0$" are true or false (to determine if the last sentence is true, we need to know the value of x). According to the law of excluded middle all questions, slogans and meaningless phrases are left out. The law of non-contradiction also excludes many paradoxes, for example "This sentence is wrong" or "I am lying at the moment", because it is not possible to determine the truth values of these claims.

If a proposition is true, then we say that its truth value is *t*, and if a proposition is false, then its truth value is *f*. Numbers 1 and 0 are also used to mark the truth values of propositions.

The goal of propositional logic is not to examine the content of the propositions, but to form new propositions from already given propositions. By using logical operators we can form **compound propositions**. Propositions that we combine to form a compound proposition are called **component propositions**. Just like all component propositions the compound proposition can also be true or false and its truth value depends only on the truth values of component propositions. To form a compound proposition we denote the component propositions and the relations and we write the proposition by using symbols. To denote component propositions we use uppercase Latin letters *X, Y, Z* etc, that are called **propositional variables**. However, for denoting grammatical relations we use respective logical operations. Two sentences that are identical in content, but different in form are considered equal and denoted by one and same letter. For example, propositions "The height of a right angled triangle is the geometric average of the projections of its legs" and "The square of the height of a right angled triangle is equal to the product of the projections of its legs" express the same idea and are equal in their content. Therefore, we can denote them with the same letter. Propositions that have different content are denoted with different letters.

3.3 Important logical operators

- **Negation** (symbol $\neg$) is a logical operator that is applied to only one proposition. In everyday language negation means that the sentence is not true, for example "Lemon is not sour". That sentence can be written as $\neg A$, where $A =$ „Lemon is sour".

The **negation** of a proposition is the proposition $\neg A$ that is true if and only if proposition A is false.
If a proposition contains quantifiers, then the negations are constructed as follows:

$$\exists x\ P(x) \text{ negation is } \forall x\ \neg P(x)$$

$$\forall x\ Q(x) \text{ negation is } \exists x\ \neg Q(x)$$

To negate a proposition that contains quantifiers, we need to change the quantifier and negate the proposition.

Example 3.1. $A =$ "Every natural number has a logarithm that is not zero," $\neg A =$ "There exists a natural number such that its logarithm is zero."

Example 3.2. $A =$ "There exists a real number that can not be a divisor," $\neg A =$ "Every real number can be a divisor."

- **Conjunction** is an operator that in words means "and". Conjunction is denoted with symbols $\wedge$ or &. For example, "The wind is blowing and it is raining" can be written as $A \wedge B$ or $A\&B$, where $A =$ "The wind is blowing" and $B =$ "It is raining". Conjunction is sometimes also called logical product.

The **conjunction** of propositions A and B is denoted by $A \wedge B$ and it is true if and only if both component propositions A and B are true.

- **Disjunction** (symbol $\vee$) represents the relation "or". For example "Helen sings or Mart sings" can be written as $A \vee B$. The word "or" is used in a non-exclusive way: "If A or B or both". In everyday language we use also exclusive "or": "If A or B, but not both", for example "I will seed the field with potatoes or with rye". Disjunction is always the non-exclusive "or".

The **disjunction** of A and B is denoted by $A \vee B$ and it is true if and only if at least one of its components A or B is true.
The proposition formed by non-exclusive "or" is false if and only is both component propositions are false.

- **Implication** (symbol $\Rightarrow$ or $\rightarrow$ or $\supset$) expresses conditional sentences "if ..., then ...". For example "If Sven studies well the whole year, then he can easily pass the exams in the spring" or "If theorem A is true, then theorem B is also true". Both propositions can be written as $A \Rightarrow B$. There are many ways to phrase an implication. For example:

  1. If A, then B.

2. From A we can conclude B.
3. A is sufficient for B.
4. B is necessary for A.
5. A is true only if B is true.

The **implication** of propositions A and B is denoted by $A \Rightarrow B$ and it is true if and only is A is false or B is true.
NB! Implication is not a commutative operator. It is important to notice which expression is left from the symbol $\Rightarrow$ and which expression is right from that symbol.

- **Equivalence** (symbol $\Leftrightarrow$ or $\sim$ or $\leftrightarrow$) is the relation "if and only if" that is often used in mathematics. For example, the proposition "number r is a rational number if and only if r can be written as terminating or repeating decimal" can be written as $A \Leftrightarrow B$.

The **equivalence** of propositions A and B is denoted by $A \Leftrightarrow B$ or $A \sim B$ and it is true if and only if both A and B are true or both are false.
All the definitions of the operators that we introduced can be presented in one table:

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

Negation is the only logical operator that can be applied to only one proposition. To apply the rest of the logical operators – conjunction, disjunction, implication, equivalence – we need at least two components.

Precedence of logical operators allows us to reduce the number of brackets used in formulas. Negation has the highest precedence and equivalence has the lowest precedence. The precedence of other logical operators is fixed so that in the following sequence every operator takes precedence over the operator that is on the right from it:

$$\neg \ \wedge \ \vee \ \Rightarrow \Leftrightarrow$$

Therefore, we have defined the logical operators and now we can combine simple propositions together into more complicated propositions by using logical operators. For example, we can form a proposition:

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

In such operations we assume that following conditions are satisfied:

- operators can be applied to any propositions (we do not require any connection between their content);

- the truth value of the proposition we get by combining operators depends only on the truth values of the component propositions, not on their content.

From these conditions we can see that when performing logical operations the content of the propositions is not important, but their truth values are important. In fact the main goal of propositional calculus is finding the truth values of compound propositions.

3.4 Propositional formulas

By writing propositions in a symbol form we get **propositional formulas**. Once we have done that, we can examine only formulas and leave out the sentences from where we got those formulas. The exact regulations for writing formulas is determined by the following definition.

Definition 3.3. Propositional formulas are exactly those that can be constructed by following rules:

1. every propositional variable is a propositional formula;
2. truth values t and f are propositional formulas;
3. if $\mathcal{F}$ is a propositional formula, then $\neg\mathcal{F}$ is also a propositional formula;
4. if $\mathcal{F}$ and $\mathcal{G}$ are propositional formulas, then $\mathcal{F} \wedge \mathcal{G}$, $\mathcal{F} \vee \mathcal{G}$, $\mathcal{F} \Rightarrow \mathcal{G}$ and $\mathcal{F} \Leftrightarrow \mathcal{G}$ are also propositional formulas;
5. if $\mathcal{F}$ is a propositional formula, then $(\mathcal{F})$ is also a propositional formula.

For example, $(\mathcal{A} \vee \mathcal{B}) \wedge (\mathcal{C} \Rightarrow \mathcal{D})$ is a formula, if $\mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{D}$ are formulas.

From definition we can conclude that a formula can depend on a finite number of variables and that we have regulations that allow us to form more complicated formulas from simple formulas. Such type of definitions are common in logic and they are called **inductive**, because they remind the method of mathematical induction. Conditions 1) and 2) represent the basis step of induction and conditions 3), 4) and 5) represent the inductive step (we will talk more about induction in chapter 7.2).

From two propositional variables we can form formulas that contain one logical operator; from a propositional variable and a formula that contains one logical operator we can form a formula that contains two operators and so on. All the formulas we get in the process of constructing a formula are called **components** of that formula and the operator used in the last step is called the **main operator**. If a proposition has many different logical operators, then we need to take into account the brackets and the precedence of operators (reminder: first negations, then conjunctions, then disjunctions, then implications and equivalences). If we have many disjunctions or conjunctions in a row, then we can leave out the brackets. Also we can leave out the exterior brackets of the formula.

Example 3.4. Let us consider the formula

$$\Big(((X \wedge \neg Y) \wedge (Z \Rightarrow \neg X)) \Leftrightarrow (Y \vee X)\Big).$$

Propositional variables X, Y, Z are propositional formulas according to the first item of the definition. According to the third item $\neg X$ and $\neg Y$ are also propositional formulas and according to the forth item $Y \vee X$ is also a formula. Now $X \wedge \neg Y$, $Z \Rightarrow \neg X$ and $(X \wedge \neg Y) \wedge (Z \Rightarrow \neg X)$ and also $((X \wedge \neg Y) \wedge (Z \Rightarrow \neg X)) \Leftrightarrow (Y \vee X)$ are propositional formulas. The main operator of the last formula is $\Leftrightarrow$ and its components are exactly all the formulas we mentioned.

Example 3.5. We will take another look at the formula

$$\Big(((X \wedge \neg Y) \wedge (Z \Rightarrow \neg X)) \Leftrightarrow (Y \vee X)\Big).$$

By leaving out exterior brackets we get

$$((X \wedge \neg Y) \wedge (Z \Rightarrow \neg X)) \Leftrightarrow (Y \vee X).$$

By taking into account the precedence of operators we can lose the brackets around the both sides of the equivalence:

$$(X \wedge \neg Y) \wedge (Z \Rightarrow \neg X) \Leftrightarrow Y \vee X$$

We also do not need the first brackets:

$$X \wedge \neg Y \wedge (Z \Rightarrow \neg X) \Leftrightarrow Y \vee X$$

Now the formula has a more comprehensive form.

3.5 Truth values of formulas

For every possible combination of truth values of the variables we will determine the truth value of the formula. It is practical to do that in a table form. That table is called the **truth table** of the formula. To find the truth value of the formula we need to replace the variables with their truth values and take into account the precedence and definitions of logical operators.

Example 3.6. Let us construct the truth table of the formula $(\neg X \Rightarrow Y) \vee (X \wedge Y)$. In the table header we will write the variables X and Y and operations in the correct order. For two variables there are 4 possible combinations of truth values. These we will write in the columns that have the truth values of X and Y and then we fill rest of the columns by taking into account respective logical operators.

X	Y	$\neg X$	$\neg X \Rightarrow Y$	$X \wedge Y$	$(\neg X \Rightarrow Y) \vee (X \wedge Y)$
t	t	f	t	t	t
t	f	f	t	f	t
f	t	t	t	f	t
f	f	t	f	f	f

The truth values of the formula $(\neg X \Rightarrow Y) \vee (X \wedge Y)$ are in the last column of the table. We can see that the given formula is false if and only if both variables are false ($X = f$ and $Y = f$).

3.6 Valuations of variables

Every propositional variable can either be true or false. For example, if X is true, then we write $X = 1$ or $X = t$, otherwise, is variable X is false, we will write $X = 0$ or $X = f$. If we give a truth value to each given variable, then such set of truth values is called a **valuation of variables**. For example, for variables X, Y, Z one possible valuation is $X = 1, Y = 0, Z = 1$, or in short $(1, 0, 1)$.

Let us have a propositional formula. Let us give truth values to all propositional variables of that formula, that means we give a truth value to every variable. To find the truth value of the formula, we need to execute all the operations in that formula. We get the rules to do so from the following definition.

Definition 3.7. The truth value of the propositional formula $\mathcal{F}$ in a given valuation is found by following rules:

1. If $\mathcal{F} = \neg\mathcal{G}$, then $\mathcal{F} = 1$ if and only if $\mathcal{G} = 0$.
2. If $\mathcal{F} = \mathcal{G} \wedge \mathcal{H}$, then $\mathcal{F} = 1$ if and only if $\mathcal{G} = 1$ and $\mathcal{H} = 1$.
3. If $\mathcal{F} = \mathcal{G} \vee \mathcal{H}$, then $\mathcal{F} = 1$ if and only if $\mathcal{G} = 1$ or $\mathcal{H} = 1$.
4. If $\mathcal{F} = \mathcal{G} \Rightarrow \mathcal{H}$, then $\mathcal{F} = 1$ if and only if $\mathcal{G} = 0$ or $\mathcal{H} = 1$.
5. If $\mathcal{F} = \mathcal{G} \Leftrightarrow \mathcal{H}$, then $\mathcal{F} = 1$ if and only if $\mathcal{G} = 1$ and $\mathcal{H} = 1$ or $\mathcal{G} = 0$ and $\mathcal{H} = 0$.

Negation is a simple postulate that means that propositions that negate each other have opposite truth values. Conjunction is true if and only if both component propositions are true. Disjunction is true, if at least one of the component propositions is true. Therefore, the word disjunction puts into practice the word “or” in a non-exclusive way. Implication is false if and only if the first component is true and the second component is false. In ordinary language we tend to think that a sentence with a false first component is not true (for example ”If 1=2, then today is a working day”). However, in the rules that we follow when finding truth values we have in mind the mathematical idea of deduction. For example, we have no reason to consider the conclusion “If the number x is positive, then the square of x is also positive” false in case the given number is zero or negative. Finally, equivalence is true if and only if both its components have the same truth value.

Example 3.8. Find the truth value of the formula $X \wedge \neg Y \wedge (Z \Rightarrow \neg X) \Leftrightarrow Y \vee X$ when the variables X, Y, Z have a valuation $(1, 0, 1)$.
First of all we know that $X = 1$, $Y = 0$ ja $Z = 1$. According to the first item of the definition 3.7 we see that $\neg X = 0$ and $\neg Y = 1$ and according to the third item $Y \vee X = 1$. From there on we find analogically that $X \wedge \neg Y = 1$ and $Z \Rightarrow \neg X = 0$, therefore $X \wedge \neg Y \wedge (Z \Rightarrow \neg X) = 0$. Finally, we see that $X \wedge \neg Y \wedge (Z \Rightarrow \neg X) \Leftrightarrow Y \vee X = 0$. Therefore, the formula is false in the given valuation.

Similarly to previous table, it is smart to describe the operations with the truth table that has all the possible values of variables on the left side and and on the right side the results of the operations. In the truth tables of more complicated formulas the truth values are written in the columns underneath every operator. Let us now construct the truth table of the formula in the example 3.8

X	Y	Z	X	$\wedge$	$\neg Y$	$\wedge$	$(Z$	$\Rightarrow$	$\neg X)$	$\Leftrightarrow$	Y	$\vee$	X
1	1	1		0	0	0		0	0	0		1	
1	1	0		0	0	0		1	0	0		1	
1	0	1		1	1	0		0	0	0		1	
1	0	0		1	1	1		1	0	1		1	
0	1	1		0	0	0		1	1	0		1	
0	1	0		0	0	0		1	1	0		1	
0	0	1		0	1	0		1	1	1		0	
0	0	0		0	1	0		1	1	1		0	

The truth table is an universal method for analyzing propositional formulas. Most problems that are about finding the truth value of a formula can be solved by using truth tables. However, there are some different methods for solving specific problems. Since the truth table of a formula with n variables has 2^n rows, then the volume of a truth table increases fast when the number of variable increases (when we have m operators we need to make $2^n \cdot m$ operations).

3.7 Properties of formulas

Next we will take a look at the "global" properties of propositional formulas by observing the truth value of the formula in different valuations of its variables.

Definition 3.9. A propositional formula $\mathcal{F}$ is called a **tautology** if it is true for every valuation of its variables. Formula $\mathcal{F}$ is called a **contradiction** if it is false for every valuation of its variables.

An example of a tautology is $X \vee \neg X$ that expresses the law of excluded middle. The law of non-contradiction is expressed by contradiction $X \wedge \neg X$.

Tautologies express the universal logical rules and therefore are an object of interest in logic. If we replace all propositional variables with propositions in these formulas, we will get a compound proposition that is always true. For example, if in a formula $X \vee \neg X$ we choose $X =$ "I am right", then we get a proposition "I am right or I am not right" that is true whether I am right or not.

Since a tautology is true in every case, no matter what the world is really like, then it does not contain any information and therefore it has no content (it says absolutely nothing about the world). For example, if the proposition "Tomorrow the weather will good or bad" would appear in a weather forecast, then it would be impossible to find out anything about tomorrow's weather from that sentence. Sometimes sentences that have such structure appear in everyday language,

for example “Jaan will pass the exam or he will not pass”. Even though such sentence does not carry any direct information, we still can conclude from the sentence that Jaan took some exam and we do not know yet whether he passed or not. However, such indirect interpretation is not a part of propositional logic.

Contradictions represent claims that can not be true in any condition. For example, in the formula $X \wedge \neg X$ let us choose $X =$ ”Tomorrow the weather will good”. We will get the proposition ”Tomorrow the weather will good and tomorrow the weather will bad” that can not be true, because in that case the weather of tomorrow would be both good and bad at the same time. Therefore, a contradiction does not contain any information either.

One way to find out if the formula is a tautology is to use the truth table: if a formula is a tautology, then the column that has the truth values of the formula must contain only values 1. Since a truth table is finite, then we can always determine if a formula is a tautology or not with a finite number of steps. In the terms of the theory of algorithms we say that the set of tautologies is solvable. Similar observations are true for contradictions.

Example 3.10. Show that the formula $X \wedge Y \vee X \wedge \neg Y \vee \neg X \wedge Y \vee \neg X \wedge \neg Y$ is a tautology. Let us compile the truth table:

X	Y	X	$\wedge$	Y	$\vee$	X	$\wedge$	$\neg Y$	$\vee$	$\neg X$	$\wedge$	Y	$\vee$	$\neg X$	$\wedge$	$\neg Y$
1	1		1		1		0	0	1	0	0		1	0	0	0
1	0		0		1		1	1	1	0	0		1	0	0	1
0	1		0		0		0	0	1	1	1		1	1	0	0
0	0		0		0		0	1	0	1	0		1	1	1	1

The truth value column of the given formula has only values 1, hence the formula is a tautology. That formula can be considered a generalization of the law of excluded middle for two variables.

Example 3.11. Show that the formula $\neg(X \vee Y) \wedge \neg(\neg X \vee \neg Y)$ is a contradiction. Let us compile a truth table:

X	Y	$\neg$	$(X$	$\vee$	$Y)$	$\wedge$	$\neg$	$(\neg X$	$\vee$	$\neg Y)$
1	1	0		1		0	1	0	0	0
1	0	0		1		0	0	0	1	1
0	1	0		1		0	0	1	1	0
0	0	1		0		0	0	1	1	1

Since in the truth value column of the given formula all values are 0, then the formula is a contradiction.

If two formulas are not true at the same time for any valuation of their variables, then these formulas are called **contradictory**. According to the example 3.11 we can say that formulas $\neg(X \vee Y)$ and $\neg(\neg X \vee \neg Y)$ are contradictory. Analogically we comprehend the concept of contradiction for three, four and more formulas.

Let us take a look at two classes of formulas.

Definition 3.12. A propositional formula $\mathcal{F}$ is called **satisfiable** if it is true for at least one valuation of its variables. A formula $\mathcal{F}$ is called **invalid** if it is false for at least one valuation of its variables.

For example the formula $\neg(X \vee Y)$ is satisfiable because there exists a 1 in the column of its truth values (take a look at the truth values of the second operation of the example 3.11). From the definition we can conclude that a tautology is satisfiable because such formula is true for at least one valuation of variables.

We have the following relations between the classes of formulas we have introduced.

Proposition 3.13. *Formula $\mathcal{F}$ is a tautology if and only if its negation $\neg\mathcal{F}$ is a contradiction.*

Proof. By giving a random valuation to variables in the given formula $\mathcal{F}$ we see that the truth values of formulas $\mathcal{F}$ and $\neg\mathcal{F}$ are opposite. Therefore, if $\mathcal{F}$ is always true then $\neg\mathcal{F}$ is always false and vice versa. □

Proposition 3.14. *Formula $\mathcal{F}$ is satisfiable if and only if its negation $\neg\mathcal{F}$ is not a tautology.*

Proof. If $\mathcal{F}$ is satisfiable, then there exists a valuation of variables such that $\mathcal{F}$ is true and therefore in that valuation the formula $\neg\mathcal{F}$ is false, however, that means it can not be a tautology. On the other hand, if $\neg\mathcal{F}$ is not a tautology, then there exists a valuation of variables, such that $\neg\mathcal{F}$ is false and therefore $\mathcal{F}$ is true. □

Analogically to the two previous propositions we can claim that a formula $\mathcal{F}$ is a contradiction if and only if its negation $\mathcal{F}$ is a tautology and a formula $\mathcal{F}$ is invalid if and only if $\mathcal{F}$ is not a tautology. It is always possible to determine these properties by using truth tables.

4

Transformation of formulas

***

4.1 Deductions

Deduction is a process of thinking, where by relying on one or many statements we reach a new statement. The result of deduction is called a **conclusion** and the statements we rely on are called **assumptions**. If all assumptions are true and deduction is correct, then the conclusion is also true. Therefore, concluding new statements by using logical rules is also proving these statements. We will examine the present question: when is a propositional formula true, if we know that some other propositional formulas are true. As an example we will take a look at three propositions:

1. If today is the 16th of September, then tomorrow is the 17th of September.
2. Today is the 16th of September.
3. Tomorrow is the 17th of September.

We can say that the proposition 3 can be concluded from propositions 1 and 2. Also, from the fact that a proposition and its contrapositive are logically equivalent, we can claim that the proposition "If rooftops are not wet, then it is not raining" concludes from the proposition "If it is raining, then the rooftops are wet".

Definition 4.1. We say that the formula $\mathcal{G}$ **concludes** from the formulas $\mathcal{F}_1, \ldots, \mathcal{F}_n$, if for all the valuations of the variables (that appear in the formulas), where formulas $\mathcal{F}_1, \ldots, \mathcal{F}_n$ are true, the formula $\mathcal{G}$ is also true.

The fact that the formula $\mathcal{G}$ concludes from the formulas $\mathcal{F}_1, \ldots, \mathcal{F}_n$ is denoted by symbol:

$$\mathcal{F}_1, \ldots, \mathcal{F}_n \vDash \mathcal{G},$$

where symbol $\vDash$ is read as "concludes".

Assumptions are always on the left-hand side of the symbol $\vDash$. If there are many formulas that are separated by commas on the left-hand side, then there is more than one assumption. On the left-hand side of the symbol $\vDash$ is the conclusion. Sometimes the word "conclusion" is also used in the meaning "deduction".

Deduction can be confirmed by the truth table. We will choose the rows in the truth table, where formulas $\mathcal{F}_1, \ldots, \mathcal{F}_n$ are all true and then we check if the formula $\mathcal{G}$ is also true in these rows. If that is the case, then the deduction is correct. However, if there exists a row, where formulas $\mathcal{F}_1, \ldots, \mathcal{F}_n$ are true, but the formula $\mathcal{G}$ is false, then we have found a valuation, that disproves the deduction.

Example 4.2. Let us show that from formulas $\neg(X \wedge Y)$ and $Y \Rightarrow X$ we can conclude the formula $\neg Y$. Let us compose the truth table:

X	Y	$\neg$	$(X$	$\wedge$	$Y)$	Y	$\Rightarrow$	X	$\neg Y$
1	1	0		1			1		0
1	0	1		0			1		1
0	1	1		0			0		0
0	0	1		0			1		1

Two first formulas are both true only in the second and forth row. Since the third formula is also true in these rows, the the deduction is correct, that means$\neg(X \wedge Y), Y \Rightarrow X \vDash \neg Y$.

Example 4.3. Show that from formulas $X \Rightarrow Y$ and $Y \Rightarrow Z$ we can conclude that $X \Rightarrow Z$.
This time we will not compose a truth table, instead we will check the deduction by discussion. First of all, we will notice that the only occasion, when the third formula can not be concluded from the first two formulas is when for some valuation of the variables all the assumptions (i.e., first two formulas) are true, but the conclusion (i.e., third formula) is false. In other words, both $X \Rightarrow Y$ and $Y \Rightarrow Z$ are true, but $X \Rightarrow Z$ is false. Let us remember that an implication is false if and only if the assumption is true and the conclusion is wrong. Therefore, we need to examine the case, where X is true and Z is false. We also need that the first formula $X \Rightarrow Y$ is true, hence Y must be true, but that means the second formula $Y \Rightarrow Z$ is not true, because Y is true and Z is false. Therefore, it is not possible that both $X \Rightarrow Y$ and $Y \Rightarrow Z$ are true, but $X \Rightarrow Z$ is false.

Example 4.4. Let us consider propositional variables that have the following meanings: $X =$ "The addition law for velocities is true", $Y =$ "The speed of light is the same in all directions in a frame of reference confined by fixed stars" and $Z =$ "The speed of light is same in all directions on Earth".
The formula $X \wedge Y \Rightarrow \neg Z$ is true, that means "If the addition law for velocities is true and the speed of light is same in all directions in a frame of reference confined by fixed stars, then the

speed of light is not same in all directions on Earth", because Earth clearly moves in correlation with the frame of reference confined by fixed stars. Additionally to that the formula Y is true, because it is a postulate of Einstein's relativity theory. The formula Z is also true, because it can be concluded from Michelson-Morley experiment (1887). Therefore, we will examine three equations

$$X \wedge Y \Rightarrow \neg Z, \quad Y \quad \text{and} \quad Z.$$

Let us assume that these formulas are true. Since Z is true, then $\neg Z$ is false and therefore the implication in the first formula can be true only if the conjunction $X \wedge Y$ is false. Since Y is true, then X must be false and that means $\neg X$ is true. We have shown that from these three formulas we can conclude the formula $\neg X$, that means „The addition law for velocities is not true".

Example 4.5. Check, whether the following logical deductions are true:

1. *Modus ponens* (Latin for "mode that affirms by affirming"): $X \Rightarrow Y, X \vDash Y$,
2. *Modus tollens* (Latin for "mode that denies by denying"): $X \Rightarrow Y, \neg Y \vDash \neg X$.

Let us give another example about the use of propositional logic to check that the discussion is correct.

Example 4.6. Check whether the following discussion is correct.

If a person is talented and ambitious, then he/she will have a successful career. Therefore: if a person is ambitious, but does not have a successful career, then he/she is not talented.

First of all, let us write down the discussion by propositional formulas:

$$A \wedge B \Rightarrow C \vDash B \wedge \neg C \Rightarrow \neg A.$$

The given discussion is correct if such deduction is correct. Since on the right-hand side of the symbol $\vDash$ we have a implication, we will actually start with two assumptions: $A \wedge B \Rightarrow C$ and $B \wedge \neg C$ and our goal is to show that from these assumptions we can conclude $\neg A$. Let us suppose for contradiction that the given discussion about talent and ambition is incorrect. That can only happen if both assumptions are true and the conclusion $\neg A$ is false. That also means that A is true. From the second assumption we see that since $B \wedge \neg C$ is true, then both B and $\neg C$ must also be true. However, that means C is false. Now we have a contradiction with the formula $A \wedge B \Rightarrow C$, because that is not true for the truth values of A, B and C that we found. Therefore, the discussion is correct.

Second possibility to confirm a deduction is to use the following theorem, that reduces confirming a deduction to checking whether a certain formula is a tautology. That approach is often used to analyze something with the help of computers, because there exist many algorithms for solving standard problems of propositional calculus, for example, checking if a formula is a tautology.

Theorem 4.7. *From formulas $\mathcal{F}_1, \ldots, \mathcal{F}_n$ we can conclude the formula $\mathcal{G}$ if and only if the formula $\mathcal{F}_1 \wedge \ldots \wedge \mathcal{F}_n \Rightarrow \mathcal{G}$ is a tautology.*

Proof. If from formulas $\mathcal{F}_1, \ldots, \mathcal{F}_n$ we can conclude the formula $\mathcal{G}$, then in all these valuations, where formulas $\mathcal{F}_1, \ldots, \mathcal{F}_n$ are true the formula $\mathcal{G}$ is also true. Therefore, the formula $\mathcal{F}_1 \wedge \ldots \wedge \mathcal{F}_n \Rightarrow \mathcal{G}$ is also true in these valuations. In valuations, where some of formulas $\mathcal{F}_1, \ldots, \mathcal{F}_n$ are false, the formula $\mathcal{F}_1 \wedge \ldots \wedge \mathcal{F}_n \Rightarrow \mathcal{G}$ is true, because the assumption of the implication is false. On the other hand, if the formula $\mathcal{F}_1 \wedge \ldots \wedge \mathcal{F}_n \Rightarrow \mathcal{G}$ is a tautology, then for every valuation where formulas $\mathcal{F}_1, \ldots, \mathcal{F}_n$ are true, the formula $\mathcal{F}_1 \wedge \ldots \wedge \mathcal{F}_n$ is true and that means the formula $\mathcal{G}$ is also true. □

Example 4.8. Let us take another look at the problem from the example 4.2, where we needed to confirm that from formulas $\neg(X \wedge Y)$ and $Y \Rightarrow X$ we can conclude the formula $\neg Y$. By using theorem 4.7, we will check if the formula

$$\neg(X \wedge Y) \wedge (Y \Rightarrow X) \Rightarrow \neg Y$$

is a tautology. To do so we will construct the truth table:

X	Y	$\neg(X \wedge Y)$	$\wedge$	$(Y \Rightarrow X)$	$\Rightarrow$	$\neg Y$
1	1	0	0	1	1	0
1	0	1	1	1	1	1
0	1	1	0	0	1	0
0	0	1	1	1	1	1

From the last implication column we can see that the formula is a tautology and therefore the deduction is correct. Analogically we can confirm the deductions in the other examples by showing that respective formulas are tautologies. Try to do so!

4.2 Logical equivalence

Let us compile the truth tables of formulas $\neg(X \wedge Y)$ and $\neg X \vee \neg Y$. We will see that the truth values of these formulas are the same:

X	Y	$\neg(X \wedge Y)$	$\neg X$	$\vee$	$\neg Y$
1	1	0	0	0	0
1	0	1	0	1	1
0	1	1	1	1	0
0	0	1	1	1	1

By using everyday language it is easy do see these formulas mean the same thing: first one means "It can not be that propositions X and Y are both true" and the other one means "at least one of propositions X or Y is false". There is no difference in the content of propositions that have the same truth values in every valuation, even though they might have a different form. By relying on that we give the following definition.

Definition 4.9. Formulas $\mathcal{F}$ and $\mathcal{G}$ are called **logically equivalent**, if their truth values are equal for every possible valuation of the variables.

The fact that formulas $\mathcal{F}$ and $\mathcal{G}$ are equivalent is denoted by $\mathcal{F} \equiv \mathcal{G}$.

Example 4.10. Let us show that formulas $\neg(X \vee Y)$ and $\neg X \wedge \neg Y$ are equivalent. To do so, we will compare their truth values by using the truth table:

X	Y	$\neg(X \vee Y)$	$\neg X$	$\wedge$	$\neg Y$
1	1	0	0	0	0
1	0	0	0	0	1
0	1	0	1	0	0
0	0	1	1	1	1

Therefore, we see that $\neg(X \wedge Y) \equiv \neg X \vee \neg Y$ and $\neg(X \vee Y) \equiv \neg X \wedge \neg Y$. These equivalences are called **De Morgan's laws**.

Formulas that contain different variables can also be equivalent. For example, if

$$\mathcal{F} = (Y \Rightarrow X) \wedge (\neg Y \Rightarrow X) \text{ and } \mathcal{G} = (X \vee Z) \wedge (X \vee \neg Z),$$

then $\mathcal{F} \equiv \mathcal{G}$ (check!). All tautologies are equivalent to each other, because such formulas are true for all valuations. For analogical reasons all contradictions are also equivalent.

Statements that are made by logically equivalent formulas can be considered to have the same thought or meaning, because no matter what the world is like, if one of these statements is true then so is the other and vice versa.

The next theorem shows that if we have two equivalent formulas, then we can conclude the first formula from the second and the second formula from the first.

Theorem 4.11. *Formulas $\mathcal{F}$ and $\mathcal{G}$ are equivalent if and only if $\mathcal{F} \vDash \mathcal{G}$ and $\mathcal{G} \vDash \mathcal{F}$.*

Proof. If $\mathcal{F} \equiv \mathcal{G}$, then for any valuation of variables both of these formulas are true or both are false. Therefore deductions $\mathcal{F} \vDash \mathcal{G}$ and $\mathcal{G} \vDash \mathcal{F}$ are correct.
The other way round, if $\mathcal{F} \vDash \mathcal{G}$ and $\mathcal{G} \vDash \mathcal{F}$, then there can not exit any valuation, where $\mathcal{F}$ and $\mathcal{G}$ have different truth values, that means $\mathcal{F} \equiv \mathcal{G}$.
Therefore, formulas $\mathcal{F}$ and $\mathcal{G}$ are equivalent if and only if from the formula $\mathcal{F}$ we can conclude the formula $\mathcal{G}$ and from the formula $\mathcal{G}$ we can conclude the formula $\mathcal{F}$. □

The last property is often used to prove that formulas are logically equivalent.

Checking if two formulas are logically equivalent can also be done by checking if one formula is a tautology, just like we did in the case of deduction.

Theorem 4.12. *Formulas $\mathcal{F}$ and $\mathcal{G}$ are equivalent if and only if the formula $\mathcal{F} \Leftrightarrow \mathcal{G}$ is a tautology.*

Proof. Let us assume that formulas $\mathcal{F}$ and $\mathcal{G}$ are equivalent. We will choose random truth values for all the variables in formulas $\mathcal{F}$ and $\mathcal{G}$. If for the chosen valuation both formulas $\mathcal{F}$ and $\mathcal{G}$ are true, then $\mathcal{F} \Leftrightarrow \mathcal{G}$ is also true. However, if for the chosen valuation both formulas $\mathcal{F}$ and $\mathcal{G}$

are false, then the formula $\mathcal{F} \Leftrightarrow \mathcal{G}$ is true again. Therefore, the formula $\mathcal{F} \Leftrightarrow \mathcal{G}$ is true for all valuations, that means it is a tautology.
Let us now assume that the formula $\mathcal{F} \Leftrightarrow \mathcal{G}$ is a tautology. We will choose random truth values for all variables is that formula. Since the equivalence is true, then either $\mathcal{F}$ and $\mathcal{G}$ are both true or $\mathcal{F}$ and $\mathcal{G}$ are both false. That means the truth values of formulas $\mathcal{F}$ and $\mathcal{G}$ are the same in a random valuation. According to the definition the formulas $\mathcal{F}$ and $\mathcal{G}$ are equivalent. □

4.3 Important logical equivalences

There exists a set of **important logical equivalences**. We present a selection of these type of equivalences.

