Intro to proofs

Lochverstärker#5585

March 21, 2022

Contents

0 Basics

0.1 Natural numbers and integers

We begin with a small revision about natural numbers.[1]
We will use the symbol $\mathbb{N}$ to denote the natural numbers, so

$$\mathbb{N} := \{1, 2, 3, 4, \dots\}.$$

The colon to the left of the equals sign in the above line means that the *left* side, so the symbol $\mathbb{N}$, is being *defined* by the right side. This of course means that we already have to know the right side, so the *set* $\{1, 2, \dots\}$.
We will further use the symbol $\mathbb{N}_0$ to denote the set

$$\mathbb{N}_0 := \{0, 1, 2, 3, \dots\}$$

and the symbol $\mathbb{Z}$ to denote the integers

$$\mathbb{Z} := \{\dots, -2, -1, 0, 1, 2, \dots\}.$$

It should be noted that all these definitions have to be treated carefully, as it is not exactly clear what "..." is supposed to mean.

Definition 0.1.1. An integer n *divides* the integer m if there is a natural number k such that $nk = m$. In this case we call n a *divisor* of m and denote it $n \mid m$. Otherwise n is not a divisor of m and we write $n \nmid m$.

Example 0.1.2. We have

- $2 \nmid 3$
- $2 \mid 4$
- $0 \mid 0$
- $0 \nmid z$ for all integers $z \neq 0$ and
- $z \mid 0$ for all integers z.

Definition 0.1.3. Integers that are divisible by 2 will be called *even* numbers. All other integers will be called *odd* numbers.

Definition 0.1.4. We will call a natural number n *prime* if it is not 1 and only divisible by ± 1 and $\pm n$. We will denote by $\mathbb{P}$ the set of prime numbers.

[1] What natural numbers are should be intuitively clear. We will take the easy way here by only treating them naively. In reality, it takes some time to rigorously define the natural numbers, but we will not concern ourselves with that in this introduction.

Example 0.1.5. The number 2 is prime. As $2 \nmid 3$, the number 3 is prime as well. The number 4 is not prime because $4 = 2 \cdot 2$.

The prime numbers are of fundamental importance in mathematics, but we only require them to discuss examples in the following sections.

0.2 Inequalities and estimates

The reader is probably familiar with equations, but inequalities appear frequently as well. We will therefore revise important rules for dealing with them as well as some techniques for estimation. The variables in the following section are to be understood as real numbers (or more general: as elements of an ordered field).

We will refrain from defining the symbols $\leq, <, \geq, >$ and instead treat them as known.[2]

Definition 0.2.1. We will understand a *chain of inequalities* to be an inequality of the form

$$a_1 < a_2 < a_3 < \cdots < a_n.$$

This chain of inequalities is satisfied if and only if all inequalities

$$a_1 < a_2 \text{ and } a_2 < a_3 \text{ and } \ldots \text{ and } a_{n-1} < a_n$$

are satisfied all at once.

Theorem 0.2.2. *We have*

- *The inequalities*
$$a < b \text{ and } a + c < b + c$$
are (logically) equivalent (more on what that means in the next section).
- *For positive c the inequalities*
$$a < b \text{ and } ca < cb$$
are equivalent.
- *For negative c the inequalities*
$$a < b \text{ and } ca > cb$$
are equivalent.

Analogous results are true for weak inequalities (i.e. $\leq$ instead of $<$).

[2] In fact it is not that simple to give a rigorous definition of e.g. $<$; although it would be possible to define that $a < b$ means that $b - a$ is positive, this presents the problem of defining what *positive* means. This problem will be solved in an introduction to Analysis.

Theorem 0.2.3. *From*

$$a < b \text{ and } c < d$$

it follows that

$$a + c < b + d.$$

If both inequalities are weak, the resultant inequality is as well.
In short: Inequalities "going in the same direction" may be added.

Theorem 0.2.4. *The assertion $ab > 0$ holds if and only if a and b are both positive or both negative. The assertion $ab < 0$ holds if and only if exactly one of the variables is positive and the other negative.*

Corollary 0.2.5. [3] *If $a \neq 0$, then $a^2 > 0$. In particular $1 > 0$.*

Theorem 0.2.6. *If*

$$0 < a < b \text{ and } 0 < c < d,$$

it follows that

$$0 < ac < bd.$$

Analogously for weak inequalities.
In short: Inequalities "going in the same direction" may be multiplied if all terms are positive.

Theorem 0.2.7. *A fraction with positive numerator and positive denominator can be increased by*

- *Increasing the numerator or*
- *Decreasing the denominator and keeping it positive.*

Example 0.2.8. (a) The *Complex Numbers* $\mathbb{C}$ are the result of adding an element i to the real numbers that satisfies the equation $i^2 = -1$ and then extending the basic arithmetic operations to this element.

In $\mathbb{C}$ inequalities cannot be reasonably defined. We say that $\mathbb{C}$ *can't be ordered*.

Because due to corollary 0.2.5, we'd have $-1 = i^2$ and $1 = 1^2$ positive and thus

$$-1 > 0 \text{ and } 1 > 0.$$

But with theorem 0.2.3 we then get $0 > 0$, a contradiction.

(b) If $b, d > 0$ and $\frac{a}{b} < \frac{c}{d}$, then $\frac{a}{b} < \frac{a+c}{b+d} < \frac{c}{d}$.