1. **Identity laws**:
   a) $\mathcal{F} \wedge \mathcal{F} \equiv \mathcal{F}$,
   b) $\mathcal{F} \vee \mathcal{F} \equiv \mathcal{F}$.
2. **Commutative laws**:
   a) $\mathcal{F} \wedge \mathcal{G} \equiv \mathcal{G} \wedge \mathcal{F}$,
   b) $\mathcal{F} \vee \mathcal{G} \equiv \mathcal{G} \vee \mathcal{F}$.
3. **Associative laws**:
   a) $(\mathcal{F} \wedge \mathcal{G}) \wedge \mathcal{H} \equiv \mathcal{F} \wedge (\mathcal{G} \wedge \mathcal{H})$,
   b) $(\mathcal{F} \vee \mathcal{G}) \vee \mathcal{H} \equiv \mathcal{F} \vee (\mathcal{G} \vee \mathcal{H})$.
4. **Distributive laws**:
   a) $\mathcal{F} \wedge (\mathcal{G} \vee \mathcal{H}) \equiv \mathcal{F} \wedge \mathcal{G} \vee \mathcal{F} \wedge \mathcal{H}$,
   b) $\mathcal{F} \vee (\mathcal{G} \wedge \mathcal{H}) \equiv (\mathcal{F} \vee \mathcal{G}) \wedge (\mathcal{F} \vee \mathcal{H})$.
5. **Absorption laws**:
   a) $\mathcal{F} \wedge (\mathcal{F} \vee \mathcal{G}) \equiv \mathcal{F}$,
   b) $\mathcal{F} \vee \mathcal{F} \wedge \mathcal{G} \equiv \mathcal{F}$.
6. **De Morgan's laws**:
   a) $\neg(\mathcal{F} \wedge \mathcal{G}) \equiv \neg\mathcal{F} \vee \neg\mathcal{G}$,
   b) $\neg(\mathcal{F} \vee \mathcal{G}) \equiv \neg\mathcal{F} \wedge \neg\mathcal{G}$.
7. **Double negation law**: $\neg\neg\mathcal{F} \equiv \mathcal{F}$.
8. **Domination laws**, where t is a random tautology and f is a random contradiction:
   a) $\mathcal{F} \wedge t \equiv \mathcal{F}$,
   b) $\mathcal{F} \vee t \equiv t$,

c) $\mathcal{F} \wedge f \equiv f$,

d) $\mathcal{F} \vee f \equiv \mathcal{F}$.

9. **Implication expressed by conjunction and disjunction**:

   a) $\mathcal{F} \Rightarrow \mathcal{G} \equiv \neg(\mathcal{F} \wedge \neg\mathcal{G})$,

   b) $\mathcal{F} \Rightarrow \mathcal{G} \equiv \neg\mathcal{F} \vee \mathcal{G}$.

10. **Conjunction expressed by disjunction and implication**:

    a) $\mathcal{F} \wedge \mathcal{G} \equiv \neg(\mathcal{F} \Rightarrow \neg\mathcal{G})$,

    b) $\mathcal{F} \vee \mathcal{G} \equiv \neg\mathcal{F} \Rightarrow \mathcal{G}$.

11. **Equivalence expressed by other operators**:

    a) $\mathcal{F} \Leftrightarrow \mathcal{G} \equiv \mathcal{F} \wedge \mathcal{G} \vee \neg\mathcal{F} \wedge \neg\mathcal{G}$,

    b) $\mathcal{F} \Leftrightarrow \mathcal{G} \equiv (\mathcal{F} \Rightarrow \mathcal{G}) \wedge (\mathcal{G} \Rightarrow \mathcal{F})$.

All these equivalences can be proved by truth tables.

Example 4.13. Equivalence 9. b) $\mathcal{F} \Rightarrow \mathcal{G} \equiv \neg\mathcal{F} \vee \mathcal{G}$ is proved by the following table:

$\mathcal{F}$	$\mathcal{G}$	$\mathcal{F} \Rightarrow \mathcal{G}$	$\neg\mathcal{F} \vee \mathcal{G}$
1	1	1	1
1	0	0	0
0	1	1	1
0	0	1	1

These equivalences can also be proved by discussion.

Example 4.14. For example let us prove the first distributive law $\mathcal{F} \wedge (\mathcal{G} \vee \mathcal{H}) \equiv \mathcal{F} \wedge \mathcal{G} \vee \mathcal{F} \wedge \mathcal{H}$ (item 4).

Proof. Let us assume that the formula $\mathcal{F} \wedge (\mathcal{G} \vee \mathcal{H})$ is true. That means both $\mathcal{F}$ and $\mathcal{G} \vee \mathcal{H}$ must be true. If in the last relation the formula $\mathcal{G}$ is true then $\mathcal{F} \wedge \mathcal{G}$ is also true. However, if $\mathcal{H}$ is true, then $\mathcal{F} \wedge \mathcal{H}$ is also true. In either case the second formula of the equivalence we want to prove is true, because disjunction is true if one of its components is true.
The other way round, let $\mathcal{F} \wedge \mathcal{G} \vee \mathcal{F} \wedge \mathcal{H}$ be true. If $\mathcal{F} \wedge \mathcal{G}$ is true, then $\mathcal{F}$ and $\mathcal{G}$ are both true, from that we can conclude that $\mathcal{G} \vee \mathcal{H}$ is also true. Therefore, the first formula is true. However, if $\mathcal{F} \wedge \mathcal{H}$ is true, then $\mathcal{F}$ and $\mathcal{H}$ are both true, from that we can conclude that $\mathcal{G} \vee \mathcal{H}$ is true. In that case the first formula is also true. Therefore, we have shown that we can conclude the second formula from the first formula and the other way round. That means these formulas are equivalent. □

Since the truth value of conjunction, disjunction and equivalence does not change when we change the order of the components, then these logical operators are commutative. However, implication is not commutative. Therefore, for implication it is important to notice the order of

the components.

Equivalences 9. – 11. show that some of the logical operators are equivalent to combinations of other logical operators.

4.4 Negating decisions

The rules of negating decisions are summed up in the following table:

Decision	**Negation of the decision**
All S is P	Some S is not P
None of S is not P	Some S is P
Some S is P	None of S is not P
Some S is not P	All S is P

The first row of the table corresponds to a already familiar property for quantifiers

$$\neg(\forall x\ P(x)) \equiv \exists x\ \neg P(x),$$

and the third row in the table corresponds to the equivalence

$$\neg(\exists x\ P(x)) \equiv \forall x\ \neg P(x).$$

Rules for negating compound decisions can be written with the help of propositional equivalences as follows:

Decision	**Negation of the decision**
$\neg A$	A
$A \wedge B$	$\neg A \vee \neg B$
$A \vee B$	$\neg A \wedge \neg B$
$A \Rightarrow B$	$A \wedge \neg B$
$A \Leftrightarrow B$	$(A \wedge \neg B) \vee (\neg A \wedge B)$

The last row in the table can be illustrated by the following example.

Example 4.15. Proposition: "A person is happy at work if and only if he/she gets payed reasonably".
Negation of the proposition: "Some person is happy at work even though he/she does not get payed reasonably or he/she gets payed reasonably, but is not happy at work".

Knowing equivalence 6., i.e., De Morgan's laws is helpful also for negating the following proposition.

Example 4.16. Proposition "For all integers a and b, if the product ab is even, then a is even or b is even." Its negation is following: "There exist integers a and b such that ab is even and a and b are both odd."

4.5 Transformations of formulas

Equivalences have the same role in propositional logic as identities have in algebra. Just like we use identities in algebra to simplify expressions, we can also use logical equivalences to transform and simplify propositional logic expressions and the new expression we get is always equivalent to the initial expression. One transformation means replacing a formula or one of its components with some other equivalent formula. If we replace some component $\mathcal{F}_1$ in the formula $\mathcal{F}$ with its equivalent $\mathcal{F}_2$, then the formula we get and the formula $\mathcal{F}$ have the same truth values for all valuations because the new component $\mathcal{F}_2$ has the same truth value as $\mathcal{F}_1$ for all valuations.

When making transformations it is usually reasonable to eliminate all operators besides negation, conjunction and disjunction, because between them we have the most simple relations.

Theorem 4.17. *For every propositional formula $\mathcal{F}$ there exists an equivalent formula that does not contain operators $\Rightarrow$ and $\Leftrightarrow$.*

Proof. We can conclude the theorem from previous discussion and from logical equivalences 9. and 11. □

Example 4.18. Transform the formula $\neg X \vee Y \Rightarrow X \wedge Y$.

Solution. Let us denote $\mathcal{F} = \neg X \vee Y \Rightarrow X \wedge Y$. We will replace the implication in the given formula by negation and disjunction (9b) and we get $\mathcal{F} \equiv \neg(\neg X \vee Y) \vee (X \wedge Y)$. By using De Morgan's law (6b) we will get rid of the negation before the first bracket: $\mathcal{F} \equiv (\neg\neg X \wedge \neg Y) \vee (X \wedge Y)$. We can lose the double negation and unnecessary brackets: $\mathcal{F} \equiv X \wedge \neg Y \vee X \wedge Y$. Now we can apply the distributive law (4a) and bring the variable X in front of brackets: $\mathcal{F} \equiv X \wedge (\neg Y \vee Y)$. In the last formula the term $\neg Y \vee Y$ is a tautology and we can eliminate it according to law (8a). In conclusion, we get $\mathcal{F} \equiv X$.

□

Example 4.19. Express $\neg(X \Leftrightarrow Y)$ by negation, disjunction and conjunction.

Solution.

$$\begin{aligned}\neg(X \Leftrightarrow Y) &\equiv \neg((X \Rightarrow Y) \wedge (Y \Rightarrow X)) \\ &\equiv (\neg(X \Rightarrow Y)) \vee (\neg(Y \Rightarrow X)) \\ &\equiv (X \wedge \neg Y) \vee (Y \wedge \neg X).\end{aligned}$$

□

Example 4.20. Transform the formula $(X \Rightarrow (Y \Rightarrow Z)) \Leftrightarrow \neg(Y \Rightarrow X)$ to a logically equivalent formula that does not contain operators $\Leftrightarrow$ and $\Rightarrow$.

Solution.

$$\begin{aligned}(X \Rightarrow (Y \Rightarrow Z)) \Leftrightarrow \neg(Y \Rightarrow X) &\equiv (X \Rightarrow (\neg Y \vee Z)) \Leftrightarrow (\neg(\neg Y \vee X)) \\ &\equiv (\neg X \vee (\neg Y \vee Z)) \Leftrightarrow \neg(\neg Y \vee X) \\ &\equiv ((\neg X \vee (\neg Y \vee Z)) \wedge \neg(\neg Y \vee X)) \vee (\neg(\neg X \vee (\neg Y \vee Z)) \wedge \neg\neg(\neg Y \vee X)) \\ &\equiv ((\neg X \vee (\neg Y \vee Z)) \wedge (\neg X \wedge Y)) \vee ((X \wedge (Y \wedge \neg Z)) \wedge (\neg Y \vee X)) \\ &\equiv (\neg X \vee \neg Y \vee Z) \wedge (\neg X \wedge Y) \vee (X \wedge Y \wedge \neg Z \wedge (\neg Y \vee X)).\end{aligned}$$

□

Additionally we can claim the following:

Proposition 4.21. *For every formula there exists an equivalent formula that contains only following operators:*

a) $\wedge$ *and* $\neg$*,*

b) $\vee$ *and* $\neg$*,*

c) $\Rightarrow$ *and* $\neg$*.*

Proof.

a) To prove the first statement we use equivalences (9a), (11a) and the equivalence $X \vee Y \equiv \neg(\neg X \wedge \neg Y)$ that we get from the equivalence (6).

b) To explain the second statement we use equivalences (9b), (11a) and $X \wedge Y \equiv \neg(\neg X \vee \neg Y)$ that we get from the equivalence (6).

c) To prove the third statement we use equivalences (11b), (10a) and (10b).

□

4.6 Principal disjunctive normal form

The idea behind the normal form is to reduce the syntactic diversity of propositional formulas by giving them a simple form. Additionally, for formulas that are in principal normal form it is very easy to see, when these formulas are true.

Definition 4.22. A conjunction between variables or their negations is called a **basic conjunction**.

Basic conjunctions are, for example, $X \wedge Y$, $\neg X \wedge \neg Y$, X, $X \wedge \neg Y \wedge Z$, $X \wedge Y \wedge \neg Y$.

Definition 4.23. A basic conjunction is called **principal**, if every one of the given variables appears exactly once in the conjunction.

Notice that whether a conjunction is principal or not depends on the set of given variables. If we have variables X, Y, Z, then from the previous examples only $X \wedge \neg Y \wedge Z$ is pricipal.

Definition 4.24. A propositional formula that is equivalent to formula $\mathcal{F}$ and that is a disjunction of basic conjunctions is called a **disjunctive normal form** of the propositional formula $\mathcal{F}$.

One formula can have more than one disjunctive normal form.

Example 4.25. Let $\mathcal{F} \equiv X \Rightarrow Y$. According to basic equivalences we know that formulas $\mathcal{F}$ and $\neg X \vee Y$ are equivalent. But the formula $X \wedge Y \vee \neg X \wedge Y \vee \neg X \wedge \neg Y$ is also equivalent to the formula $\mathcal{F}$ (prove by truth table!).

Definition 4.26. The **principal (full) disjunctive normal form** of a propositional formula $\mathcal{F}$ is the formula that is equivalent to the formula $\mathcal{F}$ and that is a disjunction of principal basic conjunctions.

Remark. Similarly to principal disjunctive normal form we can also define the principal conjunctive normal form that is a conjunction of principal basic disjunctions.

Example 4.27. According to the example 4.25 the only principal disjunctive normal form of formula $\mathcal{F} \equiv X \Rightarrow Y$ is $X \wedge Y \vee \neg X \wedge Y \vee \neg X \wedge \neg Y$. The formula $\neg X \vee Y$ that is equivalent to $\mathcal{F}$ is not a principal disjunctive normal form, because it does not consist of principal basic conjunctions.

Let us now examine the valuations for which the normal form is true. A very useful property of the principal disjunctive normal form, and the main reason it is used, is the fact that it is very easy to determine for which valuations it is true and for which it is false.

In the following we use the notation $X^t = X$ and $X^f = \neg X$, or in general X^α, where $\alpha = t$ or $\alpha = f$. It is easy to confirm that $X^\alpha = t \Leftrightarrow X = \alpha$ (check!).

Proposition 4.28. *A disjunction of principal basic conjunctions*

$$X_1^{\alpha_{11}} \wedge \ldots \wedge X_n^{\alpha_{1n}} \vee X_1^{\alpha_{21}} \wedge \ldots \wedge X_n^{\alpha_{2n}} \vee \ldots \vee X_1^{\alpha_{m1}} \wedge \ldots \wedge X_n^{\alpha_{mn}}$$

is true exactly for valuations $(\alpha_{i1}, \ldots, \alpha_{in})$*, where* $i = 1, \ldots, m$*.*

Example 4.29. The formula $X \wedge Y \vee \neg X \wedge \neg Y$ is in principal disjunctive normal form. That formula is true for valuations (t, t) and (f, f) and false for valuations (t, f) and (f, t).

Example 4.30. The formula

$$X \wedge \neg Y \wedge Z \vee \neg X \wedge Y \wedge Z \vee \neg X \wedge \neg Y \wedge \neg Z$$

in principal disjunctive normal form and therefore it is true exactly for valuations (t, f, t), (f, t, t) and (f, f, f).

Exercise 4.31. Find a formula that has three variables and that is true if and only if two of the variables are wrong.

Theorem 4.32. *A formula has the principal disjunctive normal form if and only if it is satisfiable.*

From theorem 4.32 we can conclude that a contradiction does not have a principal disjunctive normal form.

4.7 Transforming a formula to principal disjunctive normal form

A given (satisfiable) formula can be transformed to principal disjunctive normal form with following steps.

1. First of all we eliminate implications and equivalences by using logical equivalences $\mathcal{F} \Rightarrow \mathcal{G} \equiv \neg\mathcal{F} \vee \mathcal{G}$ and $\mathcal{F} \Leftrightarrow \mathcal{G} \equiv \mathcal{F} \wedge \mathcal{G} \vee \neg\mathcal{F} \wedge \neg\mathcal{G}$. The formula we get as a result contains only negations, conjunctions and disjunctions.

2. Next, we transform the formula so that negations only appear directly before variables. To do so we use De Morgan's laws $\neg(\mathcal{F} \wedge \mathcal{G}) \equiv \neg\mathcal{F} \vee \neg\mathcal{G}$ and $\neg(\mathcal{F} \vee \mathcal{G}) \equiv \neg\mathcal{F} \wedge \neg\mathcal{G}$. If we have a double negation somewhere, then we simply discard it. As a result we get a formula, with no negations in front of brackets.

3. We replace the conjunctions of disjunctions with disjunctions of conjunctions by using distributive law $\mathcal{F} \wedge (\mathcal{G} \vee \mathcal{H}) \equiv \mathcal{F} \wedge \mathcal{G} \vee \mathcal{F} \wedge \mathcal{H}$.

4. If there are any conjunctions that are contradictions, i.e., conjunctions that have both X and $\neg X$, then we can just leave them out. If we have equal conjunctions, then because of the idempotent law $\mathcal{F} \wedge \mathcal{F} \equiv \mathcal{F}$ we keep just one of them.

5. To get the principal disjunctive normal form we need to transform every basic conjunction to principal basic conjunction. For example, if in a basic conjunction K we have a missing variable X, then with the equivalence

$$K \equiv K \wedge (X \vee \neg X) \equiv K \wedge X \vee K \wedge \neg X$$

   we can add the variable X to both basic conjunctions $K \wedge X$ and $K \wedge \neg X$. If necessary, we will repeat that step and from equal conjunctions we will leave out all but one.

The principal disjunctive normal form of a formula can also be found with the help of the truth table.

Example 4.33. Find the principal disjunctive normal form of the formula $X \wedge \neg Y \wedge (Z \Rightarrow \neg X) \Leftrightarrow Y \vee X$.

X	Y	Z	X	$\wedge$	$\neg Y$	$\wedge$	$(Z$	$\Rightarrow$	$\neg X)$	$\Leftrightarrow$	Y	$\vee$	X
1	1	1		0	0	0		0	0	0		1	
1	1	0		0	0	0		1	0	0		1	
1	0	1		1	1	0		0	0	0		1	
1	0	0		1	1	1		1	0	1		1	
0	1	1		0	0	0		1	1	0		1	
0	1	0		0	0	0		1	1	0		1	
0	0	1		0	1	0		1	1	1		0	
0	0	0		0	1	0		1	1	1		0	

1. From the truth table we can see that the formula $X \wedge \neg Y \wedge (Z \Rightarrow \neg X) \Leftrightarrow Y \vee X$ is true only in valuations $(1, 0, 0)$, $(0, 0, 1)$ and $(0, 0, 0)$.

2. The principle basic conjunctions respective to these valuations are $X \wedge \neg Y \wedge \neg Z$, $\neg X \wedge \neg Y \wedge Z$ and $\neg X \wedge \neg Y \wedge \neg Z$.

3. Therefore, the principal disjunctive normal form of the formula $X \wedge \neg Y \wedge (Z \Rightarrow \neg X) \Leftrightarrow Y \vee X$ is
$$(X \wedge \neg Y \wedge \neg Z) \vee (\neg X \wedge \neg Y \wedge Z) \vee (\neg X \wedge \neg Y \wedge \neg Z).$$

5

Sets

***

No one shall expel us from the paradise that Cantor has created –
D. Hilbert

In this chapter, we will discuss one of the most fundamental ideas in mathematics – sets and basics of set theory. Since set is a basic conception then it is not defined by using other concepts. Sets as objects are used to construct all other mathematical structures (it is easy to notice it in the following chapters). Our goal in this course is not to look into the axiomatic structure of set theory, but to give a less formal idea of what a set is, how mathematicians denote sets and which of the important concepts and relations can be described by using sets.

We can see sets around us all the time. Let us take a look at the following examples of sets: students in this course who own an iPad, fruits bought from the store this week, negative integers, ect. As a child, we all learned to say the alphabet out loud, but actually we were saying letters that belong to the set called "English alphabet". Therefore, a set is a collection of objects.

The founder of set theory, Georg Cantor, defined a set in a more elaborate way: set is a collection of distinct objects that can be considered as a whole. What else can we gather from that definition? First of all, all the objects in the set are different. Secondly, for any object, it must be possible to determine whether it belongs to the set or not.

A collection of distinct objects that is considered an object itself is called a **set** if for any object we can determine whether it is in the set or not.

Objects that form a set (belong to the set) are called **elements of the set**. An element of the set and the set itself are always considered to be different objects, therefore a set is never an

element of itself.

Sets are usually denoted by uppercase letters $A, B, C, X, Y, \ldots$, however, elements of the set are denoted by lowercase letters $a, b, c, x, y, \ldots$. If an element a belongs to the set A, we write $a \in A$, and if a is not an element of the set A, we write $a \notin A$.

Example 5.1. Let $A = \{a \mid a \text{ is a set}\}$. That would be a „set of all sets“. If A was a set itself, then A would be one of its elements, meaning $A \in A$. However, that is impossible, therefore A is not a set. In this case we talk about a **class of all sets** or a **collection of all sets**.

We consider two sets A and B **equal**, and write $A = B$, if sets A and B contain exactly the same elements.
Previous clause can also be written as:

$$A = B \quad \Leftrightarrow \quad \forall x \, (x \in A \Leftrightarrow x \in B).$$

For example, if $A = \{x \mid x \in \mathbb{R}, x^2 - 3x + 2 = 0\}$ and $B = \{1, 2\}$, then by solving the quadratic equation we get $A = B$.

5.1 What is a set?

When describing a set, it is very important to write down exactly which elements belong to the set. The requirement that elements are different means that a set can't contain multiple elements that we consider equal. For example, we can not talk about a set that contains two red and three blue balls, when we consider red balls equal to each other and blue balls equal to each other as well. The set of solutions to equation $(x - 1)^2 = 0$ has exactly one element, not two equal numbers 1.

If a set consists of a small number of elements, then it is possible to list the elements between commas, enclosed by braces. For example, $A = \{1, 2, 3\}$ is a set that consists of elements 1, 2 and 3. It is not important in which order we write the elements of the set. Therefore, $A = \{3, 2, 1\} = \{2, 1, 3\}$ all represent previously mentioned set A. The set of presidents of Estonia is $A = \{$Päts, Meri, Rüütel, Ilves, Kaljulaid$\}$ and the set of all positive even numbers that are smaller than 20 is $B = \{2, 4, 6, 8, 10, 12, 14, 16, 18\}$.

However, some sets contain too many elements to just list them all. For example, $X = \{1, 3, 5, \ldots, 49\}$ is the set of all positive odd numbers that are smaller than 50 and $Y = \{2, 4, 6, \ldots\}$ is the set of all positive even numbers. The three dots stand for "continue the list the same way".

Instead of listing all the elements in the set, we can determine whether an element belongs to a set or not by using a condition, because often a set contains elements that satisfy a certain condition or elements that have a common property. In those cases, we write $S = \{x \colon p(x)\}$ or $S = \{x \mid p(x)\}$, where $p(x)$ denotes a condition or a list of conditions that all the elements that belong to set S must satisfy. (In different sources either a colon or vertical bar is used between

the element general form and the condition.) For example, if we are interested in all the real solutions of an equation, then $S = \{x \in \mathbb{R} \mid (x-1)(x+2)(x+3) = 0\}$ is a set of all real numbers x, that satisfy the equation $(x-1)(x+2)(x+3) = 0$. That means S is a set of all real solutions of that equation. We could have also written $S = \{1, -2, -3\}$. Even though that way of writing is a lot easier, it does not give us any information about the fact that we were originally looking for solutions of a certain equation.

Some sets in mathematics are used so often that they are denoted by their own symbols. The most significant sets of numbers are

- **Natural numbers** $\mathbb{N} = \{1, 2, 3, \dots\}$;
- **Integers** $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$;
- **Rational numbers** $\mathbb{Q} = \{q \mid q = \frac{m}{n}, m \in \mathbb{Z}, n \in \mathbb{N}\}$;
- **Real numbers** $\mathbb{R}$;
- **Irrational numbers** $\mathbb{I}$;
- **Complex numbers** $\mathbb{C} = \{z \mid z = x + iy, x, y \in \mathbb{R}, i^2 = -1\}$.

The intervals of numbers can also be written as sets:

- **Closed interval** $[a, b] = \{x \mid x \in \mathbb{R}, a \leq x \leq b\}$;
- **Open interval** $(a, b) = \{x \mid x \in \mathbb{R}, a < x < b\}$;
- **Half open intervals** $[a, b) = \{x \mid x \in \mathbb{R}, a \leq x < b\}$ and $(a, b] = \{x \mid x \in \mathbb{R}, a < x \leq b\}$.

Example 5.2. Different ways to describe a set:

1. $A = \{x \mid x \in \mathbb{R}, x^2 - 3x + 2 = 0\} = \{1, 2\}$;
2. $B = \{3n \mid n \in \mathbb{N}, n > 2\} = \{9, 12, 15, \dots\}$.

Exercise 5.3. Write down a set of even integers in two different ways.

A set might not contain any elements. It might seem weird to look at sets, that do not have any elements, but actually we come across such sets very often and in very different situations. For example, if A is a set of real solutions of equation $x^2 + 1 = 0$, then there are no elements in set A. In mathematics there is only one set that does not contain any elements and that is the empty set. The empty set is denoted by symbol $\emptyset$. For example, a set of all real numbers x, that satisfies an inequality $x^2 < 0$, is also an empty set.

Definition 5.4. The **empty set** $\emptyset$ is a set that has no elements.

The elements of a set can also be other sets.

Example 5.5.

1. The set $S = \{1, 2, \{1, 2\}, \emptyset\}$ consists of four elements and two of those elements are sets, namely $\{1, 2\}$ and $\emptyset$.

2. The set $T = \{0, \{1, 2, 3\}, 4, 5\}$ also consists of four elements, namely three integers 0, 4 and 5, and one set $\{1, 2, 3\}$. Even though $2 \in \{1, 2, 3\}$, the number 2 is not an element of T; i.e. $2 \notin T$.

For a finite set S we use symbol $|S|$ to denote the number of elements in set S and we call it **cardinality** or **size** of the set. If $A = \{1, 2\}$ and $B = \{1, 2, \{1, 2\}, \emptyset\}$, then $|A| = 2$ and $|B| = 4$. The size of empty set is 0: $|\emptyset| = 0$. We will later return to the concept of cardinality for infinite sets.
Let us take a look at some more examples.

Example 5.6. Let $D = \{n \in \mathbb{N}, n \leq 9\}$, $E = \{x \in \mathbb{Q}, x \leq 9\}$, $H = \{x \in \mathbb{R} \colon x^2 - 2 = 0\}$ and $J = \{x \in \mathbb{Q} \colon x^2 - 2 = 0\}$.

(a) Describe the set D by listing all its elements.

(b) Name the three elements that belong to the set E, but do not belong to the set D.

(c) Describe the set H by listing all its elements.

(d) Describe the set J in a different way.

(e) Find the size of the sets D, H and J.

Solution.

(a) $D = \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$.

(b) $\frac{7}{5}, 0, -3$.

(c) $H = \{\sqrt{2}, -\sqrt{2}\}$.

(d) $J = \emptyset$.

(e) $|D| = 9, |H| = 2$ and $|J| = 0$.

□

Example 5.7. Which of the following sets contain number -2?

(a) $S_1 = \{-1, -2, \{-1\}, \{-2\}, \{-1, -2\}\}$;

(b) $S_2 = \{x \in \mathbb{N} \colon -x \in \mathbb{N}\}$;

(c) $S_3 = \{x \in \mathbb{Z} \colon x^2 = 2^x\}$;

(d) $S_4 = \{x \in \mathbb{Z} \colon |x| = -x\}$;

(e) $S_5 = \{\{-1, -2\}, \{-2, -3\}, \{-1, -3\}\}$.

Solution. Number -2 belongs to the sets S_1 and S_4. Looking at the set S_4 we see that $|-2| = 2 = -(-2)$. The set S_2 is an empty set, therefore $-2 \notin S_2$. Since $(-2)^2 = 4$ and $2^{-2} = \frac{1}{4}$, then $-2 \notin S_3$. All the elements of the set S_5 are sets and therefore -2 can not be an element of the set S_5, because it is a number not a set. □

Exercise 5.8. Come up with a five letter word, such that $|S| = 3$, where S is a set of letters that are represented in the word.

5.2 Subset

Now let us examine different cases where some elements in one set are also elements in a different set. One extreme case is when every element of some set A also belongs to another set B. A different extreme case is if none of the elements from the set A belong to the set B.

Definition 5.9. Set A is called a **subset** of set B if all the elements of the set A are also elements of the set B (that means every element in the set A belongs to the set B).

If set A is a subset of set B, we write $A \subset B$. If set A is not a subset of set B, we write $A \not\subset B$. We can also express subsets by using quantifiers:

$$A \subset B \text{ means that } \forall x\ (x \in A \Rightarrow x \in B)$$

and

$$\begin{aligned} A \not\subset B \text{ means that } & \neg(\forall x\ (x \in A \Rightarrow x \in B)) \\ & \equiv \exists x\ \neg(x \in A \Rightarrow x \in B) \\ & \equiv \exists x\ (x \in A \wedge x \notin B) \end{aligned}$$

Therefore, $A \not\subset B$ means that there exists an element in the set A that does not belong to the set B.

Example 5.10.

1. $(0, 1) \subset [0, 1]$.
2. Subsets of the set $\{a, b\}$ are: $\emptyset, \{a\}, \{b\}, \{a, b\}$.

Proposition 5.11. *The relation $\subset$ has following properties:*

1. ***Reflexivity**: For every set A we know that $A \subset A$;*
2. ***Antisymmetry**: If sets A and B satisfy $A \subset B$ and $B \subset A$, then $A = B$;*
3. ***Transitivity**: If sets A, B and C satisfy $A \subset B$ and $B \subset C$, then $A \subset C$;*
4. *Empty set $\emptyset$ is a subset of every set.*

Proof. Let us prove the third and the fourth properties. The proofs of the first two properties are left to be solved independently.
3. We assume that $A \subset B$ and $B \subset C$. Let us show that $A \subset C$. To prove that we take a random element x from the set A and show that then $x \in C$. Since we assumed $A \subset B$ then from the fact $x \in A$ we can conclude that $x \in B$. According to second assumption $B \subset C$, every element of the set B belongs to the set C. Since $x \in B$ we can conclude that $x \in C$. Now we have shown that a random element x from the set A belongs to the set C. Therefore, $A \subset C$.
4. Let us prove by contradiction that $\emptyset \subset A$ for every set A. Let us assume that there exists a set A such that $\emptyset \not\subset A$. According to definition in that case there exists an element x in the empty set that does not belong to the set A. However, that is impossible, because set $\emptyset$ does not contain any element. Therefore $\emptyset \subset A$ for every set A. □

Remark. The second property of the relation $\subset$ is often used to prove that two sets are equal. To prove equality it is sufficient to show that each of the sets is a subset of the other set. Therefore, to prove the equality $A = B$ it is shown that $A \subset B$ and $B \subset A$. If $A \neq B$, then there must exists at least one element that belongs to one of those sets but not to the other set.

Example 5.12. It is easy to notice the transitivity property between the sets of numbers: since $\mathbb{Q} \subset \mathbb{R}$ and $\mathbb{R} \subset \mathbb{C}$, then of course $\mathbb{Q} \subset C$.

Proposition 5.13. *There exists exactly one empty set* $\emptyset$.

Proof. Suppose for contradiction, that there exists two empty sets $\emptyset_1$ and $\emptyset_2$. Now according to proposition 5.11 property 4. we know that $\emptyset_1 \subset \emptyset_2$ (because $\emptyset_1$ is an empty set) and $\emptyset_2 \subset \emptyset_1$ (because $\emptyset_2$ is an empty set). Since $\emptyset_1 \subset \emptyset_2$ and $\emptyset_2 \subset \emptyset_1$, then according to proposition 5.11 property 2. we get $\emptyset_1 = \emptyset_2$. However, that is in contradiction with the assumption $\emptyset_1 \neq \emptyset_2$. Therefore, there exists only one empty set. □

Exercise 5.14. Find two sets A and B such that A is both an element and a subset of the set B.

Solution. We are looking for two sets A and B such that $A \in B$ and $A \subset B$. Let us begin with a set that has only one element, for example $A = \{1\}$. We want the statement $A \in B$ to be true, therefore the set B must contain the set $\{1\}$ as an element. On the other hand, we want statement $A \subset B$ to be true, that means every element of the set A must also be an element of the set B. Since number 1 in the only element of the set A, then number 1 must also be an element of the set B. Therefore one possibility to choose set B is $B = \{1, \{1\}\}$. However a set $B = \{1, 2, \{1\}\}$ also satisfies the conditions, as well as many other sets. □

Definition 5.15. Set A is called a **proper subset** of set B if set A is a subset of set B and $A \neq B$. In that case we write $A \subsetneq B$.

Remark. The difference between relations $A \subset B$ and $A \subsetneq B$ is analogical to the difference between strict and non-strict inequality.

Example 5.16.

1. If $S = \{4, 5, 7\}$ and $T = \{3, 4, 5, 6, 7\}$, then $S \subsetneq T$.

2. The relations between sets of numbers $\mathbb{N} \subsetneq \mathbb{Z} \subsetneq \mathbb{Q} \subsetneq \mathbb{R} \subsetneq \mathbb{C}$.

3. If $a < b$, then $(a, b) \subsetneq (a, b] \subsetneq [a, b]$.

Exercise 5.17. Prove that the set of integers $\mathbb{Z}$ is a proper subset of the set of rational numbers $\mathbb{Q}$.

Solution. We need to show two things. First of all, we need to show that if element x belongs to the set $\mathbb{Z}$, then x also belongs to the set $\mathbb{Q}$ (the condition that one set is a subset of other set). Secondly, we need to show that there exists an element y that belongs to the set $\mathbb{Q}$, but does not belong to the set $\mathbb{Z}$ (the condition that one set is a proper subset of another set). We can write these conditions by using propositional calculus:

$$\forall x \, (x \in \mathbb{Z} \Rightarrow x \in \mathbb{Q}) \quad \text{and} \quad \exists y \, (y \in \mathbb{Q} \wedge y \notin \mathbb{Z}).$$

Proving the first formula is easy. Let $x \in \mathbb{Z}$. Since every integer can be divided by 1, we can write $x = \frac{x}{1}$. Now we have presented the number x in a form, where both numerator and denominator are integers. According to the definition of rational numbers, we know that x is a rational number, therefore $x \in \mathbb{Q}$.
To prove the second formula we need to find a rational number that is not an integer. For example let us choose $y = \frac{1}{2}$. According to the definition y is a rational number, but y in not an integer. Therefore we have found a number y that belongs to the set of rational numbers, but does not belong to the set of integers. Now we have shown that the set of integers $\mathbb{Z}$ is a proper subset of the set of rational numbers $\mathbb{Q}$. □

Exercise 5.18. Prove that the set of rational numbers $\mathbb{Q}$ is a proper subset of the set of real numbers $\mathbb{R}$.

Let A be a set. The **power set** of A is a **set of all subsets** of A and is usually denoted by $\mathcal{P}(A) = \{X \mid X \subset A\}$.

Exercise 5.19. Find the power sets of all the following sets. Also determine $|A|$ and $|\mathcal{P}(A)|$.

1. $A = \emptyset$;

2. $A = \{a, b\}$;

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

Solution.

1. $\mathcal{P}(A) = \{\emptyset\}$, $|A| = 0$ and $|\mathcal{P}(A)| = 1$;

2. $\mathcal{P}(A) = \{\emptyset, \{a\}, \{b\}, \{a, b\}\}$, $|A| = 2$ and $|\mathcal{P}(A)| = 4$;

3. $\mathcal{P}(A) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}$, $|A| = 3$ and $|\mathcal{P}(A)| = 8$.

□

Let us notice that for every set in previous example we have a relation $|\mathcal{P}(A)| = 2^{|A|}$. As it turns out, the relation is always true. Therefore if a set A has n elements, then that set has 2^n distinct subsets.

Proposition 5.20. *If set A has n elements, then the set A has 2^n distinct subsets.*

Proof. Solve independently. □

Example 5.21. If $C = \{\emptyset, \{\emptyset\}\}$, then $\mathcal{P}(C) = \{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}, \{\emptyset, \{\emptyset\}\}\}$. In this case it is important to understand that none of the sets $\emptyset, \{\emptyset\}$ and $\{\{\emptyset\}\}$ are equal to each other. (An empty box and a box that contains an empty box are not the same thing.) For the given set C it is correct to write

$$\emptyset \subset C, \quad \emptyset \subsetneq C, \quad \emptyset \in C, \quad \{\emptyset\} \subset C, \quad \{\emptyset\} \subsetneq C, \quad \{\emptyset\} \in C$$

as well as it is correct to write $\{\{\emptyset\}\} \subset C$, $\{\{\emptyset\}\} \notin C$ and $\{\{\emptyset\}\} \in \mathcal{P}(C)$.

6

Set operations

***

In mathematics the art of proposing a question must be held of higher value than solving it. – G. Cantor

6.1 Union

We can combine integers (by adding, subtracting, multiplying and sometimes dividing) to get new integers. The same way we can form new sets by uniting two sets.

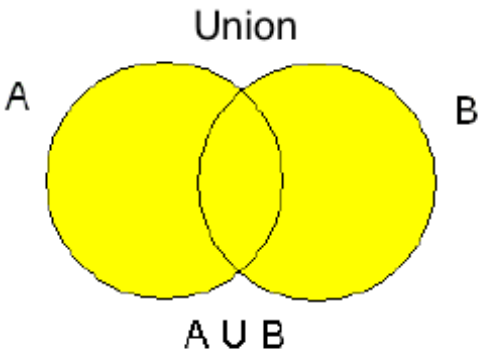
Definition 6.1. The **union** of two sets A and B is a set $A \cup B$ that consists of all elements that belong to at least one of the sets A or B, i.e.

$$A \cup B = \{x \mid x \in A \vee x \in B\}.$$

Word "or" is used in a non-exclusive way again, that means the element x either belongs to the set A or to the set B or to both sets at the same time. However, the elements that belong to both sets are only considered once.

We notice that $A \subset A \cup B$ and $B \subset A \cup B$ for every pair of sets A and B.

To get a graphical overview of the sets we get by applying set-theoretic operations, we use **Venn diagrams**. If sets A and B are represented by circles, then the colored area in the diagram is their union.



Example 6.2.

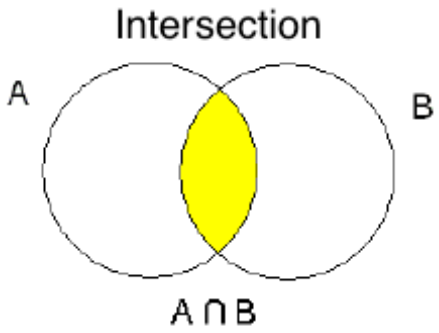
1. If $A = \{a, b, c\}$ and $B = \{a, c, d, e\}$, then $A \cup B = \{a, b, c, d, e\}$;
2. $[0, 1) \cup (0, 1] = [0, 1]$;
3. $\mathbb{N} \cup \mathbb{Q} = \mathbb{Q}$.

6.2 Intersection

Definition 6.3. The **intersection** of two sets A and B is the set $A \cap B$ that consists of all elements that belong both to the set A and to the set B, i.e.

$$A \cap B = \{x \mid x \in A \wedge x \in B\}.$$

It is easy to see that $A \cap B \subset A$ and $A \cap B \subset B$ for any sets A and B. By using the Venn diagram we can describe the intersection as follows:



Example 6.4.

1. If $A = \{a, b, c\}$ and $B = \{a, c, d, e\}$, then $A \cap B = \{a, c\}$;
2. $[0, 1) \cap (0, 1] = (0, 1)$;
3. $\mathbb{N} \cap \mathbb{Q} = \mathbb{N}$.

Proposition 6.5. *Let A and B be sets. Then $A \cap B \subset A \cup B$.*

Proof. We need to show that if $x \in A \cap B$, then $x \in A \cup B$. Therefore, let x be a random element of the set $A \cap B$. According to the definition of the intersection, the element x belongs both to the set A and to the set B. Without loss of generality we examine the set A (we could just as easily choose the set B). Since $x \in A$, then according to the definition of the union $x \in A \cup B$. Therefore, we have shown that $A \cap B \subset A \cup B$. □

If two sets A and B do not have any common elements, then $A \cap B = \emptyset$ and sets A and B are called **disjoint**. For example, the sets of rational numbers and irrational numbers are disjoint.

Exercise 6.6. What can we say about sets A and B, when $A \cap B = \emptyset$? When $A \cap B = A$? When $A \cap B = B$? Draw the corresponding Venn diagrams.

Exercise 6.7. Prove that if an element x does not belong to the union of two sets A and B, then it does not belong to their intersection.

Theorem 6.8. *Union and intersection have following properties:*

1. ***Idempotent laws**: $A \cup A = A$, $A \cap A = A$;*
2. ***Commutative laws**: $A \cup B = B \cup A$, $A \cap B = B \cap A$;*
3. ***Associative laws**: $(A \cup B) \cup C = A \cup (B \cup C)$, $(A \cap B) \cap C = A \cap (B \cap C)$;*

4. ***Distributive laws:*** $(A \cup B) \cap C = (A \cap C) \cup (B \cap C)$, $(A \cap B) \cup C = (A \cup C) \cap (B \cup C)$.

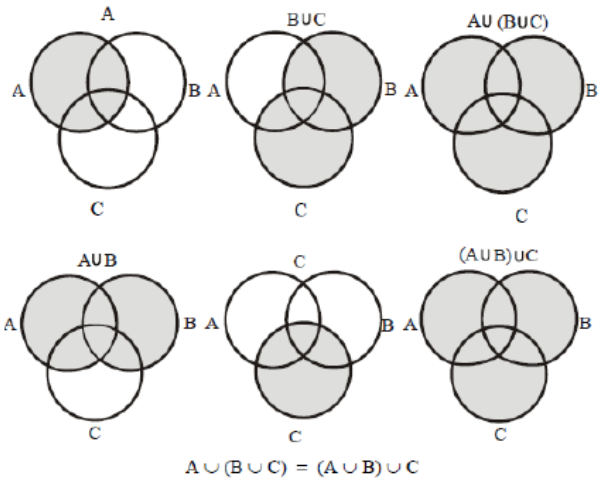
Proof. Properties 1.– 3. can be concluded directly from the definition and are to be solved independently. As an example we will prove the second law of distribution $(A \cap B) \cup C = (A \cup C) \cap (B \cup C)$.

(i) Let $x \in (A \cap B) \cup C$. Then $x \in A \cap B$ or $x \in C$. If $x \in C$, then $x \in A \cup C$ and $x \in B \cup C$, therefore $x \in (A \cup C) \cap (B \cup C)$. However, if $x \notin C$, then $x \in A \cap B$, i.e., $x \in A$ and $x \in B$. Therefore, $x \in A \cup C$ and $x \in B \cup C$, i.e. $x \in (A \cup C) \cap (B \cup C)$. Now we have proved that $(A \cap B) \cup C \subset (A \cup C) \cap (B \cup C)$.

(ii) Let $x \in (A \cup C) \cap (B \cup C)$. Then $x \in (A \cup C)$ and $x \in (B \cup C)$. If $x \in C$, then $x \in (A \cap B) \cup C$. However, if $x \notin C$, then $x \in A$ and $x \in B$, that means $x \in A \cap B$ and $x \in (A \cap B) \cup C$. We have proved that $(A \cup C) \cap (B \cup C) \subset (A \cap B) \cup C$ and $(A \cap B) \cup C \subset (A \cup C) \cap (B \cup C)$. From that we can conclude the second distributive law.

□

The associative laws can also be illustrated by Venn diagrams as follows: (However, please notice that drawing Venn diagrams is not a proof!)



6.3 Difference

Definition 6.9. The **difference** of two sets A and B is the set $A \setminus B$, that consists of all elements that belong to the set A, but do not belong to the set B, i.e.

$$A \setminus B = \{x \mid x \in A \wedge x \notin B\}.$$

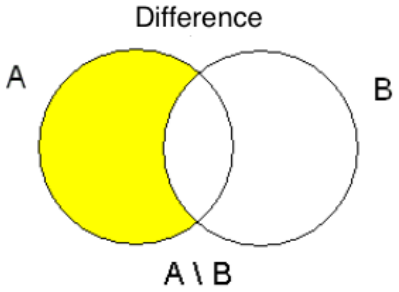
Example 6.10.

1. If $A = \{1, 2, 3, 4, 5\}$ and $B = \{2, 4, 6\}$, then $A \setminus B = \{1, 3, 5\}$ and $B \setminus A = \{6\}$;
2. $[0, 1) \setminus (0, 1) = \{0\}$;

3. $\mathbb{N} \setminus \mathbb{Z} = \emptyset$.

The first example also confirms the fact that usually $A \setminus B \neq B \setminus A$.

The Venn diagram of the difference of two sets is following:



Exercise 6.11. Let $A = \{x \in \mathbb{R} \colon |x| \leq 3\}$, $B = \{x \in \mathbb{R} \colon |x| > 2\}$ and $C = \{x \in \mathbb{R} \colon |x-1| \leq 4\}$.

1. Describe the sets A, B and C by using intervals;
2. Find $A \cap B$, $A \setminus B$, $B \cap C$, $B \cup C$, $B \setminus C$ and $C \setminus B$.

Solution.

1. $A = [-3, 3], B = (-\infty, -2) \cup (2, \infty)$ and $C = [-3, 5]$;
2. $A \cap B = [-3, -2) \cup (2, 3]$, $A \setminus B = [-2, 2]$, $B \cap C = [-3, -2) \cup (2, 5]$, $B \cup C = (-\infty, \infty)$, $B \setminus C = (-\infty, -3) \cup (5, \infty)$ and $C \setminus B = [-2, 2]$.

□

Proposition 6.12. *Let A, B and C be sets. Then*

$$A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C) \quad \text{and} \quad A \setminus (B \cap C) = (A \setminus B) \cup (A \setminus C).$$

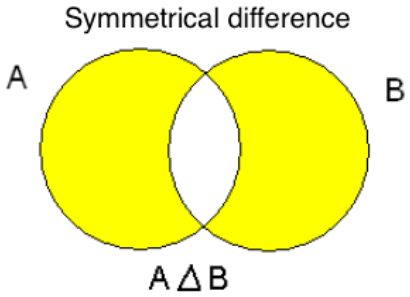
Proof. Solve independently. □

6.4 Symmetric difference

Definition 6.13. The **symmetric difference** of two sets A and B is the set $A \triangle B$ that consists of all elements that belong to exactly one of the sets A and B, i.e.

$$A \triangle B = \{x \mid (x \in A \wedge x \notin B) \vee (x \notin A \wedge x \in B)\} = (A \setminus B) \cup (B \setminus A).$$

Symmetrical difference is illustrated by the following Venn diagram:



Example 6.14. If $A = \{a, b, c\}$ and $B = \{a, c, d, e\}$, then $A \triangle B = \{b, d, e\}$.

Proposition 6.15. *Let A and B be sets. Then $A \triangle B = (A \cup B) \setminus (A \cap B)$.*

Remark. Examine and compare that result with the Venn diagram that describes the symmetric difference.

Proof of the proposition 6.15. We need to prove that two sets $A \triangle B$ and $(A \cup B) \setminus (A \cap B)$ are equal. To do that we show $A \triangle B \subset (A \cup B) \setminus (A \cap B)$ and $(A \cup B) \setminus (A \cap B) \subset A \triangle B$.

1. Firstly, we will show that if $x \in A \triangle B$, then $x \in (A \cup B) \setminus (A \cap B)$. Let $x \in A \triangle B$. The symmetric difference is defined through union, therefore $x \in (A \setminus B) \cup (B \setminus A)$. From that we can conclude that $x \in A \setminus B$ or $x \in B \setminus A$. We now divide the proof into two separate parts and for both of them we need to show that $x \in (A \cup B) \setminus (A \cap B)$.

   (a) Let $x \in A \setminus B$, which means $x \in A$ but $x \notin B$. Since $x \in A$, then we can see that $x \in A \cup B$. Since $x \notin B$, then the element x does not belong to both sets, that means $x \notin A \cap B$. In conclusion, $x \in (A \cup B) \setminus (A \cap B)$.

   (b) Let $x \in B \setminus A$, which means $x \in B$ but $x \notin A$. Analogically we can see that $x \in A \cup B$ but $x \notin A \cap B$. Therefore, $x \in (A \cup B) \setminus (A \cap B)$.

2. Secondly, we need to show that $(A \cup B) \setminus (A \cap B) \subset A \triangle B$. Let $x \in (A \cup B) \setminus (A \cap B)$. By definition $x \in A \cup B$ but $x \notin A \cap B$. Our goal is to show that $x \in A \triangle B = (A \setminus B) \cup (B \setminus A)$, therefore we need to show $x \in A \setminus B$ or $x \in B \setminus A$. What information is at our disposal right now? Since $x \in (A \cup B) \setminus (A \cap B)$, then x belongs to one of the sets A or B but not to both. In other words $x \in A$ and $x \notin B$ or $x \in B$ but $x \notin A$. However, that means $x \in A \setminus B$ or $x \in B \setminus A$, exactly what we were looking for! Therefore, $x \in (A \setminus B) \cup (B \setminus A) = A \triangle B$. Since we have shown that both sets are subsets to one another, then $A \triangle B = (A \cup B) \setminus (A \cap B)$.

□

In addition to proposition 6.15, symmetrical difference also has the following properties.

Proposition 6.16. *Let A, B and C be sets. Then*

1. ***Commutative law:*** $A \triangle B = B \triangle A$;
2. ***Associative law:*** $(A \triangle B) \triangle C = A \triangle (B \triangle C)$;
3. ***Distributive law:*** $(A \triangle B) \cap C = (A \cap C) \triangle (B \cap C)$;
4. $A \triangle B = A \cup B \Leftrightarrow A \cap B = \emptyset$.

Proof. Solve independently. □

Exercise 6.17. Use Venn diagrams to describe sets $A \setminus (B \cup C)$, $A \cap (B \setminus C)$, $(A \setminus B) \setminus C$ and $A \setminus (B \setminus C)$.

6.5 Complement

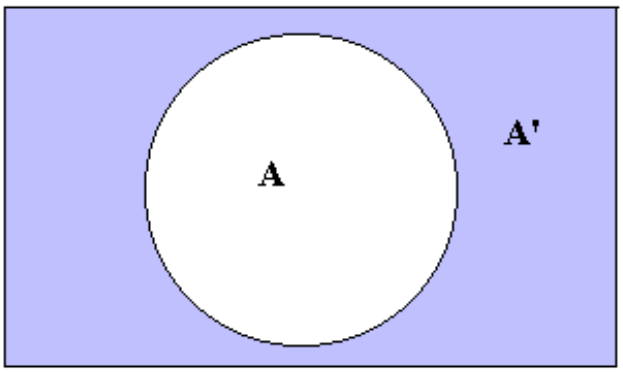
In school mathematics we work with several sets, for example, the set of natural numbers and the set of real numbers. We examine the elements and subsets of those sets as well as we take a closer look at the relations, operations and functions defined between the elements of those sets. In set theory, if for some set we examine its elements and subsets as well as relations, operation and functions that are defined between its elements, then that set is called an **universal set** and is denoted by letter U.

If we work with the elements of some universal set U, then for every subset $A \subset U$, we might also be interested in such elements of the universal set that do not belong to the set A. For example, if in arithmetic the universal set is the set of natural numbers, then we are interested in even numbers but additionally we are also interested in odd numbers.

Definition 6.18. The **complement** of a set A is the set A' that consists of all elements of the universal set U that do not belong to the set A, i.e.

$$A' = \{x \in U : x \notin A\} = U \setminus A.$$

We can describe complement of set A by using Venn diagram:



Example 6.19.

1. If $U = \mathbb{Z}$, then $\mathbb{N}' = \{0, -1, -2, \dots\}$;
2. If $U = \mathbb{R}$, then $\mathbb{Q}' = \mathbb{I}$.

Proposition 6.20. *Let U be a universal set and $A, B \subset U$. The complement has the following properties:*

1. $\emptyset' = U$;
2. $U' = \emptyset$;
3. $A \cup A' = U$;
4. $A \cap A' = \emptyset$;
5. $A'' = A$;
6. $(A \cup B)' = A' \cap B'$;
7. $(A \cap B)' = A' \cup B'$.

Proof. Properties 1. – 5. can be concluded directly from the definition and are to be solved independently. Properties 6. and 7. are called De Morgan's laws. These laws express the duality of union and intersection. We will prove only the De Morgan's law 7. The proof of law 6. is analogical.
7. To show that two sets are equal we need to show that both of them are subsets of one another; firstly that $(A \cap B)' \subset A' \cup B'$ and secondly that $A' \cup B' \subset (A \cap B)'$. Let $x \in (A \cap B)'$. Then $x \notin A \cap B$. However, that means $x \notin A$ or $x \notin B$. Therefore $x \in A'$ or $x \in B'$, but that is same as $x \in A' \cup B'$.
Now let $x \in A' \cup B'$. Then $x \in A'$ or $x \in B'$, that means $x \notin A$ or $x \notin B$. Since x does not belong to at least one of the sets A or B, then it does not belong to their intersection, that is $x \notin A \cap B$. Hence $x \in (A \cap B)'$. Therefore, we have shown that both sets are subsets of each other and that means sets $(A \cap B)'$ and $A' \cup B'$ are equal. □

The difference $A \setminus B$ of the sets A and B is sometimes also called the **relative complement** of the set B with respect to the set A. The reason for that is the definition $A \setminus B = \{x \mid x \in A \wedge x \notin B\}$.

The four set-theoretic operations (union, intersection, difference and symmetrical difference) are related in the sense that every one of them can be expressed through others. From De Morgan's laws we can conclude the **duality principle**, which means that from given sets, for example sets X, Y and Z, we can form new sets by using operations $\cap$, $\cup$ and $'$. Also, when we have any true equality between those sets we formed, then we get another true equality by replacing all sets with their complements and operations $\cap$ and $\cup$ with operations $\cup$ and $\cap$ respectively.

For example, we can write $A \cap B = A \setminus (A \setminus B)$ and we already know that $A \triangle B = (A \setminus B) \cup (B \setminus A)$.

Exercise 6.21.

1. Express $A \cup B$ and $A \setminus B$ through operations $\cap$ and $\triangle$;
2. Express $A \cap B$ and $A \setminus B$ through operations $\cup$ and $\triangle$;
3. Express $A \cup B$ through operations $\setminus$ and $\triangle$.

Exercise 6.22. Prove that it is not possible to express $A \cup B$ through operations $\cap$ and $\setminus$ as well as it is not possible to express $A \setminus B$ through operations $\cup$ and $\cap$.

6.6 Properties of operations – summary

It is easy to notice that when simplifying and comparing expressions it is useful to know the algebraic properties of operations. When introducing a new set-theoretic operation we always brought out some properties that are easy to conclude from definitions. For example, we found out that union, intersection and symmetrical difference are commutative operations, but difference is not (find a counterexample!).

Some set-theoretic equalities are deduced from equalities that we know from propositional calculus. Union, intersection and complement are defined through elements belonging to sets by using disjunction, conjunction and negation respectively. Therefore, these operations have the same properties that the respective operations in propositional calculus have.

There are also many more complicated equalities that apply to set-theoretic operations and that include more than just one operation. Additionally to idempotent, commutative and associative laws there are also a few distributive laws – that means some operations can be expressed through others, etc. We will now present some more important distributive laws, which are often used, and some of which we are already familiar with.

1. Just like there are distributive laws between disjunction and conjunction, there are also two distributive laws between union and intersection. Additionally, taking an intersection with difference or symmetrical difference is also distributive.

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C), \qquad A \cup (B \cap C) = (A \cup B) \cap (A \cup C),$$
$$A \cap (B \setminus C) = (A \cap B) \setminus (A \cap C), \qquad A \cap (B \triangle C) = (A \cap B) \triangle (A \cap C).$$

2. Absorption laws
$$A \cup (A \cap B) = A, \qquad A \cap (A \cup B) = A.$$

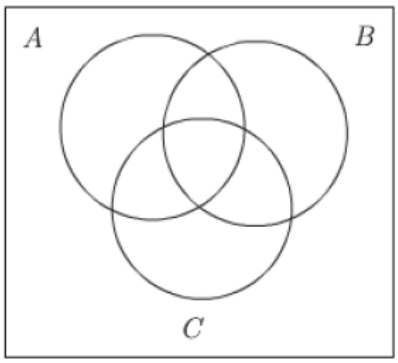
3. De Morgan's laws
$$(A \cap B)' = A' \cup B', \qquad (A \cup B)' = A' \cap B'.$$

4. Relations between difference and other operations
$$A \setminus B = A \setminus (A \cap B), \qquad A \cup B = A \cup (B \setminus A), \qquad (A \setminus B) \setminus C = A \setminus (B \cup C).$$

5. Symmetrical difference is symmetrical between A and B:
$$A \triangle B = (A \cup B) \setminus (A \cap B).$$

6.7 Finite and infinite unions and intersections

Often we want to unite three or more sets by using set-theoretic operations. Typical Venn diagram for three sets is following:



The union of three sets is defined as $A \cup B \cup C = \{x \mid x \in A \vee x \in B \vee x \in C\}$. Again, if we want element x to belong to the union of three sets, then it has to belong to at least one of those sets.

Exercise 6.23. Let us assume that $x \in A \cup B \cup C$, but $x \notin A \cap B \cap C$. To which sets can the element x belong to?

The definitions of union and intersection of two sets can be generalized to:

- n sets, where $n \in \mathbb{N}$;
- sequence of sets $\{A_i \colon i = 1, 2, 3, \dots\}$;
- and even to an arbitrary system of sets.

All these generalized definitions apply the same idea that is used for two elements: union consists of objects that belong to at least one of the sets and intersection consists of objects that belong to each of the sets.

Therefore we can define the union and intersection of n sets ($n \in \mathbb{N}$) with equalities:

$$A_1 \cup A_2 \cup \ldots \cup A_n = \{x \mid x \in A_1 \vee x \in A_2 \vee \ldots \vee x \in A_n\},$$
$$A_1 \cap A_2 \cap \ldots \cap A_n = \{x \mid x \in A_1 \wedge x \in A_2 \wedge \ldots \wedge x \in A_n\}.$$

Example 6.24. Let $A_1 = \{0, 2, 5\}$, $A_2 = \{1, 2, 5\}$ and $A_3 = \{2, 5, 7\}$. Then

$$\bigcup_{i=1}^{3} A_i = \{0, 1, 2, 5, 7\} \quad \text{and} \quad \bigcap_{i=1}^{3} A_i = \{2, 5\}.$$

The union and intersection of the sequence of sets $A_1, A_2, A_3, \dots$ can be defined with equalities:

$$\bigcup_{i=1}^{\infty} A_i = A_1 \cup A_2 \cup A_3 \cup \ldots = \{x \mid \text{exists } i \geq 1 \text{ such that } x \in A_i\},$$
$$\bigcap_{i=1}^{\infty} A_i = A_1 \cap A_2 \cap A_3 \cap \ldots = \{x \mid \text{for every } i \geq 1 \text{ we have } x \in A_i\}.$$

Now let $\mathcal{I}$ be a set and let us take a look at the system of sets $(A_\alpha)_{\alpha\in\mathcal{I}}$. Then we can define the union and intersection of that system of sets as follows:

$$\bigcup_{\alpha\in\mathcal{I}} A_\alpha = \{x \mid \exists\alpha \in \mathcal{I} \text{ such that } x \in A_\alpha\},$$
$$\bigcap_{\alpha\in\mathcal{I}} A_\alpha = \{x \mid \forall\alpha \in \mathcal{I} \text{ we have } x \in A_\alpha\}.$$

For example,

$$\bigcup_{i\in\{1,\dots,n\}} A_i = \bigcup_{i=1}^{n} A_i \quad \text{and} \quad \bigcap_{i\in\{1,\dots,n\}} A_i = \bigcap_{i=1}^{n} A_i$$

and

$$\bigcup_{i\in\mathbb{N}} A_i = \bigcup_{i=1}^{\infty} A_i \quad \text{and} \quad \bigcap_{i\in\mathbb{N}} A_i = \bigcap_{i=1}^{\infty} A_i$$

Example 6.25. For every $i \in \mathbb{N}$ let $A_i = \{-i, 0, i\}$. Then

$$\bigcup_{i=1}^{\infty} A_i = \mathbb{Z} \quad \text{and} \quad \bigcap_{i=1}^{\infty} A_i = \{0\}.$$

Example 6.26. Let $\mathcal{I} = [1, 4]$ and for every $\alpha \in \mathcal{I}$ let $A_\alpha = [0, \alpha]$. Then we have, for example, $A_2 = [0, 2]$, $A_{\sqrt{2}} = [0, \sqrt{2}]$ and $A_\pi = [0, \pi]$ and

$$\bigcup_{\alpha\in\mathcal{I}} A_\alpha = \bigcup_{\alpha\in[1,4]} A_\alpha = [0, 4] \quad \text{and} \quad \bigcap_{\alpha\in\mathcal{I}} A_\alpha = \bigcap_{\alpha\in[1,4]} A_\alpha = [0, 1].$$

Example 6.27.

1. $\bigcup_{n\in\mathbb{Z}}[n - \frac{1}{2}, n + \frac{1}{2}) = \mathbb{R}$;
2. $\bigcap_{n=1}^{\infty}(0, \frac{1}{n}) = \emptyset$;
3. $\bigcup_{a,b\in\mathbb{Q}}(a, b) = \mathbb{R}$;
4. For every set A we know $\cup_{a\in A}\{a\} = A$.

De Morgan's laws can be generalized to any number (even infinite) of sets. For example, for union and intersection they are following:

$$\left(\bigcup_{\alpha\in\mathcal{I}} A_\alpha\right)' = \bigcap_{\alpha\in\mathcal{I}} A'_\alpha, \qquad \left(\bigcap_{\alpha\in\mathcal{I}} A_\alpha\right)' = \bigcup_{\alpha\in\mathcal{I}} A'_\alpha.$$

6.8 Cartesian product

To define more complex mathematical structures it is necessary to have so called ordered pairs (a, b), where $a \in A$, $b \in B$ and A, B are some random sets.

Definition 6.28. The **Cartesian product** of two sets A and B is a set of all pairs (a, b), where $a \in A$, $b \in B$ and where the order of the elements is important.

The Cartesian product of sets A and B is denoted by symbol $A \times B$. Therefore

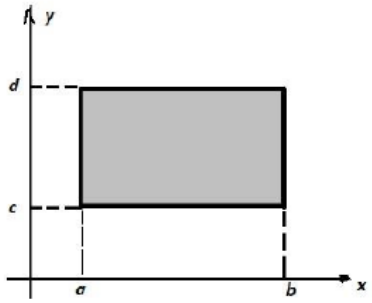
$$A \times B = \{(a, b) \mid a \in A,\ b \in B\}.$$

The set $A \times B$ is also called the set of all ordered pairs (a, b), where $a \in A$, $b \in B$. Word „ordered" means in this case that two pairs are considered equal if and only if the elements are equal respectively, i.e.

$$(a, b) = (c, d) \Leftrightarrow a = c \wedge b = d.$$

The Cartesian product $A \times A$ is also called a **Cartesian square** of the set A and is denoted by A^2.

Example 6.29. We can present the rectangle $R = \{(x, y) \colon a \leq x \leq b, c \leq y \leq d\}$ as a Cartesian product of intervals $[a, b]$ and $[c, d]$, that means $R = [a, b] \times [c, d]$.



Example 6.30. If $A = \{a, b, c, d, e, f, g, h\}$ and $B = \{1, 2, 3, 4, 5, 6, 7, 8\}$, then the Cartesian product $A \times B = \{(a, 1), \ldots, (h, 8)\}$ is equivalent to the grid of the chessboard (for chess we write it shorter $a1, \ldots, h8$).

It should be easy to see that taking a Cartesian product of sets is usually not a commutative operation, i.e. if $A \neq B$, then $A \times B \neq B \times A$. For example, $[1, 3] \times [4, 5] \neq [4, 5] \times [1, 3]$ (make a graph!).

Proposition 6.31. *Let A, B, C and D be sets. If $A \subset B$ and $C \subset D$, then $A \times C \subset B \times D$.*

Proof. Let A, B, C and D be such sets that satisfy $A \subset B$ and $C \subset D$. We need to prove that $A \times C \subset B \times D$. Therefore, let w be an element from the set $A \times C$. We need to show that $w \in B \times D$. Since $w \in A \times C$, then we can write w in the form (a, c), where $a \in A$ and $c \in C$ (according to the definition of Cartesian product.). Since $a \in A$ and $A \subset B$, then also $a \in B$. Analogically, since $c \in C$ and $C \subset D$, then $c \in D$. According to the definition of Cartesian product, we can state that $(a, c) \in B \times D$, that is same as $w \in B \times D$. Therefore, we have shown that every element of the set $A \times C$ is also an element of the set $B \times D$. According to the definition of subset, we know that $A \times C \subset B \times D$. □

Exercise 6.32. Prove that if $A \neq \emptyset$ and $B \neq \emptyset$, then $A \times B = B \times A$ if and only if $A = B$.

Theorem 6.33. *Let A, B, C and D be sets. Then we have the following equalities:*

1. $A \times \emptyset = \emptyset$, $\emptyset \times A = \emptyset$;
2. $A \times (B \cup C) = (A \times B) \cup (A \times C)$;
3. $A \times (B \cap C) = (A \times B) \cap (A \times C)$;
4. $(A \times B) \cap (C \times D) = (A \cap C) \times (B \cap D)$;
5. $A \times (B \setminus C) = (A \times B) \setminus (A \times C)$.

Proof. Let us prove the equality 2. by using equivalence:

$$\begin{aligned}(a,b) \in A \times (B \cup C) &\Leftrightarrow a \in A \wedge b \in B \cup C \\ &\Leftrightarrow a \in A \wedge (b \in B \vee b \in C) \\ &\Leftrightarrow (a \in A \wedge b \in B) \vee (a \in A \wedge b \in C) \\ &\Leftrightarrow (a,b) \in A \times B \vee (a,b) \in A \times C \\ &\Leftrightarrow (a,b) \in (A \times B) \cup (A \times C).\end{aligned}$$

Prove the rest of the equalities independently. □

The concept of the Cartesian product of two sets can easily be generalized to any finite number of sets. We denote ordered n-tuples by $(a_1, a_2, \ldots, a_n)$. The **Cartesian product** of sets $A_1, \ldots, A_n$ is the set $A_1 \times \ldots \times A_n$ that consists of all the ordered n-tuples $(a_1, a_2, \ldots, a_n)$, where the element a_i belongs to the set A_i for every $i = 1, \ldots, n$. In other words,

$$A_1 \times \ldots \times A_n = \{(a_1, \ldots, a_n) \colon a_1 \in A_1, \ldots, a_n \in A_n\}.$$

The Cartesian product $\underbrace{A \times \ldots \times A}_{n}$ is denoted by A^n and called an n-th **Cartesian power** of set A.

If set A has m elements and set B has n elements, then the set $A \times B$ has $m \cdot n$ elements. In general, if A_1 has m_1 elements, ..., A_n has m_n elements, then $A_1 \times \ldots \times A_n$ kas $m_1 \cdot \ldots \cdot m_n$ elements.

Exercise 6.34. Prove that if $A_i \neq \emptyset$ and $B_i \neq \emptyset$ $(i = 1, \ldots, n)$, then

1. $A_1 \times \ldots \times A_n \subset B_1 \times \ldots \times B_n$ if and only if $A_1 \subset B_1, \ldots, A_n \subset B_n$;
2. $A_1 \times \ldots \times A_n = B_1 \times \ldots \times B_n$ if and only if $A_1 = B_1, \ldots, A_n = B_n$.

7

Number theory and mathematical induction

***

7.1 Divisibility and prime numbers

Definition 7.1. We say that an integer a **divides** an integer b (denoted by $a \mid b$), if there exists an integer c, such that $ac = b$.

Notation $a \mid b$ means the same as notation $b \vdots a$ i.e integer b is divisible by a.

Example 7.2. $3 \mid 15$

Divisibility relation has the following properties.

Proposition 7.3. *Let a, b and c be integers. Then*

1. $a \mid a$
2. *If $a \mid b$ and $b \mid c$, then $a \mid c$.*
3. *If $a \mid b$ and $a \mid c$, then $a \mid (b \pm c)$*
4. *If $a \mid b$, then $ac \mid bc$ for every $c \in \mathbb{Z}$.*
5. $a \mid 1$ *if and only if* $a = 1$ *or* $a = -1$.