We will show that the first $<$ symbol is correct: The term $b(b + d)$ is positive, therefore the inequalities

$$\frac{a}{b} < \frac{a+c}{b+d} \text{ and } a(b+d) < (a+c)b$$

[3] A corollary (from latin corollarium – present, gratuity) is a (usually simple) consequence of a mathematical result

are equivalent. Expanding yields

$$ab + ad < ab + bc, \text{ therefore } ad < bc.$$

Multiplying with the positive number $\frac{1}{bd}$ yields

$$\frac{a}{b} < \frac{d}{c}.$$

The inequality $\frac{a}{b} < \frac{a+c}{b+d}$ is therefore equivalent to the initial inequality $\frac{a}{b} < \frac{c}{d}$, which was assumed true and therefore also true.

One can prove the second inequality analogously.

(c) For all natural numbers n the inequality

$$\frac{3n-6}{n^2+2n+3} \leq \frac{3}{n}$$

holds. Because we have

$$\frac{3n-6}{n^2+2n+3} \overset{\text{increasing numerator}}{\leq} \frac{3n}{n^2+2n+3} \overset{\text{decreasing denominator}}{\leq} \frac{3n}{n^2} = \frac{3}{n}.$$

1 Propositional logic

Formal logic provides us with the tools to rigorously formulate mathematical statements and also prove them.

1.1 Mathematical statements

A *(mathematical) statement* is a linguistic construct that can reasonably be called *either* true (in short: *t*) *or* false (in short: *f*). This is called the principle of bivalence in mathematical logic.[4] It is not required that you are actually able to tell whether a given statement is true or false.

For example the sentences "Today is Monday" and "Tomorrow is Wednesday" are both statements, that are either true or false depending on when you read this and the sentence "Today is Monday and tomorrow is Wednesday" is always false, but still a statement. The sentence "How is the weather today" is not a statement.
For some sentences it is a bit harder to decide whether they are statements or not. For example, can you tell if "This statement is false" is a mathematical statement in the above sense?

We will often denote statements by capital letters $A, B, C, \ldots$.

Example 1.1.1. We give examples of a few statements of a number theoretic nature. Can you tell which are true?

A: 7 is a prime number.

B: Every prime number is odd.

C: Every number greater or equal to 4 is the product of exactly two prime numbers.

D: Every even number greater or equal to 4 is the sum of exactly two prime numbers.

Here are the solutions:

Statement A is true. Statement B is false, since 2 is even and prime. Statement C is false, since $8 = 2 \cdot 2 \cdot 2$ is the product of three, but not of two prime numbers.
Statement D is known as *Goldbach's conjecture*, which has been unsolved since 1742; nevertheless it is a mathematical statement.

1.2 Operations on statements

One can use *logical operations* on statements to form more complex statements out of simpler ones. When this is done, the truth values of the simpler statements uniquely determine the truth value of the complex statement. The most important logical operations are:

[4] There is also many-valued or even fuzzy logic, but we will not further concern ourselves with that.

- *Conjunction* (*"and"*), denoted $A \wedge B$:

  Example: Let A and B denote the statements given in example 1.1.1, then $A \wedge B$ stands for

  7 is prime and every prime number is odd.

  This is a new statement (and it is false).

  In general the truth value of $A \wedge B$ is defined in terms of the truth values of A and B according to the following table (a so called truth table):

A	B	$A \wedge B$
t	**t**	**t**
t	**f**	**f**
f	**t**	**f**
f	**f**	**f**

The following truth table defines further logical operations, with additional information and examples below it.

A	B	$\neg A$	$A \wedge B$	$A \vee B$	$A \implies B$	$A \iff B$
t	**t**	**f**	**t**	**t**	**t**	**t**
t	**f**	**f**	**f**	**t**	**f**	**f**
f	**t**	**t**	**f**	**t**	**t**	**f**
f	**f**	**t**	**f**	**f**	**t**	**t**

- *Disjunction* (*"or"*), denoted $A \vee B$:[5]

  Example: Consider the statements

  $$C_1 : \text{The number 2 is even}$$

  and

  $$C_2 : \text{The number 2 is prime.}$$

  Then $C_1 \vee C_2$ is a true statement since at least one of C_1, C_2 is true; in fact both are.

- *Negation* (*"not"*), denoted $\neg A$:

  Example: The negation of "2 is not a prime number" is "2 is a prime number".

  Notice that always either A or $\neg A$ is true.

- *Implication* (*"A implies B"*, *"B follows from A"*), denoted $A \implies B$:

  Remark: An implication $A \implies B$ with A false is always true! Ex falso sequitur quodlibet – From falsehood, anything follows.

[5] This is *not* to be understood as an exclusive or.

Example: The statement

If 9 is prime, then Goldbach's conjecture holds

is true, because 9 is not prime (even though we do not know whether Goldbach's conjecture is true).

- *Equivalence* ("*A equivalent to B*", "*A if and only if B*"), denoted $A \iff B$:

  Example: Let q be a natural number. The statements "q is an even prime" and "q is 2" are equivalent. They are either both true (if $q = 2$) or both false (if $q \neq 2$).