Proof. Let us prove property 2., rest of the properties can be proven analogically.
Let $a, b, c \in \mathbb{Z}$ be such integers that $a \mid b$ and $b \mid c$. Since $a \mid b$, then there exists an $m \in \mathbb{Z}$ such that $b = am$. Analogically there exists an $n \in \mathbb{Z}$ such that $c = bn$. Now we see that

$$c = bn = (am) \cdot n = a \cdot (mn).$$

Since $mn \in \mathbb{Z}$, then we have proven that $a \mid c$. □

Lemma 7.4. *Inequality $a^2 + a \geq 0$ is true for every integer a.*

Proof. Prove independently. □

Theorem 7.5. *Let a be an integer and b be a natural number. Then there exist unique integers q (quotient) and r (remainder), such that*

$$a = bq + r \quad \text{and} \quad 0 \leq r < b.$$

Proof. Let $a \in \mathbb{Z}$ and $b \in \mathbb{N}$. We examine the set

$$A = \{a - bx \mid x \in \mathbb{Z}, a - bx \geq 0\} \subset \mathbb{N} \cup \{0\}.$$

First of all, we notice that $A \neq \emptyset$. Indeed,

$$a - b(-a^2) = a + ba^2 \geq a + a^2 \geq 0,$$

where the last inequality is true according to the lemma 7.4 and therefore $a - b(-a^2) \in A$. Since every nonempty subset of the set $\mathbb{N} \cup \{0\}$ has the smallest element, then the set A also has the smallest element $r = a - bq \in A$, where $q \in \mathbb{Z}$.
Let us show that $r < b$. To do so, we suppose that $r \geq b$. Let us denote $r' := r - b$, then

$$0 \leq r' = r - b = a - b(q + 1) \in A \quad \text{and} \quad r' < r,$$

that is in contradiction with the choice of r. Therefore we have found such $q, r \in \mathbb{Z}$ that $a = bq + r$ and $0 \leq r < b$.
Let us now show that q and r are unique. To do so, we will assume that there exist q_1, q_2, r_1, r_2 such that

$$a = bq_1 + r_1 = bq_2 + r_2 \quad \text{and} \quad 0 \leq r_1, r_2 < b.$$

Then $b(q_1 - q_2) = r_2 - r_1$. Since $b \geq 1$, $|r_2 - r_1| < b$ and $q_1 - q_2 \in \mathbb{Z}$, then from the equality $|r_2 - r_1| = |b| \cdot |q_1 - q_2|$ we can conclude that $q_1 - q_2 = 0$ and therefore $r_2 - r_1 = 0$. Now we have proven that $q_1 = q_2$ and $r_1 = r_2$. □

Definition 7.6. A natural number $p > 1$ that has exactly two positive dividers; 1 and p, is called a **prime number**. A natural number that is bigger than 1 and that is not a prime number is called a **composite number**.

Let us now formulate the fundamental theorem of arithmetic that originates from the Euclid's Elements IV (around 350 B.C) and that is a foundation for many theorems about natural numbers. We will prove the theorem in the chapter 7.3, because it requires the use of mathematical induction.

Theorem 7.7 (Fundamental theorem of arithmetic)**.** *Every natural number $n > 1$ has a unique prime factorization (that means there exists a unique $r \in \mathbb{N}$ and unique prime numbers $p_1, \ldots, p_r$ such that $n = p_1 \cdot \cdots \cdot p_r$).*

Theorem 7.8 (Euclid)**.** *The set of prime numbers is infinite.*

Proof. Let prime numbers be denoted by $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, $p_4 = 7, \ldots$. Let us suppose that there exists the largest prime number p_n. We will examine the integer $a = p_1 p_2 \ldots p_n + 1$. Since $a > 1$, then according to the fundamental theorem of arithmetic there exists a prime number that divides a. Since we assumed that $p_1, p_2, \ldots, p_n$ are the only prime numbers, then there must exist $i \in \{1, \ldots, n\}$ such that $p_i \mid a$. According to property 3 of proposition 7.3 we get that $p_i \mid a - p_1 p_2 \ldots p_n$ that means $p_i \mid 1$ and is in contradiction with $p_i > 1$. □

7.2 Mathematical induction

We all think that we know natural numbers well and that we are familiar with many properties of natural numbers. For example, we know that natural numbers can be divided into a product of prime numbers and that the sum of natural numbers does not depend on the order of the addends and so on. But in reality the set of natural numbers has a very rich nature and even the best mathematicians do not know all of its properties. For example, it is not known whether the set of twin primes (i.e. primes that have a difference of two) is finite or infinite. The twin primes are for example 3 and 5, 5 and 7, 11 and 13, 17 and 19, 29 and 31, 41 and 43, 59 and 61, 71 and 73, 101 and 103, etc. This is only one of many unsolved problems among the natural numbers.

In this chapter we will get acquainted with the property of natural numbers that claims that every natural number is followed by a natural number. More specifically, each natural number is followed by exactly one natural number. That is one of the most important properties of natural numbers and therefore an axiom. That property expresses the nature of natural numbers and also shows that natural numbers are infinite and ordered by size. Another axiom is the existence of number 1, because the property can be used only if we have the first element.

The statements that are true for all natural numbers can not be proven by checking if the statement is true for each number individually, because the set of natural numbers is infinite. Therefore, we need a method that uses the property of following. The following statement is true: **if a set that consists of some natural numbers contains the number 1 and satisfies the property of following then that set contains all natural numbers**. We can use that to prove that a statement is true for all natural numbers with just a finite number of steps.

First of all, we need to show that the statement is true for the natural number 1. That can be done by checking.

Second of all, we need to show that the statement has the property of following. If we have done that, then we can say that the statement is true for all natural numbers.

When solving problems by mathematical induction, we often need to first put together a series of statements according to the problems.

The process of generalizing from one natural number to all natural numbers is called *induction*.

In philosophy induction is a way of discussion, where from knowing that some objects have a certain property it is concluded that other object or even all similar objects also have the property. Induction is an inductive discussion. Unlike deduction, induction does not guarantee that if all assumptions are true, then the conclusion is true as well, that means it is not proven that the generalization is correct. However, for us it is very important that true assumptions would guarantee us a true conclusion and that can be achieved by mathematical induction. In this chapter we will examine a new way of proving – the method of *mathematical induction* – that is better than regular induction, because it avoids incorrect generalizations. Even though the method name contains the word „induction“, it is still a deductive way of proving.

We will start with an example of a problem and prove it by mathematical induction.

Statement. The sum of the first n odd numbers is n^2.

We will illustrate the statement with the table:

n	the sum of the first n odd numbers	n^2
1	$1 =$	1
2	$1 + 3 =$	4
3	$1 + 3 + 5 =$	9
4	$1 + 3 + 5 + 7 =$	16
5	$1 + 3 + 5 + 7 + 9 =$	25
$\vdots$	$\vdots$	$\vdots$
n	$1 + 3 + 5 + 7 + 9 + 11 + \cdots + (2n - 1) =$	n^2
$\vdots$	$\vdots$	$\vdots$

Let us notice that in the first five rows the sum of the first n odd numbers is indeed equal to n^2. Also, it is easy to see that the last addend of each row is $2n-1$ (i.e. if $n = 2$, then the last addend of the second column is $2 \cdot 2 - 1 = 3$; if $n = 3$, then the third odd number in the sum is $2 \cdot 3 - 1 = 5$, etc.). However, we still do not know for sure it the sum $1 + 3 + 5 + 7 + 9 + 11 + \ldots + (2n - 1)$ is indeed equal to n^2. Is the statement true for all natural numbers? Let us rephrase the statement as follows. For every natural number n (every row in the table) let the statements S_n be the following:

$$
\begin{aligned}
&S_1 \colon 1 = 1^2 \\
&S_2 \colon 1 + 3 = 2^2 \\
&S_3 \colon 1 + 3 + 5 = 3^2 \\
&\quad \vdots \\
&S_n \colon 1 + 3 + 5 + 7 + \cdots + (2n - 1) = n^2 \\
&\quad \vdots
\end{aligned}
$$

We want to know: are all of them true?

Mathematical induction is designed to answer that type of questions, where we have lots of statements $S_1, S_2, \ldots, S_n, \ldots$ and we need to prove that all of them are true. Method is actually very simple and to understand it better, we can think of statements as a line of dominoes. Now let us assume we proved the first statement. That corresponds to knocking over the first domino. Now let us assume we also proved that if statement S_k is true (respective domino falls), then also the following statement S_{k+1} is true (the next domino also falls). Therefore, if S_1 is knocked over, then the next domino S_2 also falls and knocks over domino S_3 that knocks over domino S_4 and so on. Then we have no other option than to admit that all of the statements are true (all dominoes are knocked over).

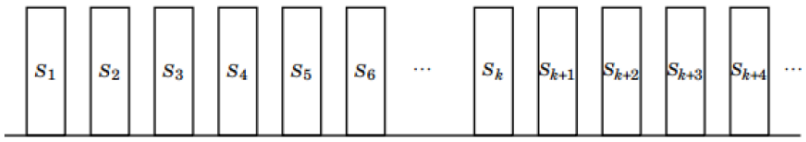


Figure 7.1: Statements are lined up as dominoes.

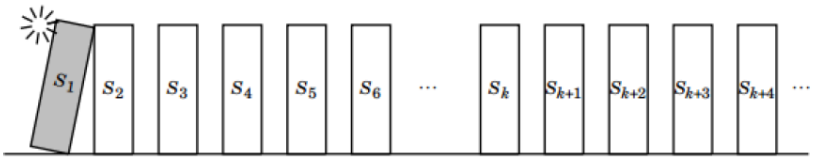


Figure 7.2: Let us assume that the fist statement is proved (first domino is knocked over).

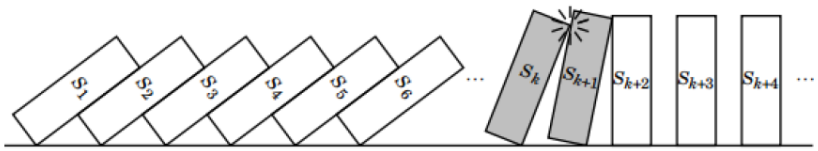


Figure 7.3: Let us assume that the domino S_k always knocks over the domino S_{k+1}.

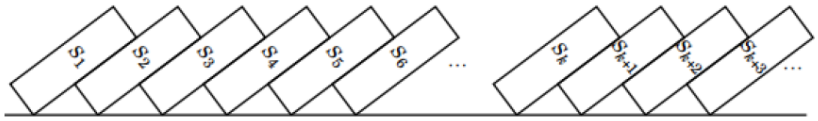


Figure 7.4: All dominoes must fall (i.e. all statements are true).

Now we can see all the steps that are necessary to conduct the method of mathematical induction.

Definition 7.9. Mathematical induction. Let us have a series of statements $S_1, S_2, \ldots, S_n, \ldots$. Every statement S_n of the given series is true if:

1. **Basis step.** S_1 is true, that means the first statement of the series is true;
2. **Inductive step.** $S_k \Rightarrow S_{k+1}$, that means if we assume that statement S_k is true, then we can conclude that the statement S_{k+1} is also true.

Remark.

1. The basis step does not always have to be checking the statement for $n = 1$. If the statement is satisfied for any natural number n, then we can generalize the statement to all the numbers following n.
2. The relations and formulas that are proved by mathematical induction are true only for natural numbers $n = 1, 2, 3, \ldots$.
3. Mathematical induction can be applied only if both steps (basis step and inductive step) are satisfied.

Example 7.10. Prove by mathematical induction that the sum of the first n natural numbers is equal to $\frac{n(n+1)}{2}$, that means

$$1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}, \quad n \geq 1.$$

Proof. We can use mathematical induction, because we are proving the formula for all natural numbers n. Therefore, first we will check if the formula is true for $n = 1$.

1. Basis step. If $n = 1$, then the left-hand side of the formula is $LHS = 1$ and the right-hand side is $RHS = \frac{1(1+1)}{2} = 1$. Therefore, $LHS = RHS$ and the formula is true for $n = 1$.
2. Inductive step. Let us assume that formula is true for $n = k$, that means $1+2+3+\cdots+k = \frac{k(k+1)}{2}$. Now we will check if $1 + 2 + 3 + \cdots + k + k + 1 = \frac{(k+1)(k+2)}{2}$. To prove that we will try to transform the left-hand side to the right-hand side. To do that we will use the assumption that formula is true for k.

$$\begin{aligned} LHS &= \underbrace{1 + 2 + 3 + \cdots + k}_{assumption} + (k+1) = \frac{k(k+1)}{2} + (k+1) \\ &= \frac{k(k+1) + 2(k+1)}{2} = \frac{(k+1)(k+2)}{2} = RHS. \end{aligned}$$

We have shown that the inductive step is satisfied. By uniting the basis step and the inductive step we can conclude that the formula is true for all natural numbers n. □

Let us now prove the statement we made previously about the sum of the first n odd numbers.

Example 7.11. Prove by mathematical induction that the sum of the first n odd numbers is n^2.

Proof.

1. If $n = 1$, then the left-hand side of the equation is $LHS = 1$ and the right-hand side is $RHS = 1^2 = 1$. Therefore, $LHS = RHS$ and formula is true for $n = 1$.

2. Now let us assume that formula is true for $n = k$, that means $1+3+5+\cdots+(2k-1) = k^2$. We will show that the formula is also true for $n = k + 1$, that means $S_k \Rightarrow S_{k+1}$.

$$\begin{aligned} LHS &= \underbrace{1 + 2 + 3 + \cdots + (2k-1)}_{assumption} + (2(k+1)-1) = k^2 + (2(k+1)-1) \\ &= k^2 + 2k + 1 = (k+1)^2 = RHS. \end{aligned}$$

Now we have proved by mathematical induction that the formula is true for all natural numbers n. □

Example 7.12. Prove that $2^{2n} - 1$ is divisible by 3 for all natural numbers n.

Proof.

1. Let us prove that the statement is true for $n = 1$. Since $2^{2\cdot 1} - 1 = 4 - 1 = 3$ is divisible by 3, then the statement is indeed true for $n = 1$.

2. Let us now assume that the statement is true for $n = k$, that means $S_k = 2^{2k} - 1$ is divisible by 3. We will prove that the statement is also true for $n = k + 1$. To do that we will find

$$\begin{aligned} S_{k+1} &= 2^{2(k+1)} - 1 = 2^{2k+2} - 1 = 2^{2k} \cdot 4 - 1 = 2^{2k} \cdot (1+3) - 1 \\ &= 2^{2k} \cdot 1 + 2^{2k} \cdot 3 - 1 = 2^{2k} \cdot 1 - 1 + 2^{2k} \cdot 3 = S_k + 2^{2k} \cdot 3. \end{aligned}$$

   That sum is divisible by 3, because both addends are divisible by 3 (the fist addend S_k is divisible according to the assumption of induction and the second addend $2^{2k} \cdot 3$ has 3 as a coefficient).

Therefore, we have proved by mathematical induction that $2^{2n} - 1$ is divisible by 3 for all natural numbers n. □

Example 7.13. (Sum of the first n members of a geometric progression.) Prove by mathematical induction that if $a, r \in \mathbb{R}$ and $|r| < 1$, then

$$a + ar + ar^2 + ar^3 + \cdots + ar^n = \frac{a(1 - r^{n+1})}{1 - r},\ n \geq 0.$$

Proof. Prove independently. □

Example 7.14. Prove that for every $n \geq 1$:

$$1 + \frac{1}{2} + \cdots + \frac{1}{2^{n-1}} < 2.$$

Proof. We will use the example 7.13 and choose $a = 1$ and $r = \frac{1}{2}$. Then

$$1 + \frac{1}{2} + \cdots + \frac{1}{2^{n-1}} = 1 \cdot \frac{1 - (\frac{1}{2})^n}{1 - \frac{1}{2}} = 2 \cdot \left(1 - \left(\frac{1}{2}\right)^n\right) = 2 - \frac{1}{2^{n-1}} < 2.$$

□

Example 7.15. (The sum of the first n members of an arithmetic progression.) Prove by mathematical induction that

$$\sum_{k=1}^{n}(a + (k-1)d) = \frac{n}{2}(2a + (n-1)d),\ n \geq 1.$$

Proof. Prove independently. □

In the beginning of the chapter we mentioned that mathematical induction can be used only if both conditions (basis step and inductive step) are satisfied. Now we will present some examples of situations, where only one of the conditions is satisfied and we can not use mathematical induction. We will start with an already familiar statement.

Example 7.16. The number $n^2 + n + 41$ is a prime number for all natural numbers n.

Let us start with the basis step and check the statement for $n = 1$: $1^2 + 1 + 41 = 43$, that is indeed a prime number. Furthermore, it turns out that $n^2 + n + 41$ is a prime number for all $n = 1, 2, \ldots, 39$. Next, we will assume that the statement is true for $n = k$, that means $k^2 + k + 41$ is a prime number. We will try to prove that $(k+1)^2 + (k+1) + 41$ is also a prime number. However, we will not succeed. Actually, we already know that when choosing $n = 40$ the number $40^2 + 40 + 41 = 40(40 + 1) + 41 = 41(40 + 1) = 41^2$ is a composite number. That example is a warning not to make generalizations too lightly. The basis step of induction was easy in this example, however, it was impossible to show the inductive step. Therefore, the statement was wrong.

Example 7.17. Prove that every natural number is equal to the natural number following it.

This time we will start by proving the inductive step, since in the last example it was missing and the statement turned out to be not true. Therefore, let us assume that the statement is true for $n = k$, that means some natural number k is equal to the natural number following it, i.e. $k = k + 1$. We will show that the statement is also true for $n = k + 1$. To do so, we will take a look at the left-hand side

$$LHS = \underbrace{k}_{assumption} + 1 = (k+1) + 1 = k + 2 = RHS,$$

and we can see that by using the assumption we get that left-hand and right-hand sides are equal. Therefore, we have proven the inductive step. Now we will try to prove the basis step, that means we try to find an example of a natural number that is equal to the natural number following it. However, it is not possible to find such example, that means there do not exist two consecutive natural numbers that coincide. Therefore, the statement is false.

Next we will bring an example of the wrong use of induction. The author of that example is G. Pólya (1954)

Proposition 7.18. *All horses are the same color.*

„Proof“.

1. **basis step**: Statement is true for $k = 1$, because if there is only one horse in a herd then obviously all horses in that herd are the same color.

2. **Inductive step**: Let us assume that $n = k$ is true, that means in every herd that has k horses, all the horses are the same color. Let us now take a look at the herd that has $k+1$ horses. According to the assumption the first k horses are the same color.

$$\underbrace{h_1, h_2, \ldots, h_k}_{\text{same color}}, h_{k+1}$$

According to the assumption the last k horses are also the same color.

$$h_1, \underbrace{h_2, \ldots, h_k, h_{k+1}}_{\text{same color}}$$

Therefore, all horses $h_1, h_2, \ldots, h_k, h_{k+1}$ must be the same color and $S_k \Rightarrow S_{k+1}$ is true.

According to the mathematical induction all horses are the same color. □

Exercise 7.19. Where is the mistake in the proof of the proposition 7.18?

7.3 Strong induction

Occasionally it happens in induction proofs that it is difficult to show that, if S_k is true, then S_{k+1} is true. Instead you may find that you need to use the fact that some „lower“ statements S_m (with $m < k$) are true in order to show that S_{k+1} is true. For these situations you can use a slight variant of induction called strong induction which is defined as follows.

Definition 7.20. Strong (mathematical) induction. Let there be a series of statements $S_1, S_2, \ldots, S_n, \ldots$. In the given series every statement S_n is true, if

1. **Basis step.** S_1 is true, which means that the first statement of the series is true;

2. **Inductive step.** $S_1 \wedge S_2 \wedge \cdots \wedge S_k \Rightarrow S_{k+1}$, which means that if all statements $S_1, \ldots, S_k$ are true, then we can conclude that the statement S_{k+1} is also true.

Remark. When you check the basis step of strong induction it is sometimes necessary to prove a few more statements in addition to the first statement (see for example proposition 7.25).

The difference from regular induction is that statement S_{k+1} now follows from all previous statements $S_1, \ldots, S_k$, which means we have more information to prove the inductive step. In regular induction we made the assumption that statement S_k is true, from which we show that statement S_{k+1} must be true, now we can assume that all statements $S_1, \ldots, S_k$ are true and we can use those to prove that S_{k+1} is true.

Even though we call this method strong induction, it is still as „strong“ as regular induction. Every statement which we can prove by strong induction can be proven by regular induction.

The only difference is that some proofs can be simplified by using strong induction. Still, if it is possible to prove S_{k+1} from S_k, then we shall use regular induction.

Now we can prove the previously unproven fundamental theorem of arithmetic.

Theorem 7.21 (Fundamental theorem of arithmetic)**.** *Every natural number $n > 1$ can be represented as the product of prime numbers (this means that there exist $r \in \mathbb{N}$ and prime numbers $p_1, \ldots, p_r$ such that $n = p_1 \cdot \cdots \cdot p_r$) and this representation is unique up to the order of the factors.*

Proof. First we prove by strong induction that every natural number $n > 1$ can be represented as the product of prime numbers. For $n = 2$ this is clear (basis step). Assume that $n > 2$ and that every natural number $1 < m < n$ can be represented as the product of prime numbers (inductive hypothesis). Natural number n has to be a prime number or a composite number. In the first case we have nothing to prove. But if n is a composite number, then there exists a natural number $d \mid n$ such that $1 < d < n$. Let $n = da$, where $a \in \mathbb{N}$ and $1 < a < n$. According to the inductive hypothesis we have that d and a can be represented as the products of prime numbers and thus n can also be represented as the product of prime numbers.
To prove the uniqueness we assume that n can be represented as the product of prime numbers in two ways:

$$n = p_1 p_2 \ldots p_r = q_1 q_2 \ldots q_s,$$

where without the loss of generality we assume $r \leq s$ and prime numbers p_i and q_j are in non-decreasing order, this means that $p_1 \leq p_2 \leq \cdots \leq p_r$ and $q_1 \leq q_2 \leq \cdots \leq q_s$. Because $p_1 \mid q_1 q_2 \ldots q_s$ and p_1 is a prime number, we have that $p_1 = q_k$ for some $k \in \{1, \ldots, s\}$. Thus $p_1 \geq q_1$. In similar fashion we get that $q_1 \geq p_1$ and therefore $p_1 = q_1$. By reducing p_1 we get $p_2 \ldots p_r = q_2 \ldots q_s$. By repeating this thought process we get $p_2 = q_2$ and $p_3 \ldots p_r = q_3 \ldots q_s$. If $r < s$ then we end up with $1 = q_{r+1} q_{r+2} \ldots q_s$, which is impossible because $q_i > 1$ for all $i \in \{1, \ldots, s\}$. Thus $r = s$ and $p_1 = q_1, \ldots, p_r = q_r$. □

Example 7.22. Crate stacking game. Assume that in one stack we have n crates on top of each other. In the game you do a number of moves, in which for every move you split one stack of crates into two nonempty stacks. The game ends if every stack has only one crate. For every move you get points. For example, if you split a stack of $a + b$ crates into two stacks, where one has a crates and the other has b crates, then for that move you gain ab points. The final score is the sum of points gained from every move. Which strategy would increase your final score?

Let us play the game with 10 crates. One possible move in this game could be like this:
Are you able to find a better strategy? Let us prove by strong induction that the final score only depends on the number of crates and not the strategy!

Proposition. Whatever way you put n crates into stacks the final score will always be $\frac{n(n-1)}{2}$.

Proof of proposition.

1. Basis step. If $n = 1$, then we only have one crate in a stack. Because it is impossible to perform any moves in this game, then the final score is $\frac{1(1-1)}{2} = 0$. Thus the formula holds for $n = 1$.

Stack height	Points
10	
5 5	25
5 3 2	6
4 3 2 1	4
2 3 2 1 2	4
2 2 2 1 2 1	2
1 2 2 1 2 1 1	1
1 1 2 1 2 1 1 1	1
1 1 1 1 2 1 1 1 1	1
1 1 1 1 1 1 1 1 1 1	1
Final score =	45 points

2. Inductive step. Assume that the statements $S_1, \ldots, S_k$ are all true for a random k. Let us show that then S_{k+1} is also true. Thus let a stack have $k+1$ crates and for our first move let us split it into two stacks of i and $(k+1)-i$ crates (for some i, where $1 \leq i \leq k$). The final score of our game is now the sum of this move's points and every following move's points after it. Thus

$$\begin{aligned}\text{Final score} &= (1.\text{ step points}) + (\text{points for splitting } i \text{ crates}) \\ &\quad + (\text{ points for splitting } k+1-i \text{ crates}) \\ &= i(k+1-i) + \frac{i(i-1)}{2} + \frac{(k+1-i)(k+1-i-1)}{2} \\ &= \frac{k^2+k}{2} = \frac{k(k+1)}{2}.\end{aligned}$$

On the second step we used the fact that based on our assumptions statements S_i and S_{k+1-i} are true and the rest was simplification. Thus we have shown that for any arbitrary k the statements $S_1, \ldots, S_k$ give us statement S_{k+1}, and therefore we have proven our general proposition by strong induction. □

Italian mathematician Leonardo Fibonacci (1175 - 1250), who is recognized as one of most distinguished mathematicians of the Middle Ages, observed the following problem in his writing „Liber abaci“ (1202).

Exercise 7.23. Farmer has one pair of newborn rabbits, male and female. One month after birth the rabbits are able to mate and two months after birth the female rabbit gives birth to a pair of successors. Assume that not a single rabbit dies and that a female rabbit gives birth to a new pair of male and female rabbits every month from the second month on. How many pairs of rabbits will the farmer have on the n-th month?

Let F_n be the number of pairs on the n-th month. Then next month the farmer has all the rabbits which he had on the n-th month, but also as many new pairs as he had rabbits on the $(n-1)$-th month, because next month they are at least two months old and each and every one of them gives birth to a new pair of successors. Thus holds the following formula

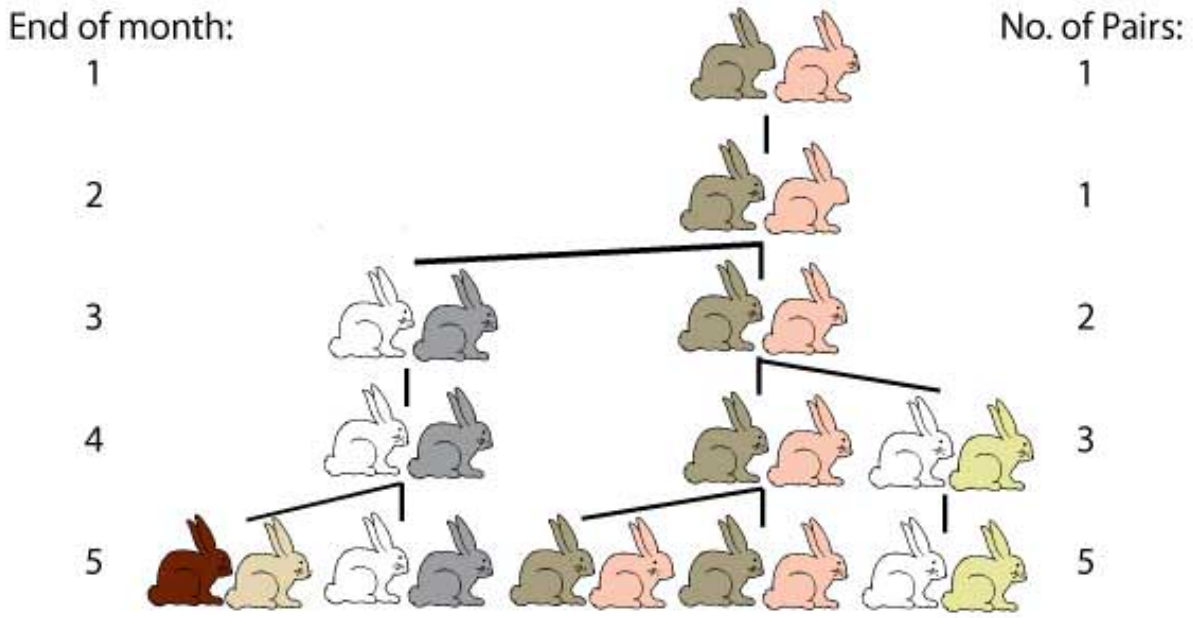


Figure 7.5: https://learnodo-newtonic.com/wp-content/uploads/2015/09/Fibonacci-Sequence-in-the-Rabbit-Problem.jpg

$$F_{n+1} = F_n + F_{n-1}$$

In addition we know that $F_1 = 1, F_2 = 1, F_3 = 2, F_4 = 3, F_5 = 5, \ldots$.
Also it is useful to note $F_0 = 0$.

Definition 7.24. Numbers $F_0, F_1, F_2, \ldots$, where $F_0 = 0$, $F_1 = 1$, and $F_{n+1} = F_n + F_{n-1}$ for every natural number n, are called **Fibonacci numbers**.

Proposition 7.25. *Prove that $F_n > 2n$ for all $n \geq 8$.*

Proof. We prove this propositions by strong induction.

1. Basis step. If $n = 8$, then $F_8 = 21 > 2 \cdot 8 = 16$. If $n = 9$, then $F_9 = 34 > 2 \cdot 9 = 18$. Thus the proposition holds for $n = 8$ and $n = 9$.

2. Inductive step. Assume now that $F_m > 2m$ for all $m \in \{8, \ldots, n\}$. We must show that $F_{n+1} > 2(n+1)$. Because of our assumptions and the connection $F_{n+1} = F_n + F_{n-1}$ we get that
$$F_{n+1} = F_n + F_{n-1} > 2n + 2(n-1) = 4n - 2.$$
Finally we notice that the inequality $4n - 2 > 2n + 2$ is equivalent with the inequality $n > 2$, which obviously holds, because $n \geq 8$.

□

8

Different methods of proof

***

I have had my results for a long time:
but I do not yet know how I am to
arrive at them. – C. F. Gauss

All natural sciences are characterized by the fact that to get results we must observe and experiment. In mathematics we do not observe nor experiment but instead we get results through strict logical discourses, which we call **proofs**.

In mathematics there are a set number of principal concepts and truths which we do not prove. Principal truths which we do not prove and assume to be true, are called **axioms**. The left-over formulae and results are formulated as propositions, which we call theorems. **Theorem** is a proposition, which is proven by strict logical discourse. The mathematical statement in a theorem is proven on the basis of axioms and previously established theorems.

The father of the axiomatic method is said to be **Euclid** (325 – 265 BC), who systematized mathematics of that time in his work „Elements“. Euclid presented an exact and logically consistent system of geometry, which is known as „Euclidean geometry”. The basis of this system are definitions, axioms and postulates (Euclid distinguished between axioms and postulates, today they are all considered axioms) from which he deduced the rest of his theorems. He thought of axioms as evident truths. For a long time (2000 years) mathematicians were engaged with the parallel postulate problem, in which they tried to prove the parallel postulate through other axioms. The parallel axiom claims that **through a point, which is not on a given line, you can only draw one new line, which is parallel with the initial line**. Only in XIX-XX century it was shown that this axiom is independent from the other axioms and thus a new geometry, where one of the axioms denies it, is also correct. Euclidean system stayed until 1820, when the distinguished Russian mathematician **Nikolai Lobachevsky** (1792 – 1856) and a little later the Ukrainian mathematician **János Bolyai** (1802 – 1860) came to the discovery of a new geometry by changing the parallel axiom. The knowledge that you could build up geometry as a mathematical theory, where through a point outside a given straight line you can draw more than one new line, which does not cut the given line, or in which the inner sum of a triangle is less than 180°, was unexpected even for famous mathematician. This new geometry is called **non-Euclidean geometry**. The creation of this kind of geometry showed that axioms can just be understood as assumptions. The search for blanks in Euclid's „Elements“ became one of the most important tasks in the end of the XIX century. This task was finally solved by the year 1900 by German mathematician **David Hilbert** (1862 – 1943).

Gottlob Frege (1848 – 1925) created the most fundamental system of modern logic - first-order predicate calculus, which is based on propositional calculus, predicates and quantifiers. Frege was sure that all of mathematics could be reduced to elementary logic rules, this meant that you should be able to conclude any true mathematical theorem from logic rules. Frege's system and logical views were adopted into their works by 20th century's most influential mathematicians **Bertrand Russell** (1872 – 1970) and **Alfred North Whitehead** (1861 – 1947), who formalized a large part of foundations of mathematics in their work *Principia Mathematica* (1910 – 1913). Russel and Whitehead began deducing mathematics through logic with integer theory also known as arithmetic, in which they took the arithmetic base truths from **Giuseppe Peano** (1858 – 1932) as foundation, from which they hoped to build arithmetic, then calculus, algebra and other branches of mathematics. In the 1930s, unexpectedly to other mathematicians of that time, **Kurt Gödel** (1906 – 1978) proved one of the most famous theorem of logic ever: the **incompleteness theorem**. This theorem shows that you cannot reduce arithmetic to logic, in particular this means that there does not exist a finite set of base assumptions (axioms) from which you can prove all arithmetic theorems. If you cannot axiomatize arithmetic with a finite number of base assumptions, then obviously you cannot do that for any other branches of mathematics. This does not mean that the tools of logic are useless for arithmetic or other difficult areas: as a rule of thumb we only require a small set of basic elementary axioms to prove assumptions that interest us. Gödel's theorem detracted interest from logic, but the invention of electronic computers in middle of the century, and the computerization of the economy, science and society, gave a new powerful push towards the science of logic. The development of mathematics formalization in computers began in the end of 1980s (for example

interactive theorem provers), and many standard theorem libraries have been created for computers. Logic and theoretical computer science have turned mutually dependent on each-other, and are indistinguishable in many concrete areas.

8.1 Inductive and deductive reasoning

In general you can split thinking mechanisms into two groups: generalization and making conclusions.

Inductive reasoning or generalization is when you generalize a property from individual cases. If we only see white swans around us then we tend to believe that all swans in the world are white. If we notice that things we usually come in contact with are usually or always together (fire = hot = pain), then we often generalize this coincidence as a rule. Most rules learned from everyday life may not apply to rare situations, these rules usually have exceptions. Thus, generalization or induction is a thinking process, which does not give us any certain knowledge. Inductive reasoning only gives us something probable, not a proof. This means that the success of generalization is statistical, the more times a rule applies, the better, but do not expect it to always hold. You have to remember that in mathematics you do not prove by experience.
The use of logic rules to get new results is called making conclusions or **deduction** or proving. A large part of rules used in logic are presented in the form of a conclusions: a new conclusion comes from the proof of one or multiple earlier conclusions. In other words, it is thought as impossible that a conclusion of true assumptions is false. Unlike induction this guarantees us that the use of correct rules on correct facts gives us a correct result.

8.2 Proof

Theorems are usually in the shape of „If ..., then ...“ or in a more mathematical form,

$$\forall x \in D, \text{ if } P(x) \text{ is true, then } Q(x) \text{ is also true.}$$

Condition $P(x)$ is the **assumption** and condition $Q(x)$ is the **assertion**. The most powerful method of proof is such that generalizes or, in other words, expands the area where the conclusions are true. We give an arbitrary x, for which the assumption $P(x)$ is true, and, based on definitions, previous results, and rules, we show that $Q(x)$ is true.

Thus, when proving a theorem we:

1. depend on the assumptions;
2. go through a discourse using axioms and previously proven theorems;
3. finally conclude that the theorem is true through logical discussion.