Proving tautologies

Using truth tables we can now verify rules of computation for logical statements (so called *tautologies*). For example, we can see that $A \wedge B$ is true if and only if $B \wedge A$ is true. This so called *commutativity* of $\wedge$ is proven by observing the following table

A	B	$A \wedge B$	$B \wedge A$
t	**t**	**t**	**t**
t	**f**	**f**	**f**
f	**t**	**f**	**f**
f	**f**	**f**	**f**

and comparing columns 3 and 4.

The following tautologies are proven in a similar fashion (feel invited to do this!):

- Commutativity:
$$A \wedge B \iff B \wedge A,$$
$$A \vee B \iff B \vee A.$$

- Associativity:
$$A \wedge (B \wedge C) \iff (A \wedge B) \wedge C,$$
$$A \vee (B \vee C) \iff (A \vee B) \vee C.$$

- Distributivity:
$$A \wedge (B \vee C) \iff (A \wedge B) \vee (A \wedge C),$$
$$A \vee (B \wedge C) \iff (A \vee B) \wedge (A \vee C).$$

- Double negation:
$$\neg(\neg A) \iff A.$$

- De Morgan's laws:
$$\neg(A \wedge B) \iff \neg A \vee \neg B,$$
$$\neg(A \vee B) \iff \neg A \wedge \neg B.$$

- Contraposition:
$$(A \implies B) \iff (\neg B \implies \neg A).$$
Remark: Don't mistake contraposition for the inversion of the implication arrow. The statements $A \implies B$ and $(\neg B) \implies (\neg A)$ are logically equivalent, but the statements
$$A \implies B \text{ and } A \impliedby B$$
are in general not related.

- Syllogism:
$$((A \implies B) \wedge (B \implies C)) \implies (A \implies C),$$
$$(A \wedge (A \implies B)) \implies B.$$

- Reformulation of implication:
$$(A \implies B) \iff (\neg A \vee B).$$

- Reformulation of equivalence:
$$(A \iff B) \iff ((A \implies B) \wedge (B \implies A)).$$

1.3 Quantifiers

Mathematical statements often depend on variables. For example the statement
$$A(n)\colon\ n \text{ is greater than } 2n$$
depends on the variable n. Often those variables are defined to be in a certain domain of discourse. To do this, we define a set M and write $n \in M$. We will talk more about this notation later. In the above example we could for instance consider natural numbers (in that case, we would have $M = \mathbb{N}$).

Definition 1.3.1. Let $A(n)$ be a statement that depends on the variable $n \in M$.

(a) We write
$$\forall n \in M\colon A(n)$$
for the statement
$$\text{For all } n \text{ in the set } M \text{ the statement } A(n) \text{ is true.}$$
The statement "$\forall n \in M\colon A(n)$" is therefore true if and only if $A(n)$ is true for every possible value of n in M.
One calls $\forall$ the *universal quantifier*.

(b) We write

$$\exists n \in M\colon A(n)$$

for the statement

There exists an $n \in M$ such that $A(n)$ is true.

The statement "$\exists n \in M\colon A(n)$" is therefore true if and only if there exists at least one $n \in M$ such that $A(n)$ is true.

One calls $\exists$ the *existential quantifier*.

Example 1.3.2. Consider the following statements about integers n and m.

(a) The statement

$$A(n)\colon n \text{ is greater than } 2n$$

is false for all natural numbers n. Because of the bivalence of mathematical logic, $\neg A(n)$ is therefore true for all natural numbers n. So we have

$$\forall n \in \mathbb{N}\colon \neg A(n).$$

(b) The statement

$$B(n)\colon n^2 > n$$

is true for some n, for example for $n = 3$. Therefore we have

$$\exists n \in \mathbb{N}\colon B(n).$$

Remark 1.3.3. When negating a quantified statement, we have to exchange $\forall$ with $\exists$ and vice versa. We have

$$\neg(\forall n \in M\colon A(n)) \iff \exists n \in M\colon \neg A(n).$$

Or in words: If $A(n)$ is not true for all n, then there is at least one n such that $\neg A(n)$ is true.

Analogously we have

$$\neg(\exists n \in M\colon A(n)) \iff \forall n \in M\colon \neg A(n).$$

Or in words: If there is no n, such that $A(n)$ is true, then $\neg A(n)$ is true for all n.

Example 1.3.4. The statement

A: For every natural number m there exists a natural number n such that $n > m$.

can be written more concisely as

$$A\colon \forall m \in \mathbb{N}\colon \exists n \in \mathbb{N}\colon n > m.$$

The statement A is entirely different from the statement

$$B\colon \exists n \in \mathbb{N}\colon \forall m \in \mathbb{N}\colon n > m.$$

The statement B in words is "There exists a natural number n such that for every natural number m the inequality $n > m$ holds".
Exchanging quantifiers can therefore change the truth value of a statement. Statement A is true, statement B is false.
The negation of A is

$$\neg A\colon \exists m \in \mathbb{N}\colon \forall n \in \mathbb{N}\colon \neg(n > m).$$

In words: "There is a natural number m such that for every natural number m the inequality $n \leq m$ holds".

Attention: The symbols $\wedge, \vee, \neg, \implies, \iff, \forall$ and $\exists$ are often useful, for example when negating nested logical statements, but they should never be used as a form of shorthand in mathematical texts. Such a text should always consist of complete sentences.

2 Proof techniques

2.1 Proving implications

Given two statements A and B, we want to prove that B follows from A, so

$$A \implies B.$$

The most important proof techniques for achieving this are:

- *Direct proof*: One assumes A to be true (for A false, the implication would be true anyway) and deduces via a chain of logical conclusions that B is true.
- *Proof by contraposition*: One instead proves

  $$\neg B \implies \neg A$$

  As already noted, this also proves $A \implies B$.

  So one assumes the negation of B and shows the negation of A.
- *Proof by contradiction*: One uses the equivalence of

  $$\neg(A \implies B) \text{ and } A \wedge (\neg B).$$

  To show $A \implies B$, one can instead show that $A \wedge (\neg B)$ is false.

  So one assumes that both A and $\neg B$ are true at once and performs logical deduction until a contradiction is reached. This shows that $A \wedge (\neg B)$ is false and therefore that $A \implies B$ is true.

Proofs by *contraposition* and *contradiction* are also called *indirect proofs*.

Example 2.1.1. Let q be a natural number. Consider the statements

$$A\colon\ q \text{ is even and prime}$$

and

$$B\colon q < 5.$$

We will prove $A \implies B$ using different techniques.

Proof.
- *Direct proof*: Let q be even and prime. Because of definition 0.1.3, we can write $q = 2 \cdot x$ with a natural number x. Because q is prime, it follows that $x = 1$ and therefore $2 = q < 5$.
- *Proof by contraposition*: The negation of B is "$q \geq 5$", the negation of A is "q is odd or not prime".

  So suppose $q \geq 5$. If q is odd, $\neg A$ is true. If q is even, we have $2 \mid q$ and therefore q is not prime; again $\neg A$ is true.

So we have $\neg B \implies \neg A$, which also shows $A \implies B$.

- *Proof by contradiction*: Let q be even and prime. Additionally let $q \geq 5$. Then $2 \mid q$. Because $q \geq 5$, this contradicts the fact that q is prime.

  Therefore $A \wedge (\neg B)$ is false and $\neg(A \wedge (\neg B))$, which is equivalent to $A \implies B$, must be true.

□

2.2 Proving equivalences

Given statements $A_1, A_2, \ldots, A_n$, we want to show that all these statements are pairwise equivalent, that is

$$A_i \iff A_j \text{ for all indices } i \neq j.$$

Again, there are different ways to attack this problem.

- *Direct proof*: Deduce via a chain of equivalences that for two arbitrary statements A_i and A_j, the statement $A_i \iff A_j$ is true.

  This technique often applies to solving of inequalities.
  Example 2.2.1. Determine all natural numbers n such that the inequality

  $$-3n + 2 < -7$$

  holds.

  Proof. We have

  $$-3n + 2 < -7 \iff -3n < -9 \iff n > 3.$$

  Therefore the inequality holds for all natural numbers $n \geq 4$. □

- *Reduction to implications*: Instead of proving $A \iff B$, one can prove the two implications

  $$A \implies B \text{ and } B \implies A.$$

  For this, one can use the techniques of the previous section.

  One drawback of this is that to prove n equivalences, one has to prove $n(n-1) = n^2 - n$ implications. To avoid that in practice, one often proves the n implications

  $$A_1 \implies A_2, A_2 \implies A_3, A_3 \implies A_4, \ldots, A_n \implies A_1.$$

  This proves the desired equivalence (just follow the implication arrows from statement A_i to A_j and vice versa).
  Example 2.2.2. Show that for a natural number n the following statements are equivalent:

  (a) n is even.

(b) n^2 is divisible by 4.

(c) n^2 is even.

Proof. We prove the statement using a circular chain of implications as outlined above.

"(a) $\implies$ (b)": Let n be even. Then $n = 2x$ for some natural number x. Therefore $n^2 = (2x)^2 = 4x^2$ and thus $4 \mid n^2$.

"(b) $\implies$ (c)": Suppose that n^2 is divisible by 4. Then there exists a natural number x with $n^2 = 4x$. Then $n^2 = 2 \cdot (2x)$, therefore n^2 is even.

"(c) $\implies$ (a)": We proceed by contraposition. So let n be odd. Then we can write n in the form

$$n = 2x - 1$$

for a natural number x. Therefore, we can compute

$$n^2 = (2x-1)^2 = 4x^2 - 2x + 1 = 1 + \underbrace{2 \cdot (2x^2 - x)}_{\text{even}}.$$

It follows that n^2 is odd. □

2.3 Disproving statements

To disprove a statement, you have to show that it is false. For statements of the form "For all ... it is true that ...", this is achieved by giving a counterexample. Ideally this is as simple and as concrete as possible.

Example 2.3.1. Disprove the statement

For every natural number m, there exists a natural number n, such that $n + m = nm$.

Proof. A counterexample to this statement is $m = 1$. For that, we get the equation

$$n + 1 = n,$$

which has no solution n in the natural numbers. □

Remark 2.3.2. While a single counterexample suffices to disprove a statement, an example generally does not suffice to prove a statement.