Different mathematical branches are not just simple collections of facts, but instead logical systems. Axioms, definitions and theorems are not given in a random fashion, but are usually masterfully ordered. Every theorem should be put in a place in which its proof is based on earlier

axioms, definitions and theorems. Euclid's „Elements“ was the first and best example of such strict systems of logic, which other sciences tried and are still trying to imitate. Subsequently we look at different methods of proof.

8.3 Direct proof

Most proofs you have come in contact with (if you have even seen or performed them), have been **direct proofs**, in which every next step supports itself on a previously shown step or known fact. A logical debate in the correct order gives us the result at the end.

By using the notations P for assumption and Q for assertion, the goal is to directly show that $P \Rightarrow Q$.

Even though in direct proofs the mathematical methods differ from each other depending on the assertion that we want to prove, the general approach is always the same: start with the information given in the assumptions and through logical debate you reach the assertion you had to prove.

To familiarize ourselves with the general proof notation we look at the following two examples.

Proposition 8.1. *Let m and n be integers. If m and n are even numbers, then so is $m + n$.*

Proof. Let m and n be even numbers. Then we can express them as $m = 2k_1$ and $n = 2k_2$, where k_1 and k_2 are some integers. Their sum $m + n$ can be expressed as $m + n = 2k_1 + 2k_2 = 2(k_1 + k_2) = 2k$. Because $k = k_1 + k_2$ is an integer, then $2k$ is an even number, thus $m + n$ is an even number. □

Proposition 8.2. *Every odd number's square when divided by* 8 *has the remainder* 1*.*

Proof. Let n be an arbitrary odd integer. If n is odd, then there exists k such, that $n = 2k + 1$. Therefore, $n^2 = (2k + 1)^2$ or $n^2 = 4k^2 + 4k + 1$ or $n^2 = 4k(k + 1) + 1$. We know that one of two consecutive integers is always even, then $k(k + 1)$ is definitely an even number. Therefore, $4k(k+1)$ is divisible by 8, and thus we have shown that n^2 when divided by 8 has the remainder 1. □

Some typical mistakes when proving theorems:

- Argumentation with examples. Just because a theorem holds for some example, it does not yet mean that it is generally true.
- The use of same notation for different terms. For example, if in theorem 8.1 we denote two arbitrary even numbers m and n both in the form $m = 2k$ and $n = 2k$, we get an error in our debate from the relation $m = n$, which is not true for two arbitrary integers.
- Jumpy conclusion to result.
- The result itself is used in the proof.

8.4 Proof by subcases

This is a method where the conclusion is proved on all possible cases.

For example, if a theorem asserts something about all integers n, then we can separately observe two different cases: 1) n is an even number and 2) n is an odd number. If a theorem asserts something about all real numbers, then sometimes it can help to observe three cases 1) $x < 0$, 2) $x = 0$ and 3) $x > 0$.

Proposition 8.3. *For every natural number n the number $n^3 + n$ is even.*

Proof. Let us split the set of natural numbers into even and odd numbers so we have two cases for which we prove the assertion.

a) Let n be an even number, which means $n = 2k$, where k is some natural number. Now if we write
$$n^3 + n = (2k)^3 + 2k = 8k^3 + 2k = 2(4k^3 + k) = 2l,$$
we see, that $n^3 + n$ is an even number, because $l = 4k^3 + k$ is a natural number.

b) Now let n be an odd number, thus $n = 2k + 1$, where k is a natural number. Now if we write
$$n^3 + n = (2k+1)^3 + (2k+1) = 8k^3 + 12k^2 + 6k + 1 + 2k + 1 = 2(4k^3 + 6k^2 + 4k + 1) = 2l,$$
we see, that $n^3 + n$ is an even number, because $l = 4k^3 + 6k^2 + 4k + 1$ is a natural number.

□

For the next result we shall recall the definition of the absolute value for real numbers. The **absolute value** of real number x is
$$|x| := \begin{cases} x, & \text{if } x \geq 0; \\ -x, & \text{if } x < 0. \end{cases}$$
Sometimes it is useful to define the absolute value of a real number x as $|x| = \max\{x, -x\}$. Make sure that both definitions are equivalent.

Proposition 8.4. *For arbitrary real numbers x and y the inequality $|x + y| \leq |x| + |y|$ holds.*

Proof. For this proof we observe four cases.

a) Let $x \geq 0$ and $y \geq 0$. Thus $x + y \geq 0$ and based on the absolute value's definition $|x + y| = x + y = |x| + |y|$.

b) Let $x \geq 0$ and $y < 0$. In this case we get two additional subcases.

   (i) If $x + y \geq 0$, then $|x + y| = x + y < x + 0 < |x| + |y|$.

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

c) If $x < 0$ and $y \geq 0$. This case's proof is analogous to case b). Try to write it down yourself!

d) If $x < 0$ and $y < 0$. Then based on the absolute value's definition $|x + y| = -(x + y) = (-x) + (-y) = |x| + |y|$.

□

8.5 Proof by contraposition

Sometimes it is difficult to show directly that Q follows from P, or in short, $P \Rightarrow Q$. We know that $P \Rightarrow Q$ is logically equivalent to its contrapositive $\neg Q \Rightarrow \neg P$. Thus we instead show that $\neg Q \Rightarrow \neg P$.

Proposition 8.5. *Let n be an integer. If n^2 is an odd integer, then n is also an odd integer.*

Proof. We prove this proposition's contrapositive: If n is an even integer, then n^2 is also an even integer. Indeed, if n is even, then there exists an integer $k \in \mathbb{Z}$ such that $n = 2k$. Therefore, we have $n^2 = (2k)^2 = 4k^2$, which is always an even number. □

8.6 Proof by contradiction

Often we find, that a direct proof is not possible due to scarceness of details, or the aim is to prove a „negative“ result, which means, that we want to show some property is not true or some element does not exist, and so on. In this case in mathematics we prove by contradiction, which is based on the logic rule: for every assertion either the assertion is true or its antithesis is true, there is no third option.

Proof by contradiction or argument to absurdity (Latin for *reductio ad absurdum*) is an indirect method of proving, in which we assume the assertion is false (or the antithesis is true), and thus we make conclusions from this assertion. This proof is a success if we reach a contradiction with either the theorem's assumptions or some well-known truth. Therefore we assert, that our antithesis cannot be true, thus only the assertion itself can be true.

Proof by contradiction is often used when it is necessary to show that an object with a specific quality does not exist, or a specific object does not have a specific quality. Therefore, if the initial assertion denies something, then we can start the double negation with a better fitting assumption. Thus, proof by contradiction requires us to know how to negate propositions.

Usually, when proving a theorem we start from the assumptions and get to the assertions trueness through logical discussion, but proof by contradiction has us do all that in reverse.

Proof by contradiction has us:

1. start from the assertion and assume, that the demonstrable assertion is false;
2. go through a discussion in which we use axioms and previously proven theorems if necessary;
3. see as the result of discussion, that denying the assertion is impossible, because this leads us to a contradiction with the theorem's assumption or known truths;
4. summarize, that the assertion is true because the assertion's negation cannot be true.

Proposition 8.6. *If on a plane two lines a and b are parallel to a third line c, then those lines a and b are parallel to each-other.*

Assumption. $a \parallel c$ and $b \parallel c$.
Assertion. $a \parallel b$.

Proof. (By contradiction). Deny the claim and thus assume that a and b are not parallel. From this assumption we get that these two lines have to intersect at a point P, because on a plain there is no third option for two straight lines. Therefore, due to our assumption, two lines go through point P, which means that due to our assertion they both are parallel to c. This contradicts the parallel postulate, which claims that for a point outside a given straight line only one straight line goes through it which is parallel to the given line. Thus lines a and b cannot intersect. Therefore, $a \parallel b$ is true because there is no third option. □

Proposition 8.7. *The set of natural number has no largest element.*

Proposition. We observe the set of natural numbers.
Assertion. This set has no largest element.

Proof. Proof by contradiction. Assume, that the theorem's assertion does not hold and thus there exists a natural number N, which is larger than all the other natural numbers. According to the axiom for every natural number n the number $n+1$ is also a natural number. Thus $n+1$ is larger than n. Thus for N there exists the natural number $N+1$, which is larger. This is in contradiction with our assumption, in which N is the largest natural number. Therefore, it is impossible for there to be a largest natural number. □

Proposition 8.8. *For every real number $x \in [0, \pi/2]$ holds $\sin x + \cos x \geq 1$.*

Proof. Let us assume the opposite, let there be some real number $y \in [0, \pi/2]$ such, that $\sin y + \cos y < 1$. Because $y \in [0, \pi/2]$, then $\sin y \geq 0$ and $\cos y \geq 0$. Therefore, from $0 \leq \sin y + \cos y < 1$, we get that $0^2 \leq (\sin y + \cos y)^2 < 1^2$ or $0 \leq \sin^2 y + 2 \sin y \cos y + \cos^2 y < 1$. Thus $2 \sin y \cos y < 0$, which contradicts $\sin y \geq 0$ and $\cos y \geq 0$. □

We often prove by contradiction claims related to rational numbers. Remind yourself, that a **rational number** is a real number r, which can be expressed in the form $r = \frac{m}{n}$, where m and n are integers and $n \neq 0$. For example, $\frac{1}{3}$, $-7\frac{2}{5}$ and 0 are rational numbers. A real number which we cannot write as a relation between two integers is called an **irrational number**. If we denote real numbers as $\mathbb{R}$ and rational numbers as $\mathbb{Q}$, then we mark irrational numbers as $\mathbb{I}$, where $\mathbb{I} = \mathbb{R} \setminus \mathbb{Q}$. With some effort you should be able to prove that $\sqrt{7}$, π and e^2 are all irrational numbers.

Proposition 8.9. *Real number $\sqrt{2}$ is irrational.*

Proof. Let us assume the opposite, $\sqrt{2}$ is a rational number. Therefore, there exist integers r and $s \neq 0$ such, that $\sqrt{2} = \frac{r}{s}$. Without loss of generality, assume that $\frac{r}{s}$ is an irreducible fraction. By taking the square of this we get $2 = \frac{r^2}{s^2}$, from which $2s^2 = r^2$. Therefore, the number r^2 is even, and thus r is an even number. Therefore, there exists an integer k such, that $r = 2k$. Now we can write the equality $2s^2 = r^2$ as $2s^2 = 4k^2$, and thus s is an even number. Now because s and r are both even numbers, they both are a multiple of 2, which contradicts with our assumption, that $\frac{r}{s}$ is an irreducible fraction. Therefore, $\sqrt{2}$ is an irrational number.
□

Proposition 8.10. *If a positive real number x is irrational, then $\sqrt{x}$ is also an irrational number.*

Proof. Let us assume the opposite, that the assertion „If a positive real number x is irrational, then $\sqrt{x}$ is also an irrational number“ does not hold. This means that we assume that x is an irrational number and $\sqrt{x}$ is a rational number. Now that $\sqrt{x}$ is a rational number, there exist integers a and b, $b \neq 0$, such, that $\sqrt{x} = \frac{a}{b}$. Therefore, $x = (\sqrt{x})^2 = \left(\frac{a}{b}\right)^2 = \frac{a^2}{b^2}$. We now have, that x is a rational number, which contradicts our claim, that x is irrational. Thus our initial assertion must be true: „If a positive real number x is irrational, then $\sqrt{x}$ is also an irrational number“. □

Theorem 8.11. *If α is an irrational number, then 3α is also an irrational number.*

Proof. This assertion is possible to be formulated negatively, which means we want to show that 3α is not a rational number. Therefore, we assume the opposite, that 3α is actually a rational number. Now we can write $3\alpha = \frac{m}{n}$, where m and n are integers and $n \neq 0$. By dividing both sides by 3, we now have $\alpha = \frac{m}{3n}$, thus both denominator and numerator are integers. We have shown that α in this case is a rational number, which goes against our initial assumption, that α is irrational. Therefore our assumption, that 3α is a rational number, does not hold and thus 3α must be irrational. □

Example 8.12. All positive integers are interesting. :)

"Reasoning". Let us assume the opposite, that there exist uninteresting numbers. This means that the set of uninteresting numbers is not empty. Now because of Zermelo's theorem (theorem **??**) we know, that this set is able to be totally ordered, and thus we can find the smallest uninteresting positive integer. But this is really interesting, what kind of a number is that!? The first uninteresting number?... Very interesting! Thus we have our contradiction. □

8.7 Proofs of equivalence

Let us begin with two equivalent claims, which in logic we denote as $A \Leftrightarrow B$ and which we read as „A if and only if B“ or „condition A is a necessary and sufficient for condition B“ or „condition A is equivalent to condition B“. In the propositional calculus chapter we showed, that expression $A \Leftrightarrow B$ is logically equivalent with the expression $(A \Rightarrow B) \wedge (B \Rightarrow A)$. The last notation gives us a strategy on how to prove such theorems.

To prove that the claims A and B are the same (equivalent), we need to show, that they both follow the other. Therefore, to prove theorem „A if and only if B“, we have to show that $A \Rightarrow B$ and then show $B \Rightarrow A$, where for both cases we use the best fitting method of proof.

Proposition 8.13. *Let a and b be integers. The product ab is an even number if and only if at least one of the numbers a or b is even.*

Discussion. Because the theorem contains the phrase „... if and only if ...“, we now have to prove two implications. First we have to show 1) if ab is an even number, then at least one of the numbers a or b is even, and then the opposite, which is 2) if at least one of the two numbers

a or b is even, then ab is an even number. Without the loss of generality assume that a is an even number. We could prove our theorem through subcases, where first a is even and then b is even, but these proofs are both exactly the same and thus we can choose just one of the numbers and assume that it is even. Secondly we notice, that if we were to use a direct proof, then we would start with the assumption, that $ab = 2k$, where k is some integer. But continuing like that would make it very difficult to say something about numbers a and b separately. Therefore, the first implication requires a different method of proof.

Proof of proposition 8.13.
1) $\Rightarrow$ 2). We prove this implication by contradiction. For this, let us assume, that ab is an even number, but both numbers a and b are odd. Therefore, we can write $a = 2m+1$ and $b = 2n+1$, where m and n are integers. Thus

$$ab = (2m + 1)(2n + 1) = 4mn + 2m + 2n + 1 = 2(2mn + m + n) + 1.$$

Now because $2mn + m + n$ is an integer, we have shown, that ab is an odd number, which gives us a contradiction with our assumption, where ab had to be an even number.
2) $\Rightarrow$ 1). For the opposite implication we assume that either a or b is an even number. Without loss of generality let us assume, that a is an even number i.e., $a = 2k$, where k is an integer. Now $ab = (2k)b = 2(kb)$ and because kb is an integer, we have shown, that ab is even. □

Proposition 8.14. *Let x and y be real numbers. Thus $x^2 = y^2$ if and only if $|x| = |y|$.*

Proof. Independently! □

8.8 Proof of multiple equivalent conditions

Often in theorems we have more than two equivalent conditions and generally such theorem's formulation may look like this:

Theorem (...assumptions...)**.** *The following conditions are equivalent:*

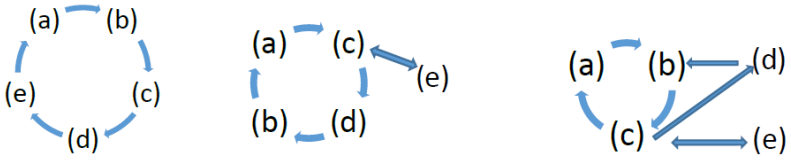
(a)

(b)

(c)

...

In these theorems we usually have three or more conditions (there is no upper bound) and the objective is to show that all these conditions are equivalent. Equivalency in this case means, that if one of the conditions is true, then all other conditions are also true, and if one is false, then due to equivalency the others are false too. If there are three equivalent conditions, then we will have to perform three proofs by equivalency („... if and only if..." type), whereby they would be $(a) \Leftrightarrow (b)$, $(b) \Leftrightarrow (c)$ and $(a) \Leftrightarrow (c)$. If there are four conditions, then we will have to perform 6 proofs by equivalency, and in general, for n equivalent conditions we would have to perform $\frac{n(n-1)}{2}$ proofs by equivalency. Luckily for us, we do not have to perform this many proofs by



equivalency. The next graph gives us three possible ways to plan the proof of a theorem with five equivalent conditions. One sided arrows stand for the corresponding implications and two sided arrows denote proofs by equivalency.

Theorem 8.15. *Let n be an integer. The following conditions are equivalent:*

(a) n is an even number

(b) $n+1$ is an odd number

(c) n^2 is an even number

Proof. Independently! □

8.9 Proof of existence and uniqueness

Let us take a look at methods of proof for theorems that have the form „ $\exists x$, for which $P(x)$“. These theorems guarantee us, that there exists at least one such x, for which condition (property) $P(x)$ is true. This is called a **proof of existence**.

Proofs of existence can be split into two categories: constructive and nonconstructive.

Constructive proof of existence. For a constructive proof of existence we try to construct the element x directly by our own or construct an algorithm to find such x with the help of a computer.

Example 8.16. Prove, that there exists an integer such that its square is 81.

Reasoning. The matching integer is 9, because $9 \cdot 9 = 81$. □

Example 8.17. Prove, that there exists a formula of propositional calculus, from which you can conclude the same formula's negation.

Reasoning. Let us take a look at the formula $X \wedge \neg X$. From the truth table we get that $X \wedge \neg X \Rightarrow \neg(X \wedge \neg X)$ is a tautology (Check!). Therefore, from the formula $X \wedge \neg X$ follows formula $\neg(X \wedge \neg X)$. This means, that the formula $X \wedge \neg X$ has the necessary property. □

Example 8.18. Show, that there exist real numbers a and b such, that $(a+b)^2 = a^2 + b^2$.

Reasoning. Even though the given relation is generally untrue, we are still able to find pairs of numbers, which satisfy this condition. Let $a, b \in \mathbb{R}$ be such, that $(a+b)^2 = a^2+2ab+b^2 = a^2+b^2$. Then $2ab = 0$. One possible solution is $a = 1$ and $b = 0$, because then $(a+b)^2 = (1+0)^2 = 1^2 = 1^2 + 0^2 = a^2 + b^2$. □

Example 8.19. From school mathematics we know that for positive real numbers x and y the following inequality is generally true: $\frac{1}{2}(x+y) \geq \sqrt{xy}$. Is it possible to find such real numbers x and y, for which $\frac{1}{2}(x+y) \leq \sqrt{xy}$?

Reasoning. Choose $x = y = 5$. Therefore, $\frac{1}{2}(x+y) = 5 = \sqrt{xy}$. The best that we could do here is to equal the two expressions, because the inequality $\frac{1}{2}(x+y) < \sqrt{xy}$ does not hold for a single pair of numbers. □

Nonconstructive proof of existence. It is possible, that based on existing results we can prove the existence of a object through logical discussion without having to find the object directly. For example, you should be familiar with a theorem which claims, that every polynomial of an odd degree with real coefficients has at least one real solution. This knowledge will not help you find this solution for every such polynomial. David Hilbert used the next example to demonstrate the idea of proof of existence:

In this class there is at least one student, let their name be 'X', who matches the next claim: No other student in this class has more hair on their head than X. Who is this student? This we will never know, but we can be absolutely sure of their existence.

Proposition 8.20. *There exist irrational numbers x and y such, that x^y is a rational number.*

Proof. We know, that $\sqrt{2}$ is an irrational number. Observe the number $(\sqrt{2})^{\sqrt{2}}$. Now let us take a look at two cases:

1. If $(\sqrt{2})^{\sqrt{2}}$ is a rational number, then we have proven our assertion.
2. If $(\sqrt{2})^{\sqrt{2}}$ is an irrational number, then

$$((\sqrt{2})^{\sqrt{2}})^{\sqrt{2}} = (\sqrt{2})^{\sqrt{2}\cdot\sqrt{2}} = (\sqrt{2})^2 = 2$$

Therefore, there exist irrational numbers x and y such, that x^y is a rational number. □

In your future math studies you will often encounter theorems, which claim, that there exists **one and only one** element with certain properties. The proofs of such theorems always start with the negation of the assertion, this means we assume, that there exist two elements, say x and y, with the requested properties. Through logical discourse, our aim is to prove that $x = y$.

Example 8.21. If k and b are real numbers and $k \neq 0$, then there exists one and only one x, which satisfies the equation $kx + b = 0$.

Reasoning. Let us claim in opposition to our assertion, that there exist two unequal real numbers x_1 andx_2, which both satisfy the given equation, this means $kx_1 + b = 0$ and $kx_2 + b = 0$. Now if we are to equal these two equations we have $kx_1 + b = kx_2 + b$, which, after subtracting b from both sides, gives us $kx_1 = kx_2$. Now dividing both sides by k gives us, that $x_1 = x_2$, because $k \neq 0$. We now have a contradiction with our assumption, which claims that $x_1 \neq x_2$. Therefore, there cannot exist two different solutions and there can only be one. □

Mathematicians, who are interested in relations and regularities, often tend to search for objects with certain qualities, be it because of interest or necessity. For example, they may ask if there exist integers a, b and c such, that $a + b + c = 3$ and $a^3 + b^3 + c^3 = 3$, in addition to the trivial solution $a = b = c = 1$? Or, if on a plain there are two arbitrary rectangles, does there exist a straight line, which divides both their areas into half? Turns out you can answer positively to both of these questions. Are you able to find the solutions?

A superficial observation makes it seem, that proofs of existence are easier to perform than other proofs. For a constructive proof we only have to find one object with the necessary property, we are not required to prove, that some property applies to all elements of a set. However, it is often incredibly difficult to find this one object. Centuries ago Euler hypothesized, that the sum of three complete fourth power numbers is never equal to some other number's fourth power. In 1986 (the age of computers!) Noam Elkies proved that Euler's statement is wrong. He showed, that

$$2682440^4 + 15365639^4 + 18796760^4 = 20615673^4.$$

8.10 Presumptions or hypotheses

One of the most exciting things you can do in math is to search for and discover new things. This is something that is not easy to do and it is even harder to give exact directions on how such process should even take place. Finding connections and patterns is a form of art, in the same vein as asking productive questions. By taking a look at the following sequence of full squares

$$0, 1, 4, 9, 16, 25, 36, 49, 64, 81, 100, 121, 144, 169, 196, 225, 256, 289, 324, 361, 400$$

we begin to notice some nice connections between these numbers. For example, we notice that the sum of two full squares is always a full square, like $64 + 225 = 289$. Now we could ask, is the sum of two full squares equal to the sum of some other two full squares? What happens if you were to multiply a full square by 2?

Turns out that this number on its own is never a full square, but it can be extremely close to a full square, for example $2 \cdot 25 = 50 = 49 + 1$ or $2 \cdot 144 = 288 = 289 - 1$. Let us present this as a table to make it easier to find connections and patterns.
In the table we notice quite a few nice connections. For example, by adding up the values of m and n in every row, we get the value m in the next row. Now try to make three presumptions on your own about different connections and patterns in the table. Based on your presumptions

$2m^2 = n^2 \pm 1$	m	n
$2 \cdot 1 = 1 + 1$	1	1
$2 \cdot 4 = 9 - 1$	2	3
$2 \cdot 25 = 49 + 1$	5	7
$2 \cdot 144 = 289 - 1$	12	17
$2 \cdot 841 = 1681 + 1$	29	41

try to find the values of the next two rows and then check if your presumptions hold.

Note, that our interesting research started by just simply squaring numbers, but then we asked the questions „what happens if we were to multiply our full squares by two“, and then we picked out a set of presumptions from our well organized table. These steps and actions describe pretty well how new discoveries are made.

Intriguing presumptions catch the interest of many mathematicians and usually these presumptions quickly find a proof or a counterexample. Sometimes it happens that some presumptions stay without proof for years until a newer and more powerful method or a really genius idea is able to solve them. One such example generalizes our number squaring idea and claims, that there exist integers a, b and c such, that $a^2 + b^2 = c^2$. Let us ask the following intriguing question: does a similar connection between numbers a, b and c exist for higher powers? This means, we want to know, if there exist integers a, b and c such, that $a^3 + b^3 = c^3$ or $a^4 + b^4 = c^4$, and so on? In 1637 **Pierre de Fermat'** made the claim, that for powers greater than 2 this connection does not hold, but he was only able to prove this for the power of four. More than a century later **Euler** showed, that this connection does not hold for cubes. Afterwards, it took until 1990, when **Wiles** with other mathematicians proved „Fermat's last theorem“ by showing that the presumption holds for all powers of integer order.

Another famous hypothesis was the **four color problem** presented by **Francis Guthrie** in 1852, which asked if it was possible to paint the world map in four colors in such a way, that all the neighbouring countries would be in different colors. Guthrie himself tried to paint England. Many of that period's famous mathematicians were engaged with this problem and hypothesized that it was possible. The proof itself came in 1976 from **Kenneth Appel** and **Wolfgang Haken** with the help of computers. Therefore, this hypothesis has been proven and it has become a theorem.

8.11 Disproving and counterexamples

Often it happens that our presumption is wrong. If this wrong presumption claims something about all the elements of a set or a class, then it is only necessary to find one example, for which the result does not hold. Therefore, we have to find a counterexample.

Example 8.22. Prove, that the following statement is false:

$$\forall a, b \in \mathbb{R} \text{ if } a < b, \text{ then } a^2 < b^2.$$

Reasoning. It is sufficient to only find one pair of numbers a and b, for which the assertion does not hold. For this we choose $a = -2$ and $b = -1$. Then $a < b$, because $-2 < -1$, but $a^2 > b^2$, because $(-2)^2 > (-1)^2$. With this the assertion is disproven. □

Example 8.23. Prove, that the following assertion is false:

$$\text{If } \alpha \text{ is a real number, then } \tan^2 \alpha + 1 = \frac{1}{\cos^2 \alpha}.$$

Reasoning. Because $\tan \alpha$ and $\frac{1}{\cos \alpha}$ do not exist when $\alpha = \frac{\pi}{2}$, our assertion can not hold for every real number. The value $\alpha = \frac{\pi}{2}$ serves as the counterexample for our expression. □

8.12 Why teach proofs?

The following story is told of Newton. As a young student he started learning geometry from reading Euclid's „Elements“ (which was the norm at that time). He read the theorems, and saw, that they were true and skipped their proofs. At the same time he wondered, as to why someone would spend so much time to prove such elementary things. Many years later he changed his stance and praised Euclid very much.

Why do we need to learn or teach proofs? The first typical answer to this is that proofs are a central part of mathematics and thus it is not possible to skip them when learning or teaching mathematics. Why in the first place do mathematicians prove their results and investigate their colleagues' works? One reason is to validate the results – a proof convinces us on the validity of the proposition, this means that it answers the question, „Is this true?“. For a mathematician this is not the only or the most important question. Even professional mathematicians are ready to believe propositions presented in smart books or scientific literature without proofs. So why do they investigate their colleagues' proofs? The most important reason is clarification – a proof gives us a good understanding of the proposition's essence, answers the question, „Why is this proposition true?“. Mathematicians themselves are most interested in this and the question „Why?“, not if something is true or false. On top of that a proof can help systematize, it binds knowledge into a complete deductive chain of discussion, passing on intuitively understood truths. Often through this function we see the beauty of mathematics and the connections that hold there.

8.13 Tips for writing proofs

Writing a good proof assumes practice and the ability to follow guidelines. You have to learn the in effect practices, use symbols and notations correctly, get used to new vocabulary, practice different proving methods, be more strict and exacting towards yourself, etc. All this is possible if you want to.

The backbone of every proof is a „waterproof“ argument. Because the mathematical methods to achieve this goal depend on the given problem, we discuss the strict proof of every case separately. Still it is possible for us to say something about the richness of details in a proof. A

general rule of thumb is, that you should only use the necessary amount of detail and explanation for every step of your proof, but do not overdo with detail, otherwise it becomes hard for the reader to pay attention to. Writing a proof is just like writing a poem, a good poet can express everything he wants to with as few words as possible.

There are many possible choices for writing shorter proofs. One sure way is knowledge of mathematical symbols and language. Instead of writing „Let x be the element of set A_1 or A_2 or A_3, and do not let it be such, that $x = 0$ is true“ we can instead write „Let $x \in (A_1 \cup A_2 \cup A_3) \setminus \{0\}$“. There is the possibility of the other extremity, where you write too little, but beginner mathematicians just like yourself usually do not encounter this sort of a problem. If possible, try to build your proof from already existing results, instead of proving those results again in your work. Also, if in your proof a similar argumentation is used in multiple parts, then it is not necessary to repeat all details. Just write „Similarly to the previous case...“ or „Similarly we can claim, that...“. Finally, to put a nice proof on paper you must be able to think it through well mathematically. Beautiful mathematical results deserve beautifully presented proofs.

Some additional tips to attain good style:

1. Split your proof into paragraphs of suitable length. It is not necessary for you to repeat what you are about to prove in the beginning of your proof, but if you do that, then it does make your proof more readable. Your formulation has to clearly express, that the assertion requires a proof, for example you can write „We need to show, that $A \cap B \subset A \cup B$“, instead of just saying „For sets A and B holds true $A \cap B \subset A \cup B$“, as if it was already proven. It is a good idea for the next sentence to always give an idea of what kind of strategy you are going to use to prove your assertion, for example „We show that if $x \in A \cap B$, then $x \in A \cup B$.“

2. Use synonyms to enrich your mathematical written language. For example, instead of writing 'prove' you can use 'show', 'explain', 'argument', etc. It also helps if you have alternatives for 'thus'. Possible synonyms could be 'therefore', 'hence', 'because of this', 'this means', etc.

3. In mathematical texts we use 'we' instead of 'I'. This is because reading mathematical texts should be an active action and not a passive one, thus by using 'we' the author tries to attract the reader to take part in the making of the proof.

4. Do not start sentences with symbols or formulae. Write „Equation $x^2 + 2x - 2 = 0$ is important, because ...“, instead of writing „$x^2 + 2x - 2 = 0$ is important, because ...“. Similarly write „We know, that n is not a prime number, because n is an even number and $n \geq 4$“ instead of writing „n is not a prime number, because n is an even number and $n \geq 4$“.

5. Especially important mathematical formulae in proofs should be written on a new row for them to attain more attention and understanding from the reader. For example, write the next expression on its own row

$$\bigcap_{r \in J} B_r = \{x \mid -1 < x \leq 0\}$$

instead of hiding it in the text.

6. At the end of your proof you can write closing lines such as „. . . , *like we wished to show*“, „. . . , *which was our purpose*“ or simply „*With this we end our proof.* “ Traditionally mathematicians leave a symbol at the end of a proof to visually separate the proof from the rest of the text and further discussion. The most popular symbols are 'QED' (Latin for *quod erat demonstratum* or '*what was to be demonstrated*'), a filled ■ or unfilled □ square.

9

Functions

***

The only way to learn mathematics is
to do mathematics – P. Halmos

The concept of functions plays a fundamental role in mathematics. For a long time functions were mainly researched in calculus and were defined either on the set of real or complex numbers, and were able to be presented through some expression (created from elementary functions). Researched were functions' continuity, differentiability, integrability, etc.

Functions of one variable are for example $f(x) = 6$, $g(x) = 3x$, $h(x) = x^2$, $k(x) = \sin x$, $l(x) = e^x$, $m(x) = \ln x$. Arithmetic operations and exponentiation on the set of real numbers gives us five two variable functions $x + y, x - y, x \cdot y, x : y$ and x^y.

Sometimes in calculus books even now mathematicians write, that „A function is a rule, which for every element of set X assigns an element of set Y". An informatics student might see that this rule is actually an algorithm (program), which allows us to find the value of a function on a specific argument. For functions in the form of expressions these algorithms do exist, but in mathematics we also observe more general cases, where we cannot express a function through elementary functions nor exists there a calculation algorithm. The theorems of calculus do not

assume the existence of such rules, because the proofs of these theorems do not require them. The only assumption is that the function has a value for every argument.

9.1 Definition

Definition 9.1. Let X and Y be sets. If there is given a rule, which associates every element of X to a single element Y, then we say, that there is defined a **function** f, and we write $f\colon X \to Y$. If element $x \in X$ is associated with element $y \in Y$, then we use the notation $y = f(x)$ or $y = fx$ or $f\colon x \mapsto y$.

Set X is called the **initial set** or **domain** of function f and set Y is called the **target set** or **codomain** of function f. Set $f(X) = \{f(x)\colon x \in X\}$ is called the **image** or **range** of function f. For more abstracts sets we say operator or map instead of function. The map $f\colon X \to X$ is called the **transformation** of set X.
Let us take a look at some examples of functions.

Example 9.2.

1. From elementary mathematics we are familiar with the linear function $y = ax + b$ $(a \neq 0)$, the quadratic function $y = ax^2 + bx + c$ $(a \neq 0)$ and the trigonometric functions $y = \sin x$ and $y = \cos x$, which are all functions from the set of real numbers to the set of real numbers: $f\colon \mathbb{R} \to \mathbb{R}$.

2. **Constant function** $f(x) = c$ assigns every element x of set X to a specific element $c \in Y$.

3. **Similarity** or **identity function** is the function $f\colon X \to X$, where $f(x) = x$ for all $x \in X$.

4. Let function $f\colon \mathbb{R}^2 \to \mathbb{R}^2$ be defined by the expression $f((x, y)) = (x, 0)$ for all $(x, y) \in \mathbb{R}^2$, this means f assigns a point $P(x, y)$ on the real plane to its first coordinate on the x-axis. This is called a **projection** onto the x-axis. Analogically we can define the projection onto the y-axis.

5. Let $X \neq \emptyset$ set. A bijective function $s\colon X \to X$ is called a **substitution** on set X. Now let X be finite. For easier understanding, let us assume that X only has the first n natural numbers, this means $X = \{1, 2, \ldots, n\}$. A substitution s is usually represented as the following table:
$$s = \begin{pmatrix} 1 & 2 & \ldots & n \\ s(1) & s(2) & \ldots & s(n) \end{pmatrix},$$
where in the first row we have the elements of X and below every element you have its image by substitution s. For example, a possible substitution is
$$s = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}.$$

6. The **floor** function $\lfloor x \rfloor\colon \mathbb{R} \to \mathbb{Z}$ assigns the greatest integer that is less than or equal to a real number x, and, the **ceiling** function $\lceil x \rceil\colon \mathbb{R} \to \mathbb{Z}$ assigns the smallest integer greater or equal to a real number x, or, in short,
$$\lfloor x \rfloor = \max\{m \in \mathbb{Z}\colon m \leq x\} \quad \text{ja} \quad \lceil x \rceil = \min\{n \in \mathbb{Z}\colon x \leq n\}.$$

7. A sequence of real numbers $a_1, a_2, a_3, \ldots$ can be viewed as the function $f\colon \mathbb{N} \to \mathbb{R}$, where for every natural number corresponds a real number, this means that $a_i = f(i)$ for all $i \in \mathbb{N}$.