3 Recursion and mathematical induction

Both mathematical induction and recursion use the property of the natural numbers that for every element n, its unique successor $n+1$ is a natural number as well.
In fact this property characterizes the natural numbers: One can define $\mathbb{N}$ as the smallest set that includes 1 and with every element also its successor (to do this, one first has to be clear about what "1", "smallest" and "successor" precisely means).
One is then able to see that every element of $\mathbb{N}$ except 1 also has a unique predecessor and that every $n \in \mathbb{N}$ can be written in the form

$$n = \underbrace{1 + 1 + \cdots + 1}_{n \text{ times}}.$$

3.1 Recursion

Recursion is primarily used to define mathematical expressions.

Definition 3.1.1 (Summation notation)**.** Let $x, y \in \mathbb{Z}$ and a_k be numbers. One defines

$$\sum_{k=x}^{y} a_k := \begin{cases} 0 & \text{if } y < x, \\ a_x & \text{if } x = y, \\ \sum_{k=x}^{y-1} a_k + a_y & \text{otherwise.} \end{cases}$$

This defines shorthand notation for sums.

The actual recursion is in the last line inside of the curly brace. Here, the symbol $\sum_{k=x}^{y} a_k$ is being defined using the symbol $\sum_{k=x}^{y-1} a_k$. If this symbol is unknown as well, it is being defined using $\sum_{k=x}^{y-2} a_k$. When continuing this long enough, one will end up at the symbol $\sum_{k=x}^{x} a_k$, which is given concretely and thus known.

Example 3.1.2. Let a_1, a_2, a_3 be arbitrary numbers. Then

$$\sum_{k=1}^{3} a_k = \sum_{k=1}^{2} a_k + a_3 = \sum_{k=1}^{1} a_k + a_2 + a_3 = a_1 + a_2 + a_3.$$

Analogously for products we define

Definition 3.1.3. Let $x, y \in \mathbb{Z}$ and a_k be numbers. One defines

$$\prod_{k=x}^{y} a_k := \begin{cases} 1 & \text{if } y < x, \\ a_x & \text{if } x = y, \\ \prod_{k=x}^{y-1} a_k \cdot a_y & \text{otherwise.} \end{cases}$$

Recursion is also often used to define ordered *sequences* of numbers.

Example 3.1.4. Let a be a positive number. We set

$$a_1 := a \text{ and } a_{n+1} := \frac{1}{2}\left(a_n + \frac{a}{a_n}\right) \text{ for } n \in \mathbb{N}.$$

This way the sequence $a_1, a_2, a_3, \ldots$ is defined. One can show that a_n is arbitrarily close to $\sqrt{a}$ for large n.
It's very easy to recursively define this sequence, but finding an explicit expression for a_n is hard.

As an exercise, compute the first few terms of this sequence for $a = 2$.

Definition 3.1.5 (Factorial)**.** For $n \in \mathbb{N}_0$ we define

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

In particular $0! = 1$.

3.2 Mathematical induction

Mathematical induction is a method that can be used to prove statements of the form

$$\forall n \in \mathbb{N}\colon A(n).$$

Example 3.2.1. Consider the statements

$$A\colon \text{For all } n \in \mathbb{N} \text{ the number } 2^{2^n} + 1 \text{ is prime}$$

and

$$B\colon \text{For all } n \in \mathbb{N} \text{ the number } 2^{2^n} - 1 \text{ is divisible by 3.}$$

Are those statements true? One could be lead to believe that statement A is true, as it is easy to compute that $2^{2^n} + 1$ is indeed prime for $n = 1, 2, 3, 4$. But $2^{2^5} + 1 = 4294967297 = 641 \cdot 6700417$, which disproves statement A.
But statement B is true. This presents us with a problem, because however many natural numbers n we test, we will not be unable to deduce a contradiction and on the other hand such tests are unable to actually prove the statement; after all, there are infinitely many natural numbers, which we are unable to test.
So how are we to prove such statements?

Principle of mathematical induction

Suppose for every natural number $n \in \mathbb{N}$ we have a statement $A(n)$. Further suppose

(a) $A(1)$ is true.

(b) The statement $A(n) \implies A(n+1)$ is true for all $n \in \mathbb{N}$. That is, if $A(n)$ is true for an $n \in \mathbb{N}$, then $A(n+1)$ is true as well.

Then $A(n)$ is true for all $n \in \mathbb{N}$.

One can intuitively convince themselves that this works in the following way:
If $A(1)$ is true, then using (b) it follows that $A(2)$ is true as well. Again using (b) it follows that $A(3)$ is true. From this it follows that $A(4)$ is true and so on.
That $A(n)$ now holds for *all* $n \in \mathbb{N}$ follows from the fact that every natural number can be written as a finite sum of 1s.

We call the requirement in (a) the *initial* or *base case*.

Proving the implication in (b) can in principle be done with all the techniques used in the previous section, but one often proceeds in the following way:
One assumes that $A(n)$ is true for an arbitrary but fixed $n \in \mathbb{N}$. This is called the *induction hypothesis* or *inductive hypothesis*. Following this is the *induction step*, *inductive step* or *step case*, in which one shows that $A(n+1)$ follows from the true statement $A(n)$.[6]

3.3 Examples

We present a few small examples of proofs using mathematical induction.

Theorem 3.3.1 (Gauss)**.** *For all natural numbers $n \in \mathbb{N}$ we have*

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

Proof. We proceed via mathematical induction. The statement we want to prove is

$$A(n)\colon \sum_{k=1}^{n} k = \frac{n(n+1)}{2}.$$

Base case: $A(1)$ is true, because

$$\sum_{k=1}^{1} k = 1 = \frac{1 \cdot 2}{2}$$

[6] Hint: If you did not use the induction hypothesis in the inductive step, you almost surely did something wrong.

Induction hypothesis: Assume that $A(n)$ is true for a $n \in \mathbb{N}$.
Inductive step: It follows that then $A(n+1)$ is true as well, because

$$\begin{aligned}\sum_{k=1}^{n+1} k &\overset{\text{Def. of } \sum}{=} \sum_{k=1}^{n} k + (n+1) \overset{\text{Induction hypthesis}}{=} \frac{n(n+1)}{2} + (n+1) \\ &= \frac{n(n+1) + 2(n+1)}{2} = \frac{(n+1)(n+2)}{2}.\end{aligned}$$

The term $\frac{(n+1)(n+2)}{2}$ is precisely the right side of $A(n+1)$, which proves the statement. □

Here another example.

Theorem 3.3.2. *Suppose $x \neq 1$ and $n \in \mathbb{N}$. Then*

$$\prod_{k=1}^{n} \left(1 + x^{2^{k-1}}\right) = \frac{1 - x^{2^n}}{1 - x}.$$

Proof. We again proceed via mathematical induction.
Base case: The statement is true for $n = 1$ because

$$\prod_{k=1}^{1} \left(1 + x^{2^{k-1}}\right) = 1 + x^{2^0} = 1 + x \overset{x \neq 1}{=} \frac{(1+x)(1-x)}{1-x} = \frac{1 - x^{2^1}}{1-x}.$$

Induction hypothesis: Suppose the statement is true for a $n \in \mathbb{N}$.
Inductive step: Then the statement is also true for $n+1$, because

$$\begin{aligned}\prod_{k=1}^{n+1} \left(1 + x^{2^{k-1}}\right) &\overset{\text{Def. of } \prod}{=} (1 + x^{2^n}) \prod_{k=1}^{n} \left(1 + x^{2^{k-1}}\right) \overset{\text{Ind. hyp.}}{=} (1 + x^{2^n}) \cdot \frac{1 - x^{2^n}}{1 - x} \\ &= \frac{(1 + x^{2^n})(1 - x^{2^n})}{1 - x} = \frac{1 - \left(x^{2^n}\right)^2}{1 - x} \\ &= \frac{1 - x^{2 \cdot 2^n}}{1 - x} = \frac{1 - x^{2^{n+1}}}{1 - x}.\end{aligned}$$

Because the term $\frac{1 - x^{2^{n+1}}}{1-x}$ is again precisely the right hand side of the statement for $n+1$, this proves the statement. □

Now let us return to our initial problem.

Theorem 3.3.3. *The number $2^{2^n} - 1$ is divisible by 3 for every $n \in \mathbb{N}$.*

Proof. Left as an exercise to the reader. □

3.4 Variations of mathematical induction

Generalization to related number systems

Mathematical induction is not just limited to the natural numbers. It is also possible to prove statements of the form

$$\forall z \in \mathbb{Z}, z \geq z_0 \colon A(z)$$

for a fixed $z_0 \in \mathbb{Z}$.

To do this, we alter the principle of induction in the following way.

Let $z_0 \in \mathbb{Z}$ be a fixed integer. Suppose for every integer $z \geq z_0$ we have a statement $A(z)$. Further suppose

(a) $A(z_0)$ is true.

(b) The statement $A(z) \implies A(z+1)$ is true for all integers $z \geq z_0$.

Then $A(z)$ is true for all integers $z \geq z_0$.

Nothing new happens here, in principle we only let the natural numbers start at z_0.

As an example, we prove the following

Theorem 3.4.1. *For $n \geq 4$ the inequality $2^n < n!$ holds.*

Proof. Base case: The inequality holds for $n = 4$, because

$$2^4 = 16 < 24 = 4!$$

Induction hypothesis: Suppose the statement is true for a $n \geq 4$.
Inductive step: Then the statement is also true for $n+1$, because

$$2^{n+1} = 2 \cdot 2^n \overset{\text{Ind. hyp.}}{<} 2 \cdot n! \overset{2<n+1}{<} (n+1) \cdot n! = (n+1)!$$

□

Generalization to $\mathbb{Z}$

Until now we have only used induction on sets with a smallest element, but one can also use it on $\mathbb{Z}$.

Suppose for every integer z there is a statement $A(z)$. Further suppose

(a) $A(0)$ is true.

(b) $A(z) \implies A(z+1)$ for all integers $z \geq 0$.

(c) $A(z) \implies A(-z)$ for all natural numbers z.

Then $A(z)$ is true for all integers.