Example 9.3. Let U be a universal set.

1. We can define a function $f\colon \mathcal{P}(U) \to \mathcal{P}(U)$ by
$$f(A) = A' \quad \text{for all } A \in \mathcal{P}(U).$$
2. We can define a function $f\colon \mathcal{P}(U) \times \mathcal{P}(U) \to \mathcal{P}(U)$ by
$$f((A, B)) = A \cap B \quad \text{for all } (A, B) \in \mathcal{P}(U) \times \mathcal{P}(U).$$

Definition 9.4. Functions $f\colon X \to Y$ and $g\colon Z \to W$ are said to be **equal**, if $X = Z$, $Y = W$ and $f(x) = g(x)$ for all $x \in X(= Z)$.

Therefore, for example the functions $\sin\colon \mathbb{R} \to \mathbb{R}$, $\sin\colon [-\pi, \pi] \to \mathbb{R}$ and $\sin\colon \mathbb{R} \to [-1, 1]$ are all different from each other.

Definition 9.5. Let $f\colon X \to Y$ be a function. The set
$$G(f) = \{(x, f(x)) \mid x \in X\} \subset X \times Y$$
is called the **graph** of function f.

Exercise 9.6. Let $f_1, f_2\colon X \to Y$ be functions. Prove, that $f_1 = f_2$ if and only if $G(f_1) = G(f_2)$.

9.2 Characteristic function

Definition 9.7. Let U be a universal set and let $A \subset U$. The **characteristic function** of set A is the function $\chi_A\colon U \to \{0, 1\}$, where
$$\chi_A(x) = \begin{cases} 1, & \text{if } x \in A \\ 0, & \text{if } x \in U \setminus A. \end{cases}$$

The value of characteristic function $\chi_A(x)$ tells us whether an element $x \in U$ is in the set A or not. Therefore, every subset $A \subset U$ has its own characteristic function. Different sets have different functions, this means that the correspondence is injective. But is such a correspondence surjective? To check this let us take a function $\chi\colon U \to \{0, 1\}$ and observe the set $A = \{x \in U\colon \chi(x) = 1\}$. Now, if $x \in A$, then $\chi(x) = 1$, but if $x \in U \setminus A$, then $\chi(x) = 0$, and therefore $\chi = \chi_A$. Thus we have shown, that the observable correspondence between sets $A \subset U$ and functions $\chi_A\colon U \to \{0, 1\}$ is a bijection.

It is clear that for a fixed universal set U two subsets A and B of it are equal if and only if they have the same characteristic functions, this means that
$$A = B \Leftrightarrow \chi_A(x) = \chi_B(x), \quad \forall x \in U.$$

Therefore, for equal sets the characteristic functions are identical. Different sets have to differ by at least one element and thus on that element the values of characteristic functions are different.

Example 9.8.

1. The value of the characteristic function of empty set is always 0 and the value of the characteristic function of universal set U is always 1;
2. If the universal set is the set of natural numbers $\mathbb{N}$, then the value of the characteristic function of set of odd numbers is the remainder we get after dividing a number by 2;
3. If the universal set is the set of natural numbers $\mathbb{N}$ and A is the set of prime numbers, then the characteristic function of set A is

$$\chi_A(x) = \begin{cases} 1, & \text{if } x \text{ is a prime number} \\ 0, & \text{if } x \text{ is not a prime number.} \end{cases}$$

The characteristic function has the following properties.

Proposition 9.9. *Let U be an universal set and $A, B \subset U$. Then for all $x, y \in U$ the following equalities hold*

1. $\chi_A(x) \cdot \chi_A(x) = \chi_A(x)$;
2. $\chi_{A'}(x) = \chi_{U \setminus A}(x) = 1 - \chi_A(x)$;
3. $\chi_{A \cap B}(x) = \chi_A(x) \cdot \chi_B(x) = \min\{\chi_A(x), \chi_B(x)\}$;
4. $\chi_{A \cup B}(x) = \chi_A(x) + \chi_B(x) - \chi_A(x) \cdot \chi_B(x) = \max\{\chi_A(x), \chi_B(x)\}$;
5. $\chi_{A \setminus B}(x) = \chi_A(x) - \chi_A(x) \cdot \chi_B(x)$;
6. $\chi_{A \triangle B}(x) = \chi_A(x) + \chi_B(x) - 2\chi_A(x) \cdot \chi_B(x)$;
7. $\chi_{A \times B}((x, y)) = \chi_A(x) \cdot \chi_B(y)$.

Proof. To check these equalities it is sufficient to go through every possible case for element x (x in both sets, only in A, only in B, neither of them) and compare the value of the right side expression with the corresponding value of the characteristic function on the left-hand side. For example, equation 1) follows from $0 \cdot 0 = 0$ and $1 \cdot 1 = 1$. Let $x \in U$. With property 3) we have to take into account four different situations:

$$\begin{aligned} &\chi_A(x) = 0 \text{ and } \chi_B(x) = 0, \qquad &&\chi_A(x) = 0 \text{ and } \chi_B(x) = 1, \\ &\chi_A(x) = 1 \text{ and } \chi_B(x) = 0, \qquad &&\chi_A(x) = 1 \text{ and } \chi_B(x) = 1. \end{aligned}$$

Therefore, we get that

$$\begin{aligned} \chi_A(x) \cdot \chi_B(x) = 1 &\Leftrightarrow \chi_A(x) = 1 \wedge \chi_B(x) = 1 \\ &\Leftrightarrow x \in A \wedge x \in B \\ &\Leftrightarrow x \in A \cap B \\ &\Leftrightarrow \chi_{A \cap B}(x) = 1, \end{aligned}$$

from which we have, that $\chi_A(x) \cdot \chi_B(x) = 0 \Leftrightarrow \chi_{A \cap B}(x) = 0$. The proofs of other properties are analogous and are left as independent work for the reader. □

Because sets and their characteristic functions are in a bijective correspondence, this allows our new formulae to be used for proving equalities in set theory. We can show that two sets are equal by showing that their corresponding characteristic functions are equal. Therefore, to check an equality between two sets, we can express either set's characteristic function through the characteristic functions of sets, which appear in the expression, then multiply all sums and differences, and finally simplify everything. When it comes to simplification, it is important to know that $\chi_A(x) \cdot \chi_A(x) = \chi_A(x)$, because the value of a characteristic function is always 0 or 1.

Example 9.10. Let U be a universal set and $A, B \subset U$. Show, that $(A \cap B)' = A' \cup B'$.

Solution. It is enough for us to show, that $\chi_{(A\cap B)'}(x) = \chi_{A'\cup B'}(x)$ for all $x \in U$. Fix $x \in U$. By applying the properties from proposition 9.9 onto the complement, intersection and union we get,

$$\begin{aligned}
\chi_{(A\cap B)'}(x) &= 1 - \chi_{A\cap B}(x) \\
&= 1 - \chi_A(x) \cdot \chi_B(x) \\
&= (1 - \chi_A(x)) + (1 - \chi_B(x)) - (1 - \chi_A(x)) \cdot (1 - \chi_B(x)) \\
&= \chi_{A'}(x) + \chi_{B'}(x) - \chi_{A'\cap B'}(x) \\
&= \chi_{A'\cup B'}(x)
\end{aligned}$$

Now we have that the sets are equal because their characteristic functions are equal for all x. □

Exercise 9.11. Let $A, B, C \subset U$ be sets. Using characteristic functions, show that

(a) $(A \cap B) \cup (A \setminus B) = A$;

(b) $(A \setminus B) \setminus C = (A \setminus C) \setminus (B \setminus C)$;

(c) $(A \cup B) \times C = (A \times C) \cup (B \times C)$.

One way to represent a set in a computer is to use the calculation algorithm of its characteristic function (subprogram/function/procedure in some programming language). It can be a real problem to calculate the value of a characteristic function even though it has only two simple values (0 or 1). It can

- require a lot of time (to decide if x is a prime or a composite number);
- not even have an algorithm (testing, if a program P calculates F).

9.3 Image of a set

Let there be a function $f\colon X \to Y$.

Definition 9.12. If $x \in X$ and $y \in Y$ are such, that $y = f(x)$, then element y is called **the image of element** x.

Every element of domain X has just one image.

Example 9.13.

1. Observe the function $f(x) = x^2$, $f\colon \mathbb{R} \to \mathbb{R}$. Then the image of number 0 is 0, because $f(0) = 0$. The image of numbers -1 and 1 is 1, because $f(-1) = 1 = f(1)$.
2. Observe the function $f(x) = \sqrt{x}$, $f\colon \mathbb{N} \to \mathbb{R}$. Then the image of number 4 is 2, because $f(4) = 2$.
3. Observe the function $f(x) = x + 1$, $f\colon \mathbb{R} \to \mathbb{R}$. Then the image of number 0 is 1, because $f(0) = 1$.

Definition 9.14. The **image** of a set $A \subset X$ is the subset $f(A)$ of set Y, which is made up of all the images of elements in A, i.e.

$$f(A) = \{f(x)\colon x \in A\} = \{y \in Y\colon \exists x\ (x \in A \wedge f(x) = y)\}.$$

Example 9.15.

1. Let us take a look at function $f(x) = x^2$, $f\colon \mathbb{R} \to \mathbb{R}$. Then $f([-10, 10]) = [0, 100]$ and $f(\mathbb{R}) = [0, \infty)$.
2. Let us take a look at function $f(x) = \sin x$, $f\colon \mathbb{R} \to \mathbb{R}$. Then $f(\mathbb{R}) = [-1, 1]$, but also $f([-\pi, \pi]) = [-1, 1]$.
3. Let us take look at function $f(x) = \ln x$, $f\colon (0, \infty) \to \mathbb{R}$. Then $f((0, 1]) = (-\infty, 0]$.

Theorem 9.16. *Let f be a function from set X to set Y. Then*

1. $f(\emptyset) = \emptyset$;
2. $f(X) \subset Y$;
3. *If $A \subset B$, then $f(A) \subset f(B)$;*
4. $f(A \cup B) = f(A) \cup f(B)$;
5. $f(A \cap B) \subset f(A) \cap f(B)$.

Remark. In general, for properties 2 and 5 equalities do not hold. For property 2, let us observe the function $f\colon X \to Y$, where $X = Y = \mathbb{R}$ and $f(x) = x^2$ for all $x \in \mathbb{R}$. Now $f(X) \neq Y$, because

$$f(\mathbb{R}) = \{f(x)\colon x \in \mathbb{R}\} = \{x^2\colon x \in \mathbb{R}\} = [0, \infty) \neq \mathbb{R}.$$

For property 5, we study the sets $A = \{-1\}$ and $B = \{1\}$. Then $f(A) = \{1\} = f(B)$, but $f(A \cap B) = f(\emptyset) = \emptyset$. Therefore,

$$\emptyset = f(A \cap B) \neq f(A) \cap f(B) = \{1\}.$$

Proof of theorem 9.16.

1. According to the definition, we have that $f(\emptyset) = \{f(x)\colon x \in \emptyset\}$. Because not a single element x is in the empty set, then the condition on the right side is not satisfied for all x. Therefore, the set on the right is empty.

2. Let $y \in f(X)$. Based on the definition we have $f(X) = \{y \in Y : \exists x\ (x \in X \wedge f(x) = y)\}$. Thus $y \in Y$.

3. Let $A, B \subset X$ and $A \subset B$. Based on the definition of a subset we have to show that, if $y \in f(A)$, then $y \in f(B)$. Let $y \in f(A)$. Then based on the definition of the image of a set, we have an $x \in A$, such, that $y = f(x)$. Because $A \subset B$, we have $x \in B$. Therefore, there exists $x \in B$, such, that $y = f(x)$, which due to the definition of the image of a set, means that $y \in f(B)$.

4. To prove this equality, we show that either set is a subset of the other.

   (a) Let $y \in f(A \cup B)$. Then there exists an $x \in A \cup B$, such that $y = f(x)$. Based on the definition of an union, we see that $x \in A$ or $x \in B$. If $x \in A$, then based on the definition of a set's image $f(x) \in f(A)$, from which $y \in f(A)$ due to $y = f(x)$, and thus finally $y \in f(A) \cup f(B)$ due to how the union of sets is defined. If $x \in B$, then similarly we get $f(x) \in f(B)$, $y \in f(B)$, and thus finally $y \in f(A) \cup f(B)$. Therefore, in both cases $y \in f(A) \cup f(B)$, which proves our claim that the set $f(A \cup B)$ is a subset of the set $f(A) \cup f(B)$.

   (b) Now, let $y \in f(A) \cup f(B)$. Then due to the union's definition $y \in f(A)$ or $y \in f(B)$. If $y \in f(A)$, then because of the definition of a set's image there exists an $x \in A$ such, that $f(x) = y$. Then $x \in A \cup B$ due to how the union of sets is defined and therefore the definition of a set's image gives us $y \in f(A \cup B)$. If $y \in f(B)$, then the proof is analogous. Again for both cases we have shown that $y \in f(A \cup B)$ and therefore the set $f(A) \cup f(B)$ is a subset of set $f(A \cup B)$.

5. Let $y \in f(A \cap B)$. The definition of a set's image assures the existence of an $x \in A \cap B$ such, that $y = f(x)$. The definition of sets' intersection gives us that $x \in A$ and $x \in B$. Because $y = f(x)$, then with the help of the definition of a set's image, we have a conjunction of $y \in f(A)$ and $y \in f(B)$. This gives us $y \in f(A) \cap f(B)$ due to how the interjection of sets is defined.

□

The fourth and fifth claims of theorem 9.16 also hold for an arbitrary number of sets, this means that

$$f\Big(\bigcup_{\alpha \in \mathcal{I}} A_\alpha\Big) = \bigcup_{\alpha \in \mathcal{I}} f(A_\alpha) \quad \text{and} \quad f\Big(\bigcap_{\alpha \in \mathcal{I}} A_\alpha\Big) \subset \bigcap_{\alpha \in \mathcal{I}} f(A_\alpha).$$

9.4 Preimage of a set

Let there be a function $f : X \to Y$.

Definition 9.17. If $x \in X$ and $y \in Y$ are such, that $y = f(x)$, then the element x is called **a preimage of element** y for the function f.

Some elements of set Y may just have one preimage, some more and some none at all. For example, if we take the quadratic function from the set of real numbers to real numbers, then

every positive real number has two preimages, zero only one preimage and negative real numbers do not have preimages at all. More specifically, if $f(x) = x^2$, $f\colon \mathbb{R} \to \mathbb{R}$, then the preimages of 1 are -1 and 1, because $f(-1) = 1$ and $f(1) = 1$.

Definition 9.18. The **preimage** of a set $B \subset Y$ is the set $f^{-1}(B)$, which consists of all the elements of set X, which map to an element of set B, this means that

$$f^{-1}(B) = \{x \in X\colon f(x) \in B\}.$$

The notation f^{-1} here does not mean that the function f has an inverse function. But if the function f does have an inverse, then the concepts – preimage of set B and the image of set B with its inverse – match (check paragraph 9.10).

We also note, that $x \in f^{-1}(B) \Leftrightarrow f(x) \in B$. This simple observation is sometimes very useful to use in proofs.

Example 9.19.

1. Observe the function $f(x) = x^2$, $f\colon \mathbb{R} \to \mathbb{R}$. Then $f^{-1}(\{1\}) = \{-1, 1\}$ and $f^{-1}([-10, -5]) = \emptyset$.
2. Observe the function $f(x) = 0$, $f\colon \mathbb{R} \to \mathbb{R}$. Then $f^{-1}(\{0\}) = \mathbb{R}$.
3. Observe the function $f(x) = x + 1$, $f\colon \mathbb{R} \to \mathbb{R}$. Then $f^{-1}(\{0\}) = \{-1\}$.

Theorem 9.20. *Let f be a function from set X to set Y and $A, B \subset Y$. Then*

1. $f^{-1}(\emptyset) = \emptyset$;
2. $f^{-1}(Y) = X$;
3. *if $A \subset B$, then* $f^{-1}(A) \subset f^{-1}(B)$;
4. $f^{-1}(A \cup B) = f^{-1}(A) \cup f^{-1}(B)$;
5. $f^{-1}(A \cap B) = f^{-1}(A) \cap f^{-1}(B)$;
6. $f^{-1}(Y \setminus B) = X \setminus f^{-1}(B)$.

Proof.

1. The definition of preimage gives us that $f^{-1}(\emptyset) = \{x \in X\colon f(x) \in \emptyset\}$. Therefore, there cannot be any elements from set X, which map to an element of the empty set, thus the equality holds.
2. The definition of preimage gives us that $f^{-1}(Y) = \{x \in X\colon f(x) \in Y\}$. Now according to the definition of a function, every element of X maps to some element of Y. Therefore, the equality holds.
3. Let $x \in f^{-1}(A)$. From the definition of preimage, we get that $f(x) \in A$. Based on our assumptions, we have that the set A is a subset of set B, and thus also $f(x) \in B$. Now $x \in f^{-1}(B)$ holds because of the definition of a preimage.

4. We show that for an arbitrary $x \in X$ the statement $x \in f^{-1}(A \cup B)$ is true if and only if $x \in f^{-1}(A) \cup f^{-1}(B)$.

$$\begin{aligned} x \in f^{-1}(A \cup B) &\Leftrightarrow f(x) \in A \cup B \\ &\Leftrightarrow f(x) \in A \vee f(x) \in B \\ &\Leftrightarrow x \in f^{-1}(A) \vee x \in f^{-1}(B) \\ &\Leftrightarrow x \in f^{-1}(A) \cup f^{-1}(B). \end{aligned}$$

5. We show that for an arbitrary $x \in X$ the statement $x \in f^{-1}(A \cap B)$ holds if and only if $x \in f^{-1}(A) \cap f^{-1}(B)$.

$$\begin{aligned} x \in f^{-1}(A \cap B) &\Leftrightarrow f(x) \in A \cap B \\ &\Leftrightarrow f(x) \in A \wedge f(x) \in B \\ &\Leftrightarrow x \in f^{-1}(A) \wedge x \in f^{-1}(B) \\ &\Leftrightarrow x \in f^{-1}(A) \cap f^{-1}(B). \end{aligned}$$

6. We show that for an arbitrary $x \in X$ the statement $x \in f^{-1}(Y \setminus B)$ is true if and only if $x \in X \setminus f^{-1}(B)$.

$$\begin{aligned} x \in f^{-1}(Y \setminus B) &\Leftrightarrow f(x) \in Y \setminus B \\ &\Leftrightarrow f(x) \in Y \wedge \neg(f(x) \in B) \\ &\Leftrightarrow x \in f^{-1}(Y) \wedge \neg(x \in f^{-1}(B)) \\ &\Leftrightarrow x \in X \setminus f^{-1}(B), \end{aligned}$$

   where the last equivalency holds due to $f^{-1}(Y) = X$.

□

The properties 4 and 5 of theorem 9.20 also hold for an arbitrary number of sets, this means that

$$f^{-1}\Big(\bigcup_{\alpha\in\mathcal{I}} A_\alpha\Big) = \bigcup_{\alpha\in\mathcal{I}} f^{-1}(A_\alpha) \quad \text{and} \quad f^{-1}\Big(\bigcap_{\alpha\in\mathcal{I}} A_\alpha\Big) = \bigcap_{\alpha\in\mathcal{I}} f^{-1}(A_\alpha).$$

Example 9.21. The image of a set does not have anything analogous to the property 6 of preimage. If, for example, $f\colon X \to Y$ is a constant function, then $f(A) = \{c\}$ (if $A \neq \emptyset$), $f(X \setminus A) = \{c\}$ (if $A \neq X$) and $Y \setminus f(A) = Y \setminus \{c\}$, but $f(X \setminus A) \subset Y \setminus f(A)$ nor $f(X \setminus A) \supset Y \setminus f(A)$ (if $Y \neq \{c\}$) do not take place.

As we can see, when it comes to sets, the properties of preimages are better than the properties of images, which is why usually in other mathematical disciplines the preimages of sets are used to define fundamental properties of functions.

9.5 Preimage of an image and image of a preimage

We get the following properties if we take the preimage of an image or image of a preimage.

Theorem 9.22. *Let $f\colon X \to Y$ be a function. Then*

1. *If $A \subset X$, then $A \subset f^{-1}(f(A))$;*
2. *If $B \subset Y$, then $f(f^{-1}(B)) \subset B$.*

Remark. In examples 9.23 and 9.24 we demonstrate that for both properties equalities generally do not hold.

Proof of theorem 9.22.

1. Let $A \subset X$ and let $x \in A$. We have to show, that $x \in f^{-1}(f(A))$. Based on the definition of a set's preimage we can write $f(x) \in f(A)$. To use the properties of preimages we consider the set $\{f(x)\}$. We get $\{f(x)\} \subset f(A)$. Now we apply property 3 of theorem 9.20 on this and get: $f^{-1}(\{f(x)\}) \subset f^{-1}(f(A))$. But $x \in f^{-1}(\{f(x)\})$, because $f(x) \in \{f(x)\}$ (look at the definition of a set's preimage). Hence, $x \in f^{-1}(f(A))$.
2. Let $B \subset Y$ and let $y \in f(f^{-1}(B))$. We have to show, that $y \in B$. Based on the definition of a set's image there exists an $x \in f^{-1}(B)$, such, that $f(x) = y$. According to the definition of a preimage, $x \in f^{-1}(B)$ implies that $f(x) \in B$. Therefore, $y \in B$.

□

Example 9.23. Let us make certain that generally $A \neq f^{-1}(f(A))$.
Let $X = Y = \mathbb{R}$, $f(x) = |x|$ and $A = \{1, 2, 3\}$. For every $x \in A$ holds $f(x) = x$, this means that $f(A) = A = \{1, 2, 3\}$. On the other hand,

$$f^{-1}(f(A)) = f^{-1}(A) = \{-3, -2, -1, 1, 2, 3\} \neq \{1, 2, 3\} = A.$$

Example 9.24. Let us make certain that generally $f(f^{-1}(B)) \neq B$.
Let $X = Y = \mathbb{R}$, $f(x) = x^2$ and $B = \{-1, 0, 4\}$. Now $f^{-1}(B) = \{-2, 0, 2\}$ and

$$f(f^{-1}(B)) = f(\{-2, 0, 2\}) = \{0, 4\} \neq \{-1, 0, 4\} = B.$$

9.6 Parity of functions

Let $X, Y \subset \mathbb{R}$ and $f\colon X \to Y$ be a function.

Definition 9.25. Function $f\colon X \to Y$ is said to be **even**, if for all $x \in X$, the following conditions hold

1. $-x \in X$;
2. $f(-x) = f(x)$.

The graph of an even function is symmetric with respect to the y-axis.

Definition 9.26. Function $f\colon X \to Y$ is said to be **odd**, if for all $x \in X$, the following conditions hold

1. $-x \in X$;

2. $f(-x) = -f(x)$.

The graph of an odd function is symmetric with respect to the origin.

Example 9.27.

1. If $X = Y = \mathbb{R}$, then functions x, x^3, $\sin x$ and $\tan x$ are all even.
2. If $X = Y = \mathbb{R}$, then functions x^2, $|x|$ and $\cos x$ are all odd.
3. If $X = Y = \mathbb{R}$, then the function $x + x^2$ is neither even or odd.

9.7 Injective, surjective and bijective functions

Definition 9.28. Function $f\colon X \to Y$ is said to be

(a) **injective** or **one-to-one**, if for all pairs $x_1, x_2 \in X$, $x_1 \neq x_2$, holds $f(x_1) \neq f(x_2)$;

(b) **surjective** or **onto**, if for all $y \in Y$ there exists an $x \in X$ with $y = f(x)$;

(c) **bijective** or a **one-to-one correspondence**, if f is both injective and surjective.

Remark. Let $A\colon x_1 \neq x_2$ and $B\colon f(x_1) \neq f(x_2)$. We know from propositional logic, that formulae $A \Rightarrow B$ and $\neg B \Rightarrow \neg A$ are equivalent. Therefore, the injectivity of a function f can be equivalently defined as: if $f(x_1) = f(x_2)$, then $x_1 = x_2$.

Injectivity means that every element of set Y has no more than one preimage.

Surjectivity means that every element of set Y has at least one preimage.

Bijectivity means that every element of set Y has exactly one preimage.

Example 9.29.

1. Let $f(x) = x^2$. We look at this function on different sets.

   Function $f\colon \mathbb{R} \to \mathbb{R}$ is neither injective or surjective, because it maps to every positive real number one positive number and one negative number. Not a single negative element of $\mathbb{R}$ has a preimage.

   Function $f\colon \mathbb{R} \to [0, \infty)$ is surjective, but it is not injective.

   Function $f\colon [0, \infty) \to [0, \infty)$ is injective and surjective, thus it is bijective.

2. Function $\sin\colon \mathbb{R} \to \mathbb{R}$ is not injective or surjective. Why?

   Function $\sin\colon \mathbb{R} \to [-1, 1]$ is surjective, but it is not injective. Why?

   Function $\sin\colon [-\pi/2, \pi/2] \to \mathbb{R}$ is injective, but it is not injective. Why?

   Function $\sin\colon [-\pi/2, \pi/2] \to [-1, 1]$ is injective and surjective, thus it is bijective.

3. Let us have two finite sets $X = \{x_1, \ldots, x_m\}$ and $Y = \{y_1, \ldots, y_n\}$, where one has m element and the other has n elements. We shall investigate under which conditions the function $f\colon X \to Y$ is injective/surjective/bijective.

(a) **Injective.** If $m > n$, then every function $f\colon X \to Y$ has to map more than element of X to a single element of Y. Therefore, there cannot exist an injective function $f\colon X \to Y$. If $m \leq n$, then we are able to construct an injective function.

(b) **Surjective.** If $m < n$, then there at most m images of elements of X in the set Y, this means that there is no surjective function. If $m \geq n$, then there exists a surjective function.

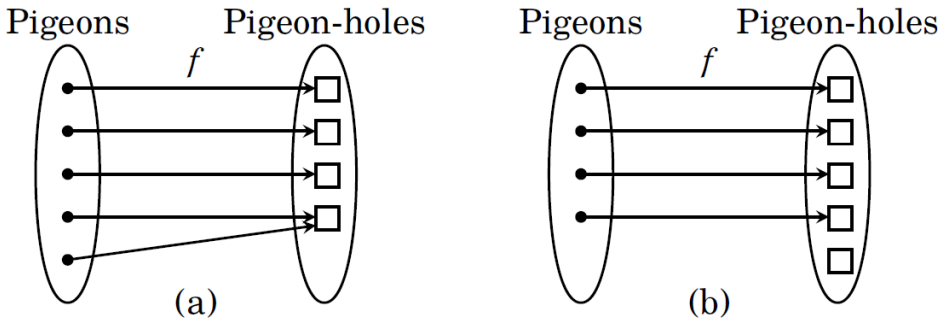
(c) A bijective function exists if and only if $m = n$.

4. Every sequence of real numbers $a_1, a_2, \ldots$ can be viewed as a function $a\colon \mathbb{N} \to \mathbb{R}$. If all members of the sequence are different, then a is injective. For example, if $a_i = 2i$ for all $i \in \mathbb{N}$. Later we will show, that not a single function $a\colon \mathbb{N} \to \mathbb{R}$ is surjective.

Exercise 9.30. Prove, that the function $f\colon X \to Y$ satisfies the conditions $f(A \cap B) = f(A) \cap f(B)$ if and only if it is injective.

9.8 Pigeon-hole principle

Let A be the set of pigeons and B be the set of pigeon-holes. Let us observe the function $f\colon A \to B$, where a pigeon x flies into the pigeon-hole $f(x)$.



- Figure (a) has more pigeons than pigeon-holes, therefore at least two pigeons have to fly into the same hole. Thus, f is not injective.
- Figure (b) has fewer pigeons than pigeon-holes, thus at least one hole is going to stay empty. Therefore, f is not surjective.

Pigeon-hole principle 9.31. *Let A and B be finite sets and $f\colon A \to B$ a function.*

1. *If $|A| > |B|$, then f is not injective.*
2. *If $|A| < |B|$, then f is not surjective.*

Example 9.32. Prove, that there are at least two Estonians, who have the same amount of hair.

Example 9.33. If we are to pick six random natural numbers, then two of them have the same remainder if we are to divide them by five.

9.9 Composition of functions

Just like there are arithmetic operations for combining numbers (like + or ·) or set theoretical operations for sets (for example ∪ and ∩), there are also operations for combining functions. In mathematics a composition of functions (maps) is a function, which you get by applying one function after another.

Definition 9.34. Let X, Y and Z be arbitrary sets. The **product** or **composition** of functions $f\colon X \to Y$ and $g\colon Y \to Z$ is the function $g \circ f\colon X \to Z$, for which $(g \circ f)(x) = g(f(x))$ for all $x \in X$.

Function g is called the **exterior**, function f is the **interior**.

Remark.

1. A composition $g \circ f$ is only possible if the domain of g is the same as the codomain of f (look at example 9.35);
2. The domain of composition $g \circ f$ is shared with function f;
3. It it possible that, you are able to define functions $g \circ f$ and $f \circ g$, but generally they are not the same, this means that $g \circ f \neq f \circ g$ (look at example 9.36). Therefore, the composition of functions is not commutative.

Example 9.35. Let f be a function from $\{a, b, c\}$ to $\{a, b, c\}$ such, that $f(a) = b$, $f(b) = c$ and $f(c) = a$. Let g be a function from $\{a, b, c\}$ to $\{1, 2, 3\}$ such, that $g(a) = 3$, $g(b) = 2$ and $g(c) = 1$. Find $g \circ f$ and $f \circ g$.

Solution. Composition $g \circ f\colon \{a, b, c\} \to \{1, 2, 3\}$ is defined by $(g \circ f)(a) = g(f(a)) = g(b) = 2$, $(g \circ f)(b) = g(f(b)) = g(c) = 1$ and $(g \circ f)(c) = g(f(c)) = g(a) = 3$.
Composition $f \circ g$ is not defined, because the domain $\{a, b, c\}$ of f differs from the codomain $\{1, 2, 3\}$ of g. □

Example 9.36. Let f and g be functions from set $\mathbb{Z}$ to set $\mathbb{Z}$ such that $f(x) = 2x + 3$ and $g(x) = 3x + 2$ for all $x \in \mathbb{Z}$. Find $g \circ f$ and$f \circ g$.

Solution. First we notice that the compositions $g \circ f$ and $f \circ g$ exist. Therefore,

$$(f \circ g)(x) = f(g(x)) = f(3x + 2) = 2(3x + 2) + 3 = 6x + 7$$

ja

$$(g \circ f)(x) = g(f(x)) = g(2x + 3) = 3(2x + 3) + 2 = 6x + 11.$$

We see, that $g \circ f \neq f \circ g$. □

We shall now show that the composition of functions is associative.

Proposition 9.37. *Let X, Y, Z and W be sets. If $f\colon X \to Y$, $g\colon Y \to Z$ and $h\colon Z \to W$, then $h \circ (g \circ f) = (h \circ g) \circ f$.*

Proof. We need to show the equality of two functions. How are we to do that? First we have to show, that their respective domains and codomains are the same, and then prove that every element x in their domain has the same value for both functions. By checking these two conditions we prove that the two functions are equal.
First, let us make sure that the respective domains and codomains of $h \circ (g \circ f)$ and $(h \circ g) \circ f$ are equal. Because $f\colon X \to Y$, $g\colon Y \to Z$ and $h\colon Z \to W$, then $g \circ f\colon X \to Z$ and $h \circ g\colon Y \to W$. Therefore, $h \circ (g \circ f)\colon X \to W$ and $(h \circ g) \circ f\colon X \to W$.
Second, let us check that for any $x \in X$ the functions have the same values. Let x be an element of X. Then $(h \circ (g \circ f))(x) = h((g \circ f)(x)) = h(g(f(x)))$ and $((h \circ g) \circ f)(x) = (h \circ g)(f(x)) = h(g(f(x)))$. Therefore, $h \circ (g \circ f) = (h \circ g) \circ f$. □

Proposition 9.38. *If $f\colon X \to Y$ and $g\colon Y \to Z$ are injective, then $g \circ f\colon X \to Z$ is also injective.*

Proof. Let $x_1, x_2 \in X$ be such, that $x_1 \neq x_2$. Due to the injectivity of function f we have that $f(x_1) \neq f(x_2)$. Based on this and the fact that function g is injective, we get $g(f(x_1)) \neq g(f(x_2))$ or $(g \circ f)(x_1) \neq (g \circ f)(x_2)$. Therefore, function $g \circ f$ is injective. □

Proposition 9.39. *If $f\colon X \to Y$ and $g\colon Y \to Z$ are surjective, then $g \circ f\colon X \to Z$ is also surjective.*

Proof. Let us pick an arbitrary $z \in Z$. Then the surjectivity of g gives us, that there exists a $y \in Y$ such, that $g(y) = z$. Now due to the surjectivity of f, we have an $x \in X$ such, that $f(x) = y$. Thus $(g \circ f)(x) = g(f(x)) = g(y) = z$, which is enough to prove the surjectivity of $g \circ f$. □

The next result follows from propositions 9.38 and 9.39.

Corollary 9.40. *If $f\colon X \to Y$ and $g\colon Y \to Z$ are bijective, then $g \circ f\colon X \to Z$ is also bijective.*

Definition 9.41. Let X be a set. **Similarity transformation** or **identity transformation** $I_X\colon X \to X$ is a function which maps every element of X to itself, this means that $I_X(x) = x$ for all $x \in X$.

We usually omit the lower index if it is clear which set's identify function we are viewing.

Proposition 9.42. *If $f\colon X \to Y$, then $f \circ I_X = I_Y \circ f = f$.*

Proof. We have to show that all three functions are equal. We use the same tactic as in the proof of proposition 9.37. First we will discuss why $f \circ I_X = f$. Because $f \circ I_X\colon X \to Y$ and $f\colon X \to Y$, we see that both functions have the same domain and codomain.
Let us take an arbitrary $x \in X$ and check $(f \circ I_X)(x) = f(I_X(x)) = f(x)$. We see, that the image of x is the same for both functions. Therefore, $f \circ I_X = f$. It is analogous to prove $I_Y \circ f = f$, and thus this is left to the reader. □

Exercise 9.43. Let $f\colon X \to Y$ and $g\colon Y \to X$ be functions. Prove, that if $g \circ f = I_X$, then f is injective and g is surjective.

9.10 Inverse function

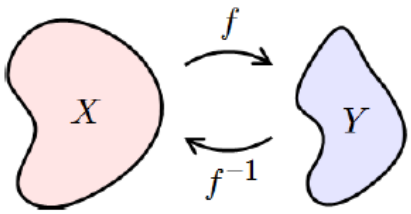
Let $f\colon X \to Y$ be a bijective function. If f is surjective, then every element of Y has a preimage in X. Additionally, because f is an injective function, then every element of Y has exactly one preimage in X. Therefore, we can define a new function from Y to X, which acts in reverse to function f. This brings us to the definition of an inverse function.