For illustration purposes we prove the following statement

Theorem 3.4.2. *For all integers z, the number $z^3 - z$ is divisible by 3.*

Proof. Base case: The statement is true for $z = 0$, because

$$3 \mid 0 = 0^3 - 0.$$

Induction hypothesis: Suppose the statement is true for a $z \geq 0$.
Inductive step 1: Then it is also true for $z+1$, because

$$(z+1)^3 - (z+1) = (z^3 + 3z^2 + 3z + 1) - (z+1) = (z^3 - z) + 3z^2 + 3z.$$

Due to the induction hypothesis, we have $3 \mid (z^3 - z)$. Because $3z^2 + 3z = 3 \cdot (z^2 + z)$, 3 is also a divisor of $3z^2 + 3z$. In total it follows that $3 \mid (z+1)^3 - (z+1)$.
Inductive step 2: Then the statement is also true for $-z$, because

$$(-z)^3 - (-z) = -(z^3 - z).$$

Because $z^3 - z$ is divisible by 3 according to the induction hypothesis, $-(z^3 - z)$ is as well. In total the statement is true for all integers. □

4 Sets

We will refrain from precisely defining what a *set* is and instead treat them only naively. Mathematically rigorous set theory is quickly becoming abstract and proof-heavy, which is counterproductive to our goals in this text. So for our purposes we note:

A *set* is a collection M of certain distinct objects m of our intuition or of our thinking (which we will call the *elements* of M), considered as an object in its own right.

This neat "definition" is unfortunately contradictory. For example, let M be the set of all sets, which are not elements of themselves. Is then M an element of itself?

Nevertheless, we will pretend not to notice that and continue with our considerations and let the set theorists worry about such nuances.

4.1 Notation

If M is a set and x an element of m, we write

$$x \in M$$

and say that x is in M or that x is included in M. If x is not in M, we instead write

$$x \notin M.$$

It is always true that either $x \in M$ or $x \notin M$.

A set can be defined by listing its elements, for example

$$M := \{a, b, c, d\}$$

is the set consisting of precisely the elements a, b, c and d. Often one uses the placeholder "..." to suggest that a set includes more elements that can be inferred from the given elements.

In most cases, sets are defined by a certain property. We write

$$M = \{x \mid x \text{ has property } E\} \quad \text{or} \quad M = \{x : x \text{ has property } E\}.$$

This is called *set-builder notation*.

Example 4.1.1. (a) The set of natural numbers

$$\mathbb{N} := \{1, 2, 3, 4, 5, 6, \dots\}.$$

(b) The set of natural numbers, including 0

$$\mathbb{N}_0 := \{0, 1, 2, 3, 4, 5, 6, \dots\}.$$

(c) The set of even natural numbers

$$2\mathbb{N} := \{2, 4, 6, \dots\} = \{n \in \mathbb{N} : 2 \mid n\}.$$

(d) The set of prime numbers

$$\mathbb{P} := \{p \in N \mid p = p_1 p_2 \text{ for } p_1, p_2 \in \mathbb{N} \text{ with } p_1 \leq p_2 \text{ implies } p_1 = 1 < p_2\}.$$

Sets don't necessarily have to consist of numbers. For example, one often deals with sets of sets, sets of functions, etc.

Definition 4.1.2. Two sets M and N are *equal*, in symbols $M = N$, if every element of M is also an elements of N and vice versa.
So the statement $M = N$ is defined as $x \in M \iff x \in N$.

Example 4.1.3. We have $\{1, 2, 3\} = \{1, 1, 1, 1, 1, 2, 3\}$, even though the element 1 appears "more often" in the set on the right side. The definition of equality of sets does not care about that.

Definition 4.1.4. A set M is called *subset* of a set N, in symbols $M \subseteq N$, if every element of M is also in N.
In particular we have $M \subseteq N$ if $M = N$[7]

If we want to state that M is a *proper subset* of N, that is $M \subseteq N$ and $M \neq N$, we write $M \subset N$.
To summarize, we have

$$\begin{aligned} M = N &\iff (x \in M \iff x \in N) \\ M \neq N &\iff \neg(M = N) \\ M \subseteq N &\iff (x \in M \implies x \in N) \\ M \subset N &\iff (M \subseteq N \wedge M \neq N) \end{aligned}$$

(Where "$\iff$" stands for "is defined as".)

An immediate consequence of the definitions is

Theorem 4.1.5 (Determining equality of sets)**.** *Let M, N be sets. Then $M = N$ holds if and only if $M \subseteq N$ and $N \subseteq M$.*

Definition 4.1.6 (Empty set)**.** The set

$$\varnothing := \{\} = \{x \in M \mid x \neq x\}$$

[7] Notation for this is unfortunately not consistent. Some authors use $\subset$ (instead of $\subseteq$) and $\subsetneq$ or even $\subsetneqq$ (instead of $\subset$). We take the sane approach and choose to use the symbols inspired by $\leq$ and $<$.

is called the *empty set*. It is uniquely determined and does not depend on the set M.

The empty set is subset of every set and includes no element.

Definition 4.1.7 (Power set)**.** Let M be a set. The *power set* 2^M of M is the set

$$2^M := \{N \mid N \subseteq M\} = \{N \mid N \text{ is a subset of } M\}$$

of all subsets of M. This means that 2^M is a set of sets.

Instead of 2^M, one also often writes $\mathbb{P}(M)$, $\mathcal{P}(M)$ or $\mathfrak{P}(M)$.

Example 4.1.8. We have

$$2^{\{0,1\}} = \{\varnothing, \{0\}, \{1\}, \{0,1\}\}, \quad 2^{\varnothing} = \{\varnothing\}, \quad 2^{2^{\varnothing}} = \{\varnothing, \{\varnothing\}\}.$$

4.2 Operations on sets

In the following we will present some important *operations on sets*. Essentially this means transferring the logical operations to the language of sets.

Union

The union

$$M \cup N := \{x \mid x \in M \vee x \in N\}$$

of two sets M, N consists precisely of those elements that are in M or in N.

Example 4.2.1.

$$\{1,2\} \cup \{2,3\} = \{1,2,3\}$$

More generally, let $\mathcal{M}$ be a set whose elements are sets themselves. The *union* of the sets included in $\mathcal{M}$ is the set

$$\bigcup_{M \in \mathcal{M}} M := \{x \mid \exists M \in \mathcal{M} \colon x \in M\}.$$

$\bigcup_{M \in \mathcal{M}} M$ is therefore the set of elements that are included in at least one $M \in \mathcal{M}$.

Often we *index* the family of sets $\mathcal{M}$, that is we assign a unique index i from some *index set* I to each element of $\mathcal{M}$:

$$\mathcal{M} = \{M_i \mid i \in I\}.$$

Instead of $\bigcup_{M \in \mathcal{M}} M$ we can then write $\bigcup_{i \in I} M_i$ and we have

$$\bigcup_{i \in I} M_i = \{x \mid \exists i \in I \colon x \in M_i\}.$$

Example 4.2.2. Let $I := \mathbb{N}$ and $M_i := \{i, i+1, \dots, 2i\}$ for $i \in I$. Then

$$\bigcup_{i \in I} M_i = \mathbb{N}.$$

Proof. "$\subseteq$": As every M_i is a subset of $\mathbb{N}$, we also have $\bigcup_{i \in I} M_i \subseteq \mathbb{N}$.

"$\supseteq$": It remains to be shown that $\mathbb{N} \subseteq \bigcup_{i \in I} M_i$. So let n be an arbitrary element of $\mathbb{N}$. Then $n \in M_n$ and therefore

$$n \in \bigcup_{i \in I} M_i = \bigcup_{n \in \mathbb{N}} M_n.$$

As n was arbitrary, we get $\mathbb{N} \subseteq \bigcup_{i \in I} M_i$. □

Intersection

The intersection of two sets M and N

$$M \cap N := \{x \mid x \in M \wedge x \in N\}$$

consists precisely of those elements that are both in M and in N.

Example 4.2.3.

$$2\mathbb{N} \cap \mathbb{P} = \{2\}.$$

More generally

$$\bigcap_{M \in \mathcal{M}} M := \{x \mid \forall M \in \mathcal{M} \colon x \in M\}$$

is the intersection of a *non-empty* family of sets $\mathcal{M}$. It consists precisely of those elements that are in all $M \in \mathcal{M}$. Using index notation, we get

$$\bigcap_{i \in I} M_i = \{x \mid \forall i \in I \colon x \in M_i\}.$$

Example 4.2.4. Let $I := \mathbb{N}$ and $M_i := \{n \in \mathbb{N} \mid i < n < 4i\}$ for $i \in I$. Then

$$\bigcap_{i \in I} M_i = \varnothing.$$

How could one prove this statement?

Complement

The *(relative) complement* or *set difference* of a set N with respect to M is the set

$$M \setminus N := \{x \mid x \in M \wedge x \notin N\}.$$

It consists precisely of those elements that are in M but not in N.

Example 4.2.5. $\mathbb{N} \setminus 2\mathbb{N}$ is the set of all odd natural numbers.

4.3 Calculation rules in set theory

For sets M, N, L, X the following holds

(a) $M \setminus M = \varnothing$, $M \setminus \varnothing = M$.

(b) $M \cap M = M$, $M \cup M = M$.

(c) Commutativity:

$$M \cup N = N \cup M,$$
$$M \cap N = N \cap M.$$

(d) Associativity:

$$(M \cup N) \cup L = M \cup (N \cup L),$$
$$(M \cap N) \cap L = M \cap (N \cap L).$$

(e) Distributivity:

$$(M \cap N) \cup L = (M \cup L) \cap (N \cup L),$$
$$(M \cup N) \cap L = (M \cap L) \cup (N \cap L).$$

(f) For subsets M, N of a set X we have:

(1) $X \setminus (X \setminus M) = M$.

(2) De Morgan's laws

$$X \setminus (M \cap N) = (X \setminus M) \cup (X \setminus N),$$
$$X \setminus (M \cup N) = (X \setminus M) \cap (X \setminus N).$$

(3) More generally, De Morgan's laws are also true for families of sets

$$X \setminus \bigcap_{M \in \mathcal{M}} M = \bigcup_{M \in \mathcal{M}} (X \setminus M),$$
$$X \setminus \bigcup_{M \in \mathcal{M}} M = \bigcap_{M \in \mathcal{M}} (X \setminus M).$$

Similar to rules in propositional calculus, those rules can be proven using truth tables. We demonstrate this for the second of De Morgan's rules and leave the rest as an exercise to the reader.

Proof. We want to prove $X \setminus (M \cup N) = (X \setminus M) \cap (X \setminus N)$.

Both on the left hand side and the right hand side we have subsets of X, so let $x \in X$ be arbitrary. Then

$x \in M$	$x \in N$	$x \in X \setminus (M \cup N)$	$x \in X \setminus M$	$x \in X \setminus N$	$x \in (X \setminus M) \