Definition 9.44. Let X and Y be sets. The **inverse function** of a bijective function $f\colon X \to Y$ is the function $f^{-1}\colon Y \to X$, which assigns to every $y \in Y$ exactly one $x \in X$, for which $f(x) = y$.

Therefore, the domain of an inverse function is Y and the codomain of it is X. The notation of an inverse function is $x = f^{-1}(y)$, but usually we will see $y = f^{-1}(x)$ (the dependent and independent variables are switched).

We note that if the function $f^{-1}\colon Y \to X$ is the inverse of function $f\colon X \to Y$, then based on the definition, for all $x \in X$ and for all $y \in Y$ we have

$$f(x) = y \Leftrightarrow f^{-1}(y) = x.$$



The discussion before the definition of an inverse function showed us, that a function f has an inverse if and only if f is bijective. Hence, the phrases „function $f\colon X \to Y$ is bijective", „there exists an inverse function $f^{-1}\colon Y \to X$", „function $f\colon X \to Y$ is invertible" are all equivalent.

Example 9.45. Let f be a function from $\{a, b, c\}$ to $\{1, 2, 3\}$, such that $f(a) = 3$, $f(b) = 2$ and $f(c) = 1$. Does it have an inverse f^{-1}, and if it does, then what is f^{-1}?

Solution. Firstly, we notice that f is bijective (check!) and thus there exists f^{-1}.
Secondly, $f^{-1}(1) = c$, $f^{-1}(2) = b$ and $f^{-1}(3) = a$. □

Example 9.46. Let $f\colon \mathbb{Z} \to \mathbb{Z}$ be a function, such that $f(x) = x + 1$ for all $x \in \mathbb{Z}$. Does it have an inverse f^{-1}, and if it does, then what is f^{-1}?

Solution. Firstly, we notice that f is bijective (check!) and thus there exists f^{-1}.
Secondly, denote $y = f(x)$. Then we get, that $y = x + 1$ or $x = y - 1$. But this means that $y - 1$ is the element which f projects to y. Therefore, $f^{-1}(y) = y - 1$. □

Next up let us take a look at some of the properties of inverse functions.

Proposition 9.47. *Let X and Y be sets, and $f\colon X \to Y$ a bijective function. Then $f \circ f^{-1} = I_Y$ and $f^{-1} \circ f = I_X$.*

Proof. Independent work. □

Theorem 9.48. *If $f\colon X \to Y$ and $g\colon Y \to X$ are functions, for which $g \circ f = I_X$ and $f \circ g = I_Y$, then there exists f^{-1} and $f^{-1} = g$.*

Proof. We start our proof by showing that f^{-1} exists. For this we have to make sure that f is bijective. First, f is injective, because if $f(x_1) = f(x_2)$, then

$$x_1 = I_X(x_1) = (g \circ f)(x_1) = g(f(x_1)) = g(f(x_2)) = (g \circ f)(x_2) = I_X(x_2) = x_2.$$

Second, f is surjective, because $f(g(y)) = (f \circ g)(y) = I_y(y) = y$ for all $y \in Y$, hence every element $y \in Y$ has a preimage $g(y) \in X$. Therefore, f is bijective.
Finally, based on the propositions 9.37, 9.42 and 9.47 we get, that

$$f^{-1} = f^{-1} \circ I_Y = f^{-1} \circ (f \circ g) = (f^{-1} \circ f) \circ g = I_X \circ g = g.$$

□

Corollary 9.49. *If $f\colon X \to Y$ is invertible, then $f^{-1}\colon Y \to X$ is also invertible, and $(f^{-1})^{-1} = f$.*

Proof. Independent work. □

Theorem 9.50. *If $f\colon X \to Y$ and $g\colon Y \to Z$ are invertible, then function $g \circ f\colon X \to Z$ is also invertible, and $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.*

Proof. First, to see that $g \circ f\colon X \to Z$ even has an inverse, we have to check if it is bijective. Because f and g are invertible, then they are also bijective. Based on corollary 9.40 we see that $g \circ f$ is bijective, so also invertible.
We will now show that $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$. Based on theorem 9.48 it is sufficient to prove that $(g \circ f) \circ (f^{-1} \circ g^{-1}) = I$ and $(f^{-1} \circ g^{-1}) \circ (g \circ f) = I$. Indeed,

$$(g \circ f) \circ (f^{-1} \circ g^{-1}) = g \circ (f \circ f^{-1}) \circ g^{-1} = g \circ I \circ g^{-1} = g \circ g^{-1} = I$$

and

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

□

Let $f\colon X \to Y$ be a bijective function. Earlier we used the notation f^{-1} to denote the preimage of set $B \subset Y$, and we used the definition $f^{-1}(B) = \{x \in X\colon f(x) \in B\}$. On the other hand, the definition of an inverse function allows us consider f^{-1} as a function from set Y to set X and $f^{-1}(B)$ as this function's image of set B. Let us check that this is consistent with what we know so far:

$$
\begin{aligned}
&f^{-1}(B) \text{ (image of set } B \text{ by function } f^{-1}) \\
&\qquad = \{f^{-1}(y) \in X : y \in B\} \\
&\qquad = \{x \in X : f(x) \in B\} \\
&\qquad = f^{-1}(B) \text{ (preimage of set } B \text{ by function } f),
\end{aligned}
$$

where the first and last equality hold because of the definitions of image and preimage, and the middle equality $\{f^{-1}(y) \in X : y \in B\} = \{x \in X : f(x) \in B\}$ due to the notation $f^{-1}(y) = x$ or $y = f(x)$.

10

Cardinality of sets

***

A mathematician is a device for
turning coffee into theorems –
P. Erdös

10.1 Equivalency of sets

Comparison of sets by $A \subset B$, $A \neq B$ does not offer us much, because sets can have very different elements. It is more interesting to compare them „quantitatively", i.e., what is the answer to the question, „Do these sets have the same amount of elements?"

In this chapter we will define which sets have „the same size". For finite sets the size of a set is equal to the number of elements it has. Therefore, for finite sets $A = \{a_1, \ldots, a_n\}$ and $B = \{b_1, \ldots, b_m\}$, we just count their elements, then compare numbers m and n. If $m = n$, then both sets have the same number of elements.

Already in ancient times, people learned how to count elements in sets and how to compare finite sets based on the number of elements they have. First, let us define finite and infinite sets, then recall what we know about comparing set sizes.

Definition 10.1. Set X is said to be **finite** if X is empty or if we can find a natural number $n \geq 1$, such that there exist a one-to-one correspondence from X to $\{1, \ldots, n\} \subset \mathbb{N}$. Set X is said to be **infinite** if it is not finite.

It is clear we cannot construct an one-to-one correspondence for multiple different n and therefore the definition of a finite set gives us exactly one natural number for every finite set – the

number of elements it has.

Definition 10.2. The **cardinality** of a finite set X is the number of its elements, and it is denoted by the symbol $|X|$.

Proposition 10.3. *Let A and B be finite sets. Then*

1. $|\mathcal{P}(A)| = 2^{|A|}$
2. $|A \cup B| = |A| + |B| - |A \cap B|$
3. $|A \setminus B| = |A| - |A \cap B|$
4. $|A \times B| = |A| \cdot |B|$

Proof. Independent work! □

The number of elements in a set as its measurement of size has the following properties:

1. Sets X and Y have the same amount of elements if and only if there exists an one-to-one correspondence between the elements of X and Y;
2. Set X has less elements than Y if and only if there does not exist an one-to-one correspondence between X and Y but there exists an one-to-one correspondence between X and some proper subset of Y, $B \subsetneq Y$.

Based on the second property it is natural for us to take every infinite set as greater than every finite set.

The first property tells us that not a single finite set can be in a one-to-one correspondence with some proper subset of itself. This property does not apply to infinite sets. Next, we will see that there exists a one-to-one correspondence between the set of natural numbers and the set of even natural numbers, and between any two positive length intervals, such as $[0, 2]$ and $[0, 1]$. In reality we can construct an one-to-one correspondence for every infinite set and its proper subset. Philosophers of Ancient Greece were already familiar with examples similar to the first one. They considered such examples paradoxical, and thus they did not research infinite sets. For them, infinity was just the denial of finity. Only by the second half of 19th century mathematicians started exploring the concept of infinity. Georg Cantor (1845–1918) generalized the concept of number of elements in a set to infinite sets by defining cardinality of a set. This resulted in the discovery of different infinities.

Definition 10.4. Sets X and Y are **equivalent** or **have the same cardinality** if there exists a bijection $f\colon X \to Y$.

To show that sets X and Y are equivalent we usually use the notation $X \sim Y$ or $|X| = |Y|$.

Let us take a look at the next few one-to-one correspondences which give us examples of equivalent sets.

Example 10.5. Two finite sets X and Y are equivalent if and only if they have the same number of elements, or in other words, if set X has k elements, then set X is equivalent to every other set which also has k elements.

Example 10.6. Let $X = \mathbb{N}$ and $Y = \{x \in \mathbb{N}\colon\ x \text{ is an even number}\}$. The bijection $f\colon X \to Y$ is $f(x) = 2x$ for all $x \in \mathbb{N}$, and therefore sets X and Y have the same cardinality, or in other words, there are as many positive even numbers as there are natural numbers.

Example 10.7. We can create an one-to-one correspondence between the set of natural numbers $\mathbb{N}$ and the set of integers $\mathbb{Z}$ with the next bijection $f\colon \mathbb{N} \to \mathbb{Z}$ if we are to define:

$$f(x) = \begin{cases} \frac{x-1}{2}, & \text{if } x \text{ is an odd number} \\ \frac{-x}{2}, & \text{is } x \text{ an even number.} \end{cases}$$

The inverse $f^{-1}\colon \mathbb{Z} \to \mathbb{N}$ has the form:

$$f^{-1}(x) = \begin{cases} 2x+1, & \text{if } x \geq 0 \\ -2x, & \text{if } x < 0. \end{cases}$$

Therefore, there are as many integers as there are natural numbers.

Example 10.8. Let $a, b, c, d \in \mathbb{R}$. If $a < b$ and $c < d$, then $[a, b] \sim [c, d]$, $(a, b) \sim (c, d)$, and $[a, b) \sim [c, d)$. The bijection for all cases is the linear function

$$f(x) = \frac{(d-c)x + bc - ad}{b-a}, \quad x \in [a, b] \text{ (or } x \in (a, b) \text{ or } x \in [a, b)).$$

Example 10.9. Interval $(-\frac{\pi}{2}, \frac{\pi}{2})$ and the set $\mathbb{R}$ have the same cardinality because the function $\tan\colon (-\frac{\pi}{2}, \frac{\pi}{2}) \to \mathbb{R}$ is bijective.

Example 10.10. The set of real number pairs $\mathbb{R}^2$ and the set of complex numbers $\mathbb{C}$ have the same cardinality, because both have a one-to-one correspondence to all points of a plane. You can create this correspondence with the function $f\colon \mathbb{R}^2 \to \mathbb{C}$, where $f((a, b)) = a + bi$ for all $(a, b) \in \mathbb{R}^2$, $i^2 = -1$.

Next we will list some of the most important properties of set equivalency.

Proposition 10.11. *Let A, B and C be sets. Then*

1. *$A \sim A$;*
2. *If $A \sim B$, then $B \sim A$;*
3. *If $A \sim B$ and $B \sim C$, then $A \sim C$.*

Proof.

1. For a set A we have the identity transformation I_A which puts every element of A to an one-to-one correspondence with itself;
2. If $A \sim B$, then there exists a bijective $f\colon A \to B$. The function f has an inverse function $f^{-1}\colon B \to A$ which is also bijective (check this!);
3. If $A \sim B$ and $B \sim C$, then there exist bijections $f\colon A \to B$ and $g\colon B \to C$. Their composition $g \circ f\colon A \to C$ is also bijective (why?).

□

10.2 Countable sets

Definition 10.12. A set X is said to be **countable**, if there exists a bijection between X and the set of natural numbers $\mathbb{N}$.

Therefore, a set X is countable if you can express it in the form $X = \{x_1, x_2, \dots, \}$. We prove this later (check proposition 10.14). First, we will have a look at some examples of countable sets.

Example 10.13.

1. Both the set of even numbers and the set of integers are countable;
2. All infinite subsets of $\mathbb{N}$ are countable and have the same cardinality as the set of natural numbers $\mathbb{N}$.
3. The set of rational numbers $\mathbb{Q}$ is countable and has the same cardinality as the set of natural numbers $\mathbb{N}$ (or the set of integers $\mathbb{Z}$).

   Intuition tells us that there should be more rational numbers than integers because between two integers there is an infinite amount of rational numbers and between every two rational numbers there is again an infinite amount of rational numbers. Cantor was the first person to show that the set of rational numbers is countable, or in other words, in an one-to-one correspondence with the set of natural numbers.
4. Now that we know that the set of rational numbers is countable, it is natural to think that all infinite sets are countable. This is not the case. Again, Cantor showed that $\mathcal{P}(\mathbb{N})$, the set of all subsets of $\mathbb{N}$, is not countable, just like the set of irrational numbers $\mathbb{I}$ and the set of real numbers $\mathbb{R}$ are not countable. Even more interesting, the interval $(0, 1)$ is not countable.

Let us prove some general theorems about countable sets.

Proposition 10.14. *Set X is countable if and only if you can present the elements of X as a sequence of pairwise distinct elements $X = \{x_1, x_2, \dots\}$.*

Proof. If X is countable, then there exists a set of pairs $\{(1, x_1), (2, x_2), (3, x_3), \dots\}$ which puts the elements of $\mathbb{N}$ and X into an one-to-one correspondence. In this set of pairs every natural number is seen exactly once as the left component of a pair and every element of X is also seen exactly once as the right component of a pair. If we look at the sequence made up of every pair's right components $\{x_1, x_2, \dots\}$, then the elements of this sequence are pairwise distinct, and therefore holds $X = \{x_1, x_2, \dots\}$. If set X is presented in the form $X = \{x_1, x_2, \dots\}$, then every infinite sequence $\{x_1, x_2, \dots\}$ has pairwise distinct elements, thus the set of pairs $\{(1, x_1), (2, x_2), (3, x_3), \dots\}$ is the one-to-one correspondence between $\mathbb{N}$ and X (check this!). □

Theorem 10.15. *Every infinite set has a countable subset.*

Proof. Let X be an arbitrary infinite set (thus it is not finite, and also $X \neq \emptyset$). We will describe how to construct an infinite pairwise distinct sequence consisting of different elements of X.

1. Choose element $x_1 \in X$. This is possible, because X is not empty.
2. Choose element $x_2 \in X \setminus \{x_1\}$. This is possible because if $X \setminus \{x_1\}$ was empty, then $X = \{x_1\}$ and it would be finite.
3. Choose element $x_3 \in X \setminus \{x_1, x_2\}$. This is possible because if $X \setminus \{x_1, x_2\}$ was empty, then $X = \{x_1, x_2\}$ and it would be finite.

We can continue this procedure infinitely and get $Y = \{x_1, x_2, x_3, \dots\}$ which has pairwise distinct elements, because, based on our construction, every element is different from previous members of the sequence. Therefore, we have found our countable subset $Y \subset X$. □

Theorem 10.16. *Every infinite subset of a countable set is countable.*

Proof. Let X be a countable set, and let Y be its infinite subset. Based on proposition 10.14 we can present the elements of X as an infinite pairwise distinct sequence: $X = \{x_1, x_2, \dots\}$. If we leave out the elements that are not in Y, then we get an infinite subsequence $\{x_{i_1}, x_{i_2}, \dots\}$, which is made from the elements of set Y. The members of sequence x_{i_j} are pairwise distinct because we got this sequence by leaving out elements from a pairwise distinct sequence. Proposition 10.14 gives us that the set Y is countable. □

Theorems 10.15 and 10.16 tell us that the countable cardinality is the smallest infinite cardinality.

Example 10.17. Every infinite subset of the set of natural numbers (integers, rational numbers) is countable.

Next, we will some properties of countable sets related to unions and intersections.

Theorem 10.18.

1. *The union of a countable set and a finite set is countable.*
2. *The union of two countable sets is countable.*
3. *The finite union of countable sets is countable.*
4. *The countable union of pairwise distinct finite sets is countable.*
5. *The countable union of countable sets is countable.*
6. *The Cartesian product of two countable sets is countable.*
7. *The countable Cartesian product of countable sets is countable.*

Proof. We will prove the fifth property, the rest are left as independent work.
Without loss of generality, we assume that A_i are pairwise disjoint sets. Let

$$\begin{aligned} A_1 &= \{a_{11}, a_{12}, \dots, a_{1n}, \dots\} \\ A_2 &= \{a_{21}, a_{22}, \dots, a_{2n}, \dots\} \\ A_3 &= \{a_{31}, a_{32}, \dots, a_{3n}, \dots\} \\ &\dots \end{aligned}$$

Then we can write that $\bigcup_{i=1}^{\infty} A_i = \{a_{11}, a_{12}, a_{21}, a_{13}, a_{22}, a_{31}, \dots\}$, or in short, set $\bigcup_{i=1}^{\infty} A_i$, is countable. □

Remark. Both proofs of theorem 10.15 and the fifth property of theorem 10.18 include the implicit use of axiom of choice which you can read more of in paragraph **??**.

Example 10.19. With the help of these general results, we can show that many sets known in mathematics are countable. Earlier we already mentioned that the set of rational numbers is countable. Indeed, all rational numbers can be uniquely presented as irreducible fractions $\frac{m}{n}$, where $m \in \mathbb{Z}$ and $n \in \mathbb{N}$; therefore the function $f\colon \mathbb{Q} \to A \subset \mathbb{Z} \times \mathbb{N}$, where $f(\frac{m}{n}) = (m, n)$ and A is made up of irreducible fractions, is a bijection (check this!). For example, $(3, 4) \in A$, but $(6, 8) \notin A$. Thus, $\mathbb{Q} \sim A$. Now because $\mathbb{Z}$ and $\mathbb{N}$ are countable, then because of the seventh claim of theorem 10.18 we have that $\mathbb{Z} \times \mathbb{N} \sim \mathbb{N}$. On the other hand, because an infinite subset of a countable sets is countable, then $A \sim \mathbb{N}$. Therefore, we have that $\mathbb{Q} \sim A \sim \mathbb{N}$, or in other words, the set of rational numbers, is countable.

Additionally, the set of points with only rational coordinates in two (or three) dimensional space is also countable. The set of polynomials with rational coefficients is also countable.

In computers we actually handle countable sets. All information in a computer's memory is presented in the form of natural numbers. This means that data presented in a fixed manner (real numbers, programs, words of a language, etc) is potentially a countable set. „Potentially" here signifies that the size of memory and/or, a filetype's definition cuts out a subset of this set, but by principle it is possible for this subset to be as big as the user wishes (by using a computer with more memory, dynamic databases, etc). When writing a program we intend it to be used with a countable set (like arbitrary integers). But for some problems we consider constraints.

The next example shows us that many sets important to informatics and programming are countable.

Example 10.20.

1. If A is a finite alphabet $\{a_1, a_2, \ldots, a_n\}$, then the set of all (finite length) words in alphabet A is countable.
2. The set of programs in every programming language is countable.
3. If A is a countable alphabet $\{a_1, a_2, \ldots\}$, then the set of all (finite length) words in alphabet A is countable.

All these assertions come pretty straightforward from the general properties of countable sets.

10.3 Cantor–Bernstein theorem

Definition 10.21. We say that the cardinality of set A **does not exceed** the cardinality of set B if there exists an injection $f\colon A \to B$.

We use the notation $|A| \leq |B|$ to signify that the cardinality of A does not exceed the cardinality of B.

Note that the existence of injection $f\colon A \to B$ is equivalent to the existence of bijection $f\colon A \to f(A) \subset B$.

Example 10.22.

1. Observe a finite set $A = \{a_1, \ldots, a_n\}$. Function $f\colon A \to \mathbb{N}$, where $f(a_k) = k$, $k = 1, \ldots, n$, is injective, therefore the cardinality of A does not exceed the cardinality of $\mathbb{N}$.
2. If $A \subset B$, then a function $f\colon A \to B$, where $f(a) = a$, $a \in A$, is injective. Therefore, the cardinality of a set's subset does not exceed the cardinality of the set it's a subset of. For example, the cardinality of both $\mathbb{N}$ and $\mathbb{Q}$ do not exceed the cardinality of $\mathbb{R}$.

An effective method for proving equivalency between sets is the next theorem which proof you can read in book [4].

Theorem 10.23 (Cantor–Bernsteini theorem)**.** *If the cardinality of set A does not exceed the cardinality of set B and the cardinality of B does not exceed the cardinality of A, then sets A and B have the same cardinality.*

In other words, Cantor–Bernstein theorem tells us that if there exist two injective functions $f\colon A \to B$ and $g\colon B \to A$, then sets A and B have the same cardinality. Or in short, if $|A| \leq |B|$ and $|B| \leq |A|$, then $|A| = |B|$.

Example 10.24. Prove that $(0, 1) \sim (0, 1]$.

Proof 1. We note that it is not immediately clear how to construct a bijection between $(0, 1)$ and $(0, 1]$. Thanks to Cantor–Bernstein theorem, it is sufficient to only construct two injections which is a much simpler task.
First, an injection from set $(0, 1)$ to set $(0, 1]$ is $f(x) = x$ for all $x \in (0, 1)$ because $(0, 1) \subset (0, 1]$.
Second, an injection from set $(0, 1]$ to set $(0, 1)$ is $g(x) = \frac{x}{2}$ for all $x \in (0, 1]$ because g is injective and $g((0, 1]) = (0, \frac{1}{2}] \subset (0, 1)$.
Now that we have constructed two injections $f\colon (0, 1) \to (0, 1]$ and $g\colon (0, 1] \to (0, 1)$, then, based on the theorem 10.23, we get $(0, 1) \sim (0, 1]$. □

Now we will present a proof where we construct a bijection between $(0, 1)$ and $(0, 1]$.

Proof 2. Let

$$A = \{\frac{1}{n+1} \colon n \in \mathbb{N}\} \subset (0, 1) \quad \text{and} \quad B = \{\frac{1}{n} \colon n \in \mathbb{N}\} \subset (0, 1].$$

Then $A \sim B$, because $f\colon A \to B$, where $f(\frac{1}{n}) = \frac{1}{n-1}$, $n \geq 2$, is bijective (check this!). The bijection (check this!) we are searching for between $(0, 1)$ and $(0, 1]$ is $g\colon (0, 1) \to (0, 1]$, where

$$g(x) = \begin{cases} f(x), & \text{if } x \in A \\ x, & \text{if } x \in (0, 1) \setminus A. \end{cases}$$

□

Exercise 10.25. Prove, that $(0, 1) \sim [0, 2)$ and $(0, 1) \sim [0, 3]$.

10.4 Cardinality of continuum

There would be no point to compare infinite sets if they all were countable. The creator of set theory, G. Cantor, spent a long time trying to prove the countability of the set of real numbers $\mathbb{R}$. Much to his surprise, he discovered that this set and all its intervals are not countable.

The first step of researching infinite cardinalities is the next theorem.

Theorem 10.26. *Interval* $(0,1)$ *and the set of natural numbers* $\mathbb{N}$ *are not equivalent.*

Proof. Let us assume the opposite, say that $(0,1)$ is countable, this means that there is a one-to-one correspondence between the sets $\mathbb{N}$ and $(0,1)$. Therefore, the set $(0,1)$ must be able to be presented as a countable set: $(0,1) = \{x_1, x_2, x_3, \dots\}$. We write down all the numbers of this set in the following fashion:

$$\begin{aligned} x_1 &= 0, a_{11}a_{12}a_{13}\dots a_{1j}\dots \\ x_2 &= 0, a_{21}a_{22}a_{23}\dots a_{2j}\dots \\ x_3 &= 0, a_{31}a_{32}a_{33}\dots a_{3j}\dots \\ &\dots\dots, \end{aligned}$$

where a_{ij} are the decimals $(0,1,2,\dots,9)$ of numbers, and a_{ij} is the j-th decimal of number x_i. Now we create a number $y = 0, b_1b_2b_3\dots b_j\dots$, where $b_1 \neq a_{11}$, $b_2 \neq a_{22}, \dots, b_j \neq a_{jj}$ and for all j it holds that $b_j \neq 9$ and $b_j \neq 0$. The first conditions makes sure that the new number y does not belong in our countable „list“ (why?), The last two conditions guarantee us that the decimal fraction is a real number and that this number is not 0. Therefore, this new real number y belongs to interval $(0,1)$ and it differs from all the numbers in our „list“, which is why our „list“ cannot be an one-to-one correspondence between $\mathbb{N}$ and $(0,1)$. □

Corollary 10.27.

1. *Every interval* (a,b) *is equivalent to* $(0,1)$*; therefore it is not countable;*
2. $\mathbb{R}$ *is equivalent to* $(0,1)$*; therefore it is not countable.*

Proof. The first assertion follows from example 10.8, and the second assertion follows from examples 10.8 and 10.9, because $(0,1) \sim (-\frac{\pi}{2}, \frac{\pi}{2}) \sim \mathbb{R}$. □

Therefore, there exist infinite sets with different cardinalities.

Definition 10.28. A set which is equivalent to $\mathbb{R}$ is said to have the **cardinality of continuum**.

Therefore, set $\mathbb{R}$ and all intervals (a,b) and $[a,b]$, where $a < b$, have the cardinality of continuum.

Because $\mathbb{Q}$ and $\mathbb{I}$ are respectively the sets of rational and irrational numbers, then $\mathbb{R} = \mathbb{Q} \cup \mathbb{I}$. Since $\mathbb{Q}$ is a countable set, then $\mathbb{I}$ cannot be countable, otherwise $\mathbb{R}$ would also be a countable set (check theorem 10.18, proposition 2). Therefore, the set of irrational numbers $\mathbb{I}$ has the cardinality of continuum.

We know that every infinite set has a countable subset (check theorem 10.15), thus it is safe to assume that when it comes to infinite sets countable sets have the smallest cardinality. Let us define the principle of comparing cardinalities.

Definition 10.29. If the cardinality of set A does not exceed the cardinality of B, and if A and B are not equivalent, then we say that the cardinality of A is **less** than the cardinality of B (or the cardinality of B is greater than the cardinality of A).

In other words, if there exists an injection $f\colon A \to B$ and there does not exist a surjection $g\colon A \to B$, then we say that the cardinality of A is less than the cardinality of B, and we write $|A| < |B|$.

For example, the cardinality of any finite set A is less than the cardinality of $\mathbb{N}$. Likewisely, the cardinality of $\mathbb{N}$ (or $\mathbb{Q}$ or $\mathbb{Z}$) is less than the cardinality of $(0, 1)$ (or $\mathbb{R}$).

Now we are finally able to resolve an earlier example (check example 9.29), where we said that the sequence $a\colon \mathbb{N} \to \mathbb{R}$ cannot be surjective. Let us take a look at $a(\mathbb{N})$. It can either be a finite or a countable set depending on if the sequence $a(1), a(2), \ldots$ has finite or infinite number of members. In both cases the cardinality of set $a(\mathbb{N})$ is less than the cardinality of $\mathbb{R}$, hence $a(\mathbb{N}) \neq \mathbb{R}$.

Notice how we have not yet defined the cardinality of an infinite set. We have only been talking about comparing the cardinalities of different sets. The popular description is that the cardinality of a set is a class of sets with the same cardinality (exact definition in the next chapter, check definition 11.49). We denote the cardinality of a set A with the symbol $|A|$ or card A and call this its **cardinal number**. If $A = \{a_1, \ldots, a_n\}$, then we write $|A| = n$, also $|\emptyset| = 0$. For a countable set we use the notation $\aleph_0$ (read aleph-zero) or $|\mathbb{N}| = \aleph_0$. For continuum sets we use the symbol c or $|\mathbb{R}| = c$. Summary,

$$n < \aleph_0 < c$$

for all $n \in \mathbb{N}$.
This prompts us to ask if there exist sets with bigger cardinalities i.e., is there something greater than continuum? The next theorem gives us a positive answer to these questions.

Theorem 10.30 (Cantor's theorem)**.** *The set $\mathcal{P}(A)$ of all subsets of set A has a greater cardinality than A, or $|A| < |\mathcal{P}(A)|$.*

Proof. We have to show that $|A| \leq |\mathcal{P}(A)|$ and $|A| \neq |\mathcal{P}(A)|$. We can assume $A \neq \emptyset$ because the assertion always holds for the empty set.
First, $|A| \leq |\mathcal{P}(A)|$, because the function $f\colon A \to \mathcal{P}(A)$, where $f(a) = \{a\}$ for all $a \in A$, is injective.
To see that $|A| \neq |\mathcal{P}(A)|$ we assume the opposite, which is that $|A| = |\mathcal{P}(A)|$. Then, there exists a bijection $g\colon A \to \mathcal{P}(A)$. Let $g(a) = A_a \subset A$, $a \in A$. Therefore, either $a \in A_a$ or $a \notin A_a$. Denote $A^* = \{a \in A\colon a \notin A_a\}$ and $a^* = g^{-1}(A^*)$, then $g(a^*) = A^*$. Because $g(a^*) = A_{a^*}$, then $A^* = A_{a^*}$. Does $a^* \in A_{a^*}$ hold?

1. If we are to assume $a^* \in A_{a^*}$, then based on the definition of A^* we get $a^* \notin A^*$ or $a^* \notin A_{a^*}$, a contradiction.

2. If we are to assume $a^* \notin A_{a^*}$, then based on the definition of A^* we get $a^* \in A^*$ or $a^* \in A_{a^*}$, a contradiction.

Hence both possibilities lead us to a contradiction, which shows us that a bijection $g\colon A \to \mathcal{P}(A)$ cannot exist.

□

Therefore, there exist a set with a cardinality greater than continuum – for example the set $X = \mathcal{P}(\mathbb{R})$ of all subsets of $\mathbb{R}$. An even greater set is $\mathcal{P}(X)$, etc. In summary, a set can be as large was we want and more. The theory of cardinalities is what made set theory (which also happens to be a convenient mathematical language) a fundamental branch of mathematics.

Cantor's theorem also tells us that there does not exist a set of all sets or that this collection cannot be viewed as a set. Indeed, this „set" would have to contain the set of all its subsets, which is impossible according to Cantor's theorem.

The concept of set cardinality was first introduced by the father of set theory, Georg Cantor, in 1878. At the same time he formulated the **continuum hypothesis**, which says that there cannot be a set with cardinality greater than $\mathbb{N}$ but less than $\mathbb{R}$. This is not a theorem. Regular set theory axiomatics (like Zermelo-Fraenkeli axiomatics plus the axiom of choice) do not make it possible to derive the continuum hypothesis or its negation. On 1940, Kurt Gödel showed that by adding the axiom of choice and continuum hypothesis to regular set theory axiomatics gives a noncontradictory (consistent) system of axiomatics. But in 1963, an American mathematician Paul Cohen showed that by adding the negation of axiom of choice and the negation of continuum hypothesis to those same axiomatics also gives a noncontradictory system of axiomatics. Simply put, we can observe two different set theories: one, where the continuum hypothesis holds (no inbetween cardinal numbers between $\aleph_0 < \aleph_1$), and two, where the negation of continuum hypothesis holds (there exist inbetween cardinal numbers between $\aleph_0 < \ldots < \aleph_1$).

On the assumption that continuum hypothesis holds, the cardinal number $\aleph_1$ is defined as the cardinality of $\mathbb{R}$. This cardinal number follows $\aleph_0$. Hence:

$$c = 2^{\aleph_0} = \aleph_1.$$

11

Relations

***

Mathematicians do not study objects,
but the relations between objects –
H. Poincaré

In everyday life we come across things and events that are related to each other. For example, every person has their own phone, work can be related to getting paid, you are related to other people by blood, etc. In mathematics we are also interested in relations, for example the relation between numbers and their divisors, or in higher mathematics the relation between argument x and corresponding value $f(x)$ of function f. An example of a relation in geometry is congruence, which we use to study triangles. These examples show us that mathematics is full of relations. Typically we use relations in the study of certain objects (triangles, integers, matrices, etc), in this chapter our objective is to study relations themselves.

11.1 Definition of relation

Definition 11.1. Let A and B be sets. A **relation** or **connection** between sets A and B is any subset of $A \times B$.

Therefore, a relation between A and B is a set of ordered pairs (a, b), where $a \in A$ and $b \in B$. In other words, a relation is a subset $R \subset A \times B$. For a pair $(a, b) \in R$ we say that the **elements a and b are in relation** R and denote aRb. Sometimes the statement $(a, b) \in R$ is also read as **element a is related to b by** R.

Relation $R = A \times B$ is called the **universal relation** and relation $\emptyset \subset A \times B$ the **empty relation**.

If $A = B$, i.e., $R \subset A \times A$, then we are talking of a **relation on set** A.

In the above definition it is more accurate to talk of a binary relation or a relation between two sets, because an n-ary relation between sets $A_1, \ldots, A_n$ is any subset of $A_1 \times \ldots \times A_n$. From now on we will generally study binary relations.

Generally we use a description or property when specifying relations and use specific symbols to signify this, for example: $=, <, \geq, \subset, \|$, etc. In reality we rarely think of a relation as a set of ordered pairs. Rather we think of a relation as a „test“, which a pair of numbers or objects (a, b) has to satisfy so that aRb. If a and b are not in a relation R, then we draw a line through the relation symbol, for example $a \neq b$ or $A \not\subset B$.

How to understand the definition of a relation as a set of ordered pairs? Think of it as a complete list of all object pairs which satisfy a given relation. Let us take a look at examples which will help us understand this definition.

Example 11.2. Let $A = \{2, 3\}$ and $B = \{1, 2, 3, 4, 5, 6\}$. Then $R_1 = \{(2, 2), (2, 3), (3, 1), (3, 5)\}$ is a binary relation between sets A and B. We can find many more relations between sets A and B, like relation R_2, which is made of all pairs (a, b) for which b is divisible by a. Then $R_2 = \{(2, 2), (2, 4), (2, 6), (3, 3), (3, 6)\}$.

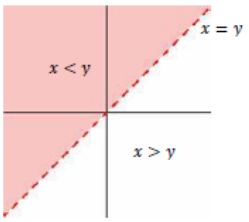
Example 11.3. Let A be the set of all natural numbers $\mathbb{N}$ and relation R be the subset of $\mathbb{N} \times \mathbb{N}$, which consists of all the pairs (a, b), where a divides b. Thus $R = \{(a, b) \colon a, b \in \mathbb{N}, a \mid b\}$. This relation R is called the **divisibility relation**.

Example 11.4. Let A be an arbitrary set and $R = \{(a, a) \colon a \in A\}$. For any elements $a, b \in A$ let $(a, b) \in R$ if and only if $a = b$. This relation R is called the **equality relation** between the elements of A.

Example 11.5. If $A = \{1, 4, 5\}$, then the relation $a < b$ („is less than”) for the set A can written as relation $R = \{(1, 4), (1, 5), (4, 5)\}$.

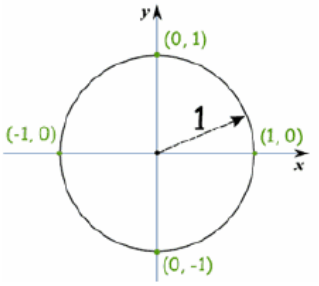
How to describe this relation if A is the set of all integers $\mathbb{Z}$? Relation $<$ („less”) on the set of integers can be presented as the set $R = \{(x, y) \colon x, y \in \mathbb{Z} \wedge y - x \in \mathbb{N}\}$, which tells that (x, y) is in the relation if $y - x$ is a positive integer, or in short $x < y$.

Let $A = \mathbb{R}$. How do we present or write the same relation $R = \{(x, y) \colon x < y\}$ for the set of real numbers? This case presents a set of points on a plane and it is visualized on the next graph.



Example 11.6. On the set of all straight lines on a plane S we can talk of a relation $s \parallel t$, which means that lines s and t are parallel. We can also talk of a relation $s \perp t$, in which line s is perpendicular to t.

Example 11.7. Let $A = B = \mathbb{R}$, $R = \{(x, y) \colon x^2 + y^2 = 1\}$. Relation R is the set of all points on a circle (the circle is centered at the origin and its radius is 1).



Example 11.8. Let K be the set of all students registered for the course „Transition to Advanced Mathematics". One relation on this set K is $xRy \Leftrightarrow$ student x is sympathetic towards student y. Therefore, relation R is the set of students sympathetic towards each other.

Example 11.9. Let M be the set of all people living on Earth. Then aRb, if people a and b have the same parents.

Example 11.10. Functions as relations. Let $f \colon X \to Y$ be a function. Define $R = G(f)$, i,e., xRy if and only if $(x, y) \in G(f) = \{(x, f(x)) \colon x \in X\}$. In other words, the graph of function f is a relation between sets X and Y.

The last example justifies the mindset that relations are a generalization of functions. In literature a function is often defined as follows.

Definition 11.11. Let X and Y be sets. Relation $R \subset X \times Y$ is called a **function**, if the following conditions are satisfied

1. for all $x \in X$ there exist a $y \in Y$ such that $(x, y) \in R$
2. if $x \in X$ and $y, z \in Y$ are such that $(x, y) \in R$ and $(x, z) \in R$, then $y = z$.

From now on we think of functions as specific relations. Based on the new definition of functions we now give similar definitions of injectivity and surjectivity.

Definition 11.12. Let $R \subset X \times Y$ be a function. Then R is

1. **injective**, if $x_1, x_2 \in X$ and $y \in Y$ are such that $(x_1, y) \in R$ and $(x_2, y) \in R$, then $x_1 = x_2$.
2. **surjective**, if for all $y \in Y$ there exists an $x \in X$ such that $(x, y) \in R$.

Exercise 11.13. Let the set of integers $\mathbb{Z}$ have the next relations:

$$R_1 = \{(a, b) \colon a \leq b\}, \qquad R_4 = \{(a, b) \colon a = b\},$$
$$R_2 = \{(a, b) \colon a > b\}, \qquad R_5 = \{(a, b) \colon a = b + 1\},$$
$$R_3 = \{(a, b) \colon a = b \vee a = -b\}, \qquad R_6 = \{(a, b) \colon a + b \leq 3\}.$$

Which relations contain the pairs $(1, 1), (1, 2), (2, 1), (1, -1)$ and $(2, 2)$?

Solution. Pair $(1, 1)$ belongs to relations R_1, R_3, R_4 and R_6. Pair $(1, 2)$ belongs to relations R_1 and R_6. Pair $(2, 1)$ belongs to relations R_2, R_5 and R_6. Pair $(1, -1)$ belongs to relations R_2, R_3 and R_6. Pair $(2, 2)$ belongs to relations R_1, R_3 and R_4. □

Exercise 11.14. How many different relations can a set of n elements have?

Solution. A relation on set A is a subset of $A \times A$. If set A has n elements, then its Cartesian product has n^2 elements. Previously we saw that if a set has m elements, then it has 2^m subsets. Therefore, the set $A \times A$ has 2^{n^2} subsets and thus the same amount of relations. For example, set $\{a, b, c\}$ has $2^{3^2} = 2^9 = 512$ relations. □

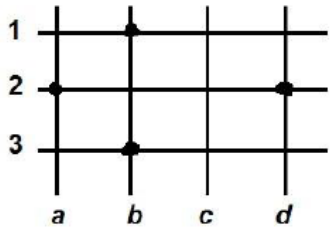
11.2 Representing relations

We can represent relations in several different ways:

1. If A and B are finite sets and do not have that many elements, then we can just list the elements which belong to relation R (check example 11.2). A relation can also be presented as a table. The relation R_1 in example 11.2 has the following table:

A	2	2	3	3
B	2	3	1	5

2. If we present the Cartesian product $A \times B$ as a rectangle, then any relation between A and B can be drawn as any figure of our liking in that rectangle. This also applies to all functions, for example the graph of $y = x^2$ is a subset of an „unbound" rectangle $\mathbb{R} \times \mathbb{R}$. For finite sets A and B we can just draw a collection of squares instead of a rectangle, where we mark down the knots which match the pairs of elements in our relation. The next graph displays the relation $R = \{(a, 2), (b, 1), (b, 3), (d, 2)\}$ between sets $A = \{a, b, c, d\}$ and $B = \{1, 2, 3\}$.



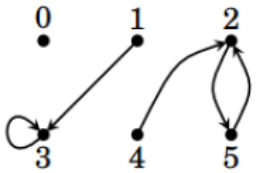
3. **Matrix representation**. Let $A = \{a_1, \ldots, a_n\}$ and $B = \{b_1, \ldots, b_m\}$ be finite sets and R be a relation between A and B. Let us put relation R into a correspondence with matrix $M_R = (m_{ij})$, where $m_{ij} = 1$, if $(a_i, b_j) \in R$ and $m_{ij} = 0$, if $(a_i, b_j) \notin R$, where $i = 1, \ldots, n$ and $j = 1, \ldots, m$.

   For example, if $A = \{a, b, c, d\}$ and $B = \{1, 2, 3\}$ and $R = \{(a, 2), (b, 1), (b, 3), (d, 2)\}$. Then

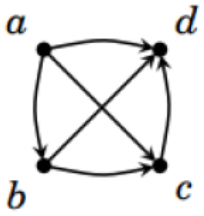
$$M_R = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$$

   It is simple to see that this matrix representation is basically the same as our „square" representation from the last point. Sometimes it is easier to check the properties of a relation when it is represented as a matrix.

4. Relations can also be represented as directed graphs. The next graph visualizes the relation R between the elements of $A = \{0, 1, 2, 3, 4, 5\}$, where $(a, b) \in R$ is represented by an arrow from a to b. If an element is in a relation with itself, then this is represented using an arrow from the point a back to itself. Let us have the example $R = \{(1, 3), (2, 5), (3, 3), (4, 2), (5, 2)\}$.



Often graphical representation gives us a good overview of a relation. For example relation R on a set $A = \{a, b, c, d\}$, where xRy, if x is before y in the alphabet, can be expressed as the set $R = \{(a, b), (a, c), (a, d), (b, c), (b, d), (c, d)\}$ and as the following graph.



5. We already mentioned before that we can describe a relation in words, by some property or condition, formula etc.

11.3 Properties of relations

We will now introduce the vocabulary needed to describe and classify relations.

Definition 11.15. A relation R on set A is said to be

(a) **reflexive**, if $(a, a) \in R$ for every element $a \in A$;

(b) **irreflexive**, if $(a, a) \notin R$ for every element $a \in A$;

(c) **symmetric**, if $(b, a) \in R$ whenever $(a, b) \in R$, for all $a, b \in A$;

(d) **antisymmetric**, if $(a, b) \in R$ and $(b, a) \in R$ for all $a, b \in A$, then $a = b$;

(e) **transitive**, if $(a, b) \in R$ and $(b, c) \in R$ for all $a, b, c \in A$, then $(a, c) \in R$.

Example 11.16. Let $A = \{1, 2, 3\}$ and let A have the relations $R_1 = \{(1, 1), (2, 1), (2, 2), (3, 3)\}$ and $R_2 = \{(1, 1), (2, 1), (1, 2), (3, 3)\}$. Relation R_1 is reflexive, because it contains all the pairs that have the form (a, a); more specifically $(1, 1), (2, 2)$ and $(3, 3)$. Relation R_2 is not reflexive, because it does not contain the pair $(2, 2)$. Relation R_2 is also not irreflexive, because it contains pairs $(1, 1)$ and $(3, 3)$.

Remark. The terms symmetric and antisymmetric are not opposites of each other, because a relation can either have both or neither of them. Likewise the terms reflexive and irreflexive are also not opposites of each other.

Exercise 11.17. Is the divisibility relation on the set of natural numbers reflexive? Symmetric? Antisymmetric?

Solution. Because $a|a$ for any natural number a, then the divisibility relation is reflexive. The divisibility relation is not symmetric on the set of natural numbers, because $1 \mid 2$, but $2 \nmid 1$. The divisibility relation is antisymmetric on the set of natural numbers, because if $a \mid b$ and $b \mid a$ for all $a, b \in \mathbb{N}$, then $a = b$. □

Exercise 11.18. Prove that if a relation is both symmetric and antisymmetric, then it is transitive.

Example 11.19. Relation $<$ („less“) on the set of real numbers is irreflexive, antisymmetric and transitive. Relation $\leq$ on set $\mathbb{R}$ is reflexive, antisymmetric and transitive.

Example 11.20. The relation of parallel lines $s \parallel t$ is symmetric and transitive but it is not reflexive, because a straight line cannot be parallel to itself (why?). The relation of parallel lines is also irreflexive. This relation does not have any other property defined above. The relation of lines being perpendicular $s \perp t$ is irreflexive and symmetric but not transitive.

Example 11.21. Let us take a look at $X = \mathcal{P}(E)$, the set of all subsets of set E, and the inclusion relation $\subset$ on set X. This relation is reflexive, antisymmetric and transitive.

Example 11.22. Let $A = \{a, b, c, d\}$ and $R = \{(a, a), (a, b), (b, a), (b, c)\}$. Relation R has none of properties described in definition 11.15.

Exercise 11.23. Let A be a set. Which properties do the universal relation $R = A \times A$ and empty relation $S = \emptyset$ have?

Exercise 11.24. Which of the properties described in definition 11.15 does the equality relation have?

Exercise 11.25. Give an example of a relation which is symmetric and transitive but not reflexive.

11.4 Inverse relation

Definition 11.26. The **inverse relation** of relation $R \subset A \times B$ is the relation $R^{-1} \subset B \times A$, which is determined by the equivalence $bR^{-1}a \Leftrightarrow aRb$ or $R^{-1} = \{(b, a) \colon (a, b) \in R\}$.

The upper index „-1“ here is just a convenient notation.

Every relation has an inverse. If R is a relation on A, then so is R^{-1}. It is easy to see $(R^{-1})^{-1} = R$, this means that the inverse of an inverse relation is the initial relation (Check this!).

Example 11.27. If $R = \{(1, 5), (2, 6), (3, 7), (3, 8)\}$, then $R^{-1} = \{(5, 1), (6, 2), (7, 3), (8, 3)\}$.

Example 11.28. Let $A = B = \mathbb{R}$ and R be the strict ordering relation $<$ on real numbers, this means that $R = \{(x, y) \colon x < y\}$. Then $R^{-1} = \{(y, x) \colon (x, y) \in R\} = \{(y, x) \colon y > x\}$, or in short the inverse of relation $<$ is $>$.

Example 11.29. Let $A = B = \mathbb{R}$ and I be the **identity relation** on real numbers, this means that $I = \{(x, y) \colon x = y\}$. Then $I^{-1} = \{(y, x) \colon (x, y) \in I\} = \{(y, x) \colon y = x\}$, this means that the inverse of the identity relation is the relation itself.

Proposition 11.30. *If relation R is reflexive, transitive, symmetric or antisymmetric, then its inverse relation R^{-1} has the same properties.*

Proof. Independent work! □

Exercise 11.31. Show that a relation R on set A is symmetric if and only if $R = R^{-1}$.

We will now answer the question **when is the inverse relation of a function also a function**? Remember that a relation $R \subset X \times Y$ is a function, if

1. for all $x \in X$ there exist a $y \in Y$ such, that $(x, y) \in R$
2. if $(x, y) \in R$ and $(x, z) \in R$ for all $x \in X$ and $y, z \in Y$, then $y = z$.

The inverse relation of a function R is $R^{-1} = \{(y, x) \colon (x, y) \in R\} \subset Y \times X$. When is R^{-1} a function? For this

1. we want that for all $y \in Y$ there is an $x \in X$ such, that $(y, x) \in R^{-1}$ or in short $(x, y) \in R$. Hence R has to be a **surjective** function.
2. we want that if $(y, x_1) \in R^{-1}$ and $(y, x_2) \in R^{-1}$ for all $y \in Y$ and $x_1, x_2 \in X$, then $x_1 = x_2$. Or, if $(x_1, y) \in R$ and $(x_2, y) \in R$, then $x_1 = x_2$. Hence R has to be **injective**.

We see that for an inverse relation R^{-1} to be a function the relation R has to be a **bijective function**. Therefore, we have proved the next proposition.

Proposition 11.32. *Let $R \subset X \times Y$ be a function. Then R is bijective if and only if its inverse relation R^{-1} is a function. Even more, inverse relation R^{-1} is the inverse of function R.*

11.5 Equivalence relations

Let A be an arbitrary nonempty set.

Definition 11.33. Relation R on set A is called an **equivalence relation**, if it is

(a) reflexive, that is to say aRa for all $a \in A$;

(b) symmetric, that is to say if aRb, then bRa;

(c) transitive, that is to say if aRb and bRc, then aRc.

If R is an equivalence relation and aRb, then we say that elements a and b are **equivalent** (by relation R). We often use the notation $a \sim b$ to denote the fact that elements a and b are equivalent with respect to a particular equivalence relation.

Example 11.34. Equality relation $aRb \Leftrightarrow a = b$ is clearly an equivalence relation on A. It is the identity relation $R_A = I = \{(a, a) \colon a \in A\}$ which we sometimes call the diagonal of A^2. Identity relation or equality relation is the smallest equivalence relation, because it is a subset of every other equivalence relation (as a reflexive relation). The relation $U = A \times A$ is also an equivalence relation on A (so called universal relation). Relations I and U are called the **trivial relations** on set A.

Example 11.35. Congruence of figures (or objects) in geometry is an equivalence relation on the set of all figures on a plane. The similarity relation of triangles (or polygons) is also an equivalence relation. Note that in this case we use the notation $\triangle ABC \sim \triangle DEF$.

Example 11.36. The collinearity or complanarity of vectors are also equivalence relations.

Example 11.37. Congruence on the set of integers $\mathbb{Z}$ is also an equivalence relation. Let $m > 0$ for a fixed natural number. Integers a and b are **congruent modulo** m, if the difference $a - b$ is divisible by m, and we write $a \equiv b \pmod{m}$.
For example, $25 \equiv 11 \pmod{7}$ and $21 \equiv 13 \pmod{4}$.

Exercise 11.38. Show that if an equivalence relation is antisymmetric, then it is an equality relation or in other words an identity relation.

11.6 Equivalence classes and partitions

Every equivelence relation $R \subset A \times A$ allows us to split A into so called equivalence classes.

Definition 11.39. Let R be an equivalence relation on a set A. The **equivalence class** of element $a \in A$ is the subset $[a]_R$ of set A, which consists of all elements of A which are in relation with a with respect to R, that is to say of elements which are equivalent to a: $[a]_R = \{x \colon x \in A \text{ ja } aRx\}$.

Hence, $x \in [a]_R$ means that aRx and also xRa because of the symmetry of relation R. Reflexivity gives us $a \in [a]_R$.

The set of equivalence classes has several important properties. To study these properties, we introduce the next concept.

Definition 11.40. We say that there is a partition $K = \{K_i \colon i \in I\}$ of set A, if

1. $K_i \neq \emptyset$ for all $i \in I$;
2. every two different sets are non overlapping, i.e, for every $i, j \in I$ from $K_i \neq K_j$, it follows that $K_i \cap K_j = \emptyset$;
3. set A equals the union of subsets K_i, i.e, $A = \bigcup_{i \in I} K_i$.

Sets K_i, $i \in I$, are called the K **classes** of the partition.

In other words a partition of set A splits the set into non overlapping nonempty subsets which form a system of sets K. Generally I can be an arbitrary set of indices (finite or infinite).

Example 11.41. Let G be the set of all students that go to a particular gymnasium and let K_{10}, K_{11} and K_{12} respectively be the sets of all students in tenth grade, eleventh grade and twelfth grade. System $\{K_{10}, K_{11}, K_{12}\}$ is a partition of G.

Example 11.42. All the one element subsets of A, $\{a\colon a \in A\}$, form a partition on set A, because $\{a\} \neq \emptyset$, $\bigcup_{a\in A}\{a\} = A$, and from $\{a\} \neq \{b\}$ (i.e. $a \neq b$) it follows that $\{a\} \cap \{b\} = \emptyset$. This is the finest partition of A.

Example 11.43. A partition consisting of just one set A, $\{A\}$, is the coarsest partition of A.

Example 11.44. If $A = \mathbb{R}$, then one partition consists of all $K_i = [i, i+1)$, $i \in \mathbb{Z}$. (Check that all the conditions are met!)

Partitions $\{K_i\}$ and $\{L_j\}$ of set A are considered equal if for every K_i there exists an L_j such that $L_j = K_i$, and in reverse, if for every L_j there exists a K_i such that $K_i = L_j$.

Proposition 11.45. *Partitions $K = \{K_i\colon i \in I\}$ and $L = \{L_j\colon j \in J\}$ coincide if for every K_i there exists an L_j such that $L_j = K_i$.*

Proof. Pick an arbitrary L_j. Let $a \in L_j$. Because $a \in A$, then due to $A = \bigcup_{i\in I} K_i$, there exists a K_i such that $a \in K_i$. Now pick an $L_{j'}$ such that $L_{j'} = K_i$. Then $a \in L_j \cap L_{j'}$, hence $L_j \cap L_{j'} \neq \emptyset$. From this it follow that $L_j = L_{j'}$, i.e. $K_i = L_j$. □

Now we will show that there is an one-to-one correspondence between a set's equivalence relations set and its partitions set (in the sense that to every equivalence relation corresponds one partition and conversely, if we take an equivalence relation of a equivalence relation's partition, then this equivalence relation matches the partition's original equivalence relation).

Theorem 11.46.

1. *Let R be an arbitrary equivalence relation on set A. Then the system of equivalence classes $\{[a]_R\colon a \in A\}$ is a partition of A.*
2. *Conversely, if $K = \{K_i\colon i \in I\}$ is a partition of A, then the relation R, where aRb means that a and b belong to the same class (some set K_i), is an equivalence relation on A.*

Proof.

1. We show that $\{[a]_R\colon a \in A\}$ is a partition of A. Indeed, aRa for all $a \in A$ due to the reflexivity of R, this means that $a \in [a]_R$ for every $a \in A$. Thus none of the classes of our partition are empty and each element is in at least one class $[a]_R$. The last claim also means that $a \in \bigcup_{a\in A}[a]_R$ for all $a \in A$, that is to say $A \subset \bigcup_{a\in A}[a]_R$. Since the opposite inclusion $A \supset \bigcup_{a\in A}[a]_R$ is obvious (why?), we have proven that $A = \bigcup_{a\in A}[a]_R$. Thus the third condition from the definition of a partition holds. For the second condition we show that if $[a]_R \cap [b]_R \neq \emptyset$, then $[a]_R = [b]_R$. For this we take two subsets $[a]_R$ and $[b]_R$, where $a, b \in A$, and element c from their intersection: $c \in [a]_R \cap [b]_R$. Because $c \in [a]_R$, we get cRa, and because $c \in [b]_R$, we have cRb. Since R is symmetric, then cRa implies aRc. Now aRc and cRb, hence aRb because R is transitive. Let x be an arbitrary element of $[a]_R$. Then xRa. Because aRb, then xRb due to the transitivity of relation R. That is to say that $x \in [b]_R$ or $[a]_R \subset [b]_R$. A similar discussion gives $[b]_R \subset [a]_R$. Thus $[a]_R = [b]_R$. In conclusion we have shown that the system of equivalence classes $\{[a]_R\colon a \in A\}$ is a partition on the set A.

2. Let there be a partition $K = \{K_i \colon i \in I\}$ on set A. Let us define the relation R, where aRb, if a and b are part of the same class, or $aRb \Leftrightarrow \exists i \in I\ (a \in K_i \wedge b \in K_i)$. We show that this relation is an equivalence relation. Relation R is reflexive: for all $a \in A$ we have aRa since $A = \bigcup_{i \in I} K_i$ and because a has to belong to at least one K_i due to $a \in A$. Relation R is symmetric: if aRb, i.e., $\exists i \in I\ (a \in K_i \wedge b \in K_i)$, then also $b \in K_i \wedge a \in K_i$, that is to say bRa. Relation R is transitive: if aRb and bRc for $a, b, c \in A$, then according to the definition of R there have to exist $i, j \in I$ such that $a \in K_i$ and $b \in K_i$ but also $b \in K_j$ and $c \in K_j$. Since $b \in K_i \cap K_j$, then we get from the second condition of partition's definition that $K_i = K_j$. Thus $a, c \in K_i$ from which aRc. To conclude, we have shown that R is reflexive, symmetric and transitive, thus it is an equivalence relation.

□

Let us take a look at previous examples of equivalence relations and partitions and find their corresponding partitions and equivalence relations.

Example 11.47. A corresponding partition of an equality relation of A consists of all sets $[a]_R = \{b \colon b \in a \wedge bRa\} = \{b \in A \colon b = a\} = \{a\}$. Thus equality relation has the narrowest partition $\{\{a\} \colon a \in A\}$.

Example 11.48. Observe a single set partition $\{A\}$ of set A. The corresponding equivalence relation R is $aRb \Leftrightarrow a \in A \wedge b \in A \Leftrightarrow (a, b) \in A \times A$. Hence for this case $R = U = A \times A$, that is to say that for the widest partition $\{A\}$ corresponds the widest equivalence relation, universal relation $A \times A$.

In the last chapter we said that two sets A and B are equivalent and used the notation $A \sim B$, if there exists a bijection from set A to set B. The use of word „equivalent" is justified, because the equivalence of sets has all the properties of an equivalence relation: reflexivity, symmetry and transitivity (check proposition 10.11).

Based on proposition 10.11 we can split sets into equivalence classes, where every class is made of sets equivalent to each other or of same cardinality, and sets of different classes are not equivalent. An equivalence class of set A contains all sets equivalent to A. It is important to note we cannot count equivalence classes as sets, because this would introduce many set theoretical paradoxes.

Definition 11.49. The **cardinality** of a set is its equivalence class of relation $\sim$.

Because the equivalency of sets is an equivalence relation, then for a fixed set X all of its subsets distribute into nonoverlapping classes of sets which are equivalent among themselves. The equivalence class of empty set just contains $\emptyset$, then there is the class of single element subsets $\{a\}, \{b\}, \ldots$, then the class of two element subsets etc. The corresponding equivalence class is called the cardinality of the set.

11.7 Quotient set

Definition 11.50. Let R be an equivalence relation on A. The set that consists of all the possible classes of the partition that corresponds to relation R, is called **the quotient set of set A by equivalence relation** R and is denoted by A/R.

Therefore, $A/R = \{[a]_R \colon a \in A\}$. Note that for different elements the corresponding equivalence classes can coincide, that is to say $[a]_R = [b]_R$ for $a \neq b$. Only one member is taken from equivalent classes to be the element of the factor set.

Example 11.51. If we take the equality relation I of A, then $A/R = \{\{a\} \colon a \in A\}$.

Example 11.52. We consider two points $x = (x_1, x_2)$ and $y = (y_1, y_2)$ of plane $X = \mathbb{R}^2$ equivalent, if they happen to be on the same vertical line. Then $[x] = \{y \in X \colon y_1 = x_1\}$ is the set of all points, which happen to be on the exact same vertical line as x, in other words it is the vertical line which goes trough the point x. The factor set X/R in this case consists of all vertical lines.

If R is the same directness relation on A, the set of lines of a plane (or a space), then the corresponding factor set's elements are concrete directions.

Example 11.53. If R is the relation of equality of vectors, $\vec{u} = \vec{v}$, then every equivalence class consists of vectors of same length and direction, which are seen as one and same vector. Therefore, the factor set consists of free vectors.

11.8 Ordering relation

Definition 11.54. Relation R on set A is called an **ordering relation**, if it is

(a) reflexive, that is to say aRa for all $a \in A$;

(b) antisymmetric, that is to say if aRb and bRa, then $a = b$;

(c) transitive, that is to say if aRb and bRc, then aRc.

If R is an ordering relation, then instead of aRb we use $a \leq b$ or equivalently $b \geq a$. We say that a **precedes** element b or b **succeeds** element a.

Exercise 11.55. Prove that if R is an ordering relation, then R^{-1} is also an ordering relation.

Definition 11.56. A set which has been given an ordering relation is called a **partially ordered set (poset)**.

If a set A has an ordering relation R, then we usually denote this as a pair (A, R). For example, $(\mathbb{R}, \leq)$ and $(\mathcal{P}(\{1\}), \subset)$ are partially ordered sets.

Definition 11.57. A partially ordered set is said to be a **linearly ordered set**, if for every pair of elements a and b either $a \leq b$ or $b \leq a$, that is to say that two arbitrary elements are comparable.

Example 11.58.

1. The inequality relation $\leq$ on the set of real numbers $\mathbb{R}$ is linearly ordered, because every two numbers are comparable.

2. The inclusion relation $\subset$ on $\mathcal{P}(X)$, the set of all subsets of X, is an ordering relation, but it is not linear, because two sets $A, B \subset X$ may not be comparable. Make a drawing of this!

3. Divisibility relation on the natural numbers set $\mathbb{N}$ is an ordering relation, but it is not linear.

Example 11.59. For alphabet $\{a_1, \ldots, a_n\}$ we define order $a_1 < a_2 < \cdots < a_n$. On the set of words we define order

$$\begin{aligned}(x_1, \ldots, x_m) < (y_1, \ldots, y_l) \Leftrightarrow (x_1 < y_1) \vee (x_1 = y_1 \wedge x_2 < y_2) \vee \\ \vee (x_1 = y_1 \wedge x_2 = y_2 \wedge x_3 < y_3) \vee \\ \vee (x_1 = y_1 \wedge \ldots x_m = y_m \wedge m < l).\end{aligned}$$

This order is called **alphabetic** or **lexicographic**, it is linear and sees use in dictionaries.

Exercise 11.60. Let A be the set of all functions defined over interval $[a, b]$, $f\colon [a, b] \to \mathbb{R}$. Define relation $f \leq g \Leftrightarrow f(x) \leq g(x)$ for all $x \in [a, b]$. Show that is is an ordering relation. Is this relation linear?

Often you will also see the strict ordering relation $<$, which based on the relation $\leq$ is defined as: $x < y \Leftrightarrow x \leq y$ and $x \neq y$.

Definition 11.61. Element a_0 of a partially ordered set A is said to be **smallest** or **first**, if $a_0 \leq a$ for all $a \in A$. Analogically, element $a_0 \in A$ is said to be **largest** or **last**, if $a \leq a_0$ for all $a \in A$.

Example 11.62.

1. The smallest element of $\mathbb{N}$ by natural order is 1, but it does not have a largest element.
2. Interval $(0, 1)$ of real numbers does not have a smallest or a largest element.
3. Set $\mathcal{P}(X)$ by inclusion order has both a smallest and a largest element, they are respectively $\emptyset$ and X.

Proposition 11.63. *A partially ordered set has no more than one smallest element and no more than one greatest element.*

Proof. Let a_0 and a_1 be the smallest elements. Then $a_0 \leq a_1$, because a_0 is a smallest element. Also $a_1 \leq a_0$, because a_1 is a smallest element. Because partial ordering is antisymmetric, then $a_0 = a_1$. The proof for greatest element is analogous. □

Definition 11.64. Element a_0 of a partially ordered set A is called **minimal**, if from $a \leq a_0$ and $a \in A$ follows $a = a_0$ (that is to say there are no elements smaller than a_0 in A). Analogically, element a_0 is called **maximal**, if from $a_0 \leq a$ and $a \in A$ follows $a = a_0$ (that is to say there are no elements greater than a_0 in A).

From definitions we see that the main difference between the smallest element and a minimal element is that for the smallest element we require all other elements to be comparable to it, but we do ask this of the minimal element.

Example 11.65.

1. The set of real numbers when it comes to its natural ordering does not have minimal or maximal elements.

2. The partially ordered set $(\{1, 2, 3, 4\}, |)$ has 1 as its smallest element (also minimal), maximal elements are 3 and 4, but it has no greatest element.

Proposition 11.66. *The smallest element of a partially ordered set is also its only minimal element, and the greatest element of this set is also its only maximal element.*

Proof. Let $a_0 \in A$ be the smallest element, that is to say $a_0 \leq a$ for all $a \in A$. If for some $b \in A$ holds $b \leq a_0$, then $b = a_0$ due to the antisymmetry of the ordering relation, which means that a_0 is a minimal element.
Finally we make certain that this element is unique. If there exists another minimal element $a_1 \in A$, then $a_0 \leq a_1$ because a_0 is the smallest element. Condition $a_0 \neq a_1$ tells us that a_1 is not a minimal element, thus $a_0 = a_1$. □

Proposition 11.67. *In a linearly ordered set the minimal element is also the smallest element and the maximal element is also the largest element.*

Proof. Let a_0 be the minimal element of a linearly ordered set A, that is to say if $a \leq a_0$ for all $a \in A$, then $a = a_0$. We will show that $a_0 \leq a$ for all $a \in A$. Assume the opposite, i.e., that there exists an $a_1 \in A$ for which $a_0 \leq a_1$ does not hold. Since the ordering is linear either $a_0 \leq a_1$ or $a_1 \leq a_0$ has to be true, hence $a_1 \leq a_0$ has to hold. Therefore $a_1 \neq a_0$, because otherwise $a_0 \leq a_1$. Now we have that $a_1 \neq a_0$ and $a_1 \leq a_0$, which leads to a contradiction with our assumption that a_0 is minimal. □

Propositions 11.66 and 11.67 lead us to the following result.

Corollary 11.68. *For linearly ordered sets the definitions of minimum and smallest element coincide. Same applies to the definitions of greatest and maximal element.*

A finite partially ordered set can be presented as a **Hasse diagram**. For this we need to go through the next steps:

1. Represent the ordering relation $(R, \leq)$ as a directed graph.

2. Because the ordering relation is reflexive, then every point (a, a) has a loop. Remove these loops.

3. Next remove all edges which have to be there due to transitivity. Remove all the edges (a, c) for which there exists $b \in R$ such that $a \leq b$ and $b \leq c$.

4. Put the edges so that that the graph's initial node is below the end node.

5. Remove all directions because all edges are already directed upwards.

Figure 1.1 is a step-by-step explanation on how to create a Hasse diagram.

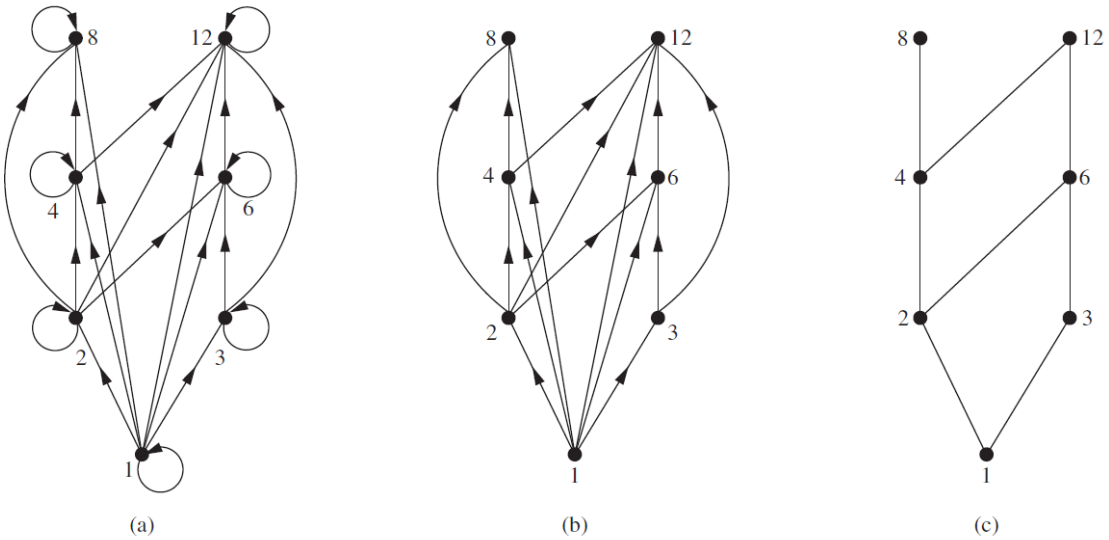


Figure 11.1: Hasse diagram of partially ordered set $(\{1, 2, 3, 4, 6, 8, 12\}, |)$

Let us consider part c) of Figure 11.1 (the Hasse diagram). Hasse diagrams are useful because they makes it possible to easily find minimal and maximal elements. This is because the lowest elements are minimal and the highest elements are maximal. For example we see that the smallest (and thus minimal) element is 1 and the maximum elements are 8 and 12 but there is no greatest element.

Bibliography

***

[1] R. Hammack, *Book of proof*, Virginia Commonwealth University, 2013

[2] M. Kilp, *Algebra I*, Eesti Matemaatika Selts, Tartu, 2005

[3] V. Laan ja L. Tart, *Arvuteooria loengukonspekt*, TÜ, 2017

[4] P. Oja, *Hulgateooria*, TÜ Kirjastus, 2006.

[5] K. Rosen, *Discrete mathematics and its applications*, Boston, McGraw-Hill, 2012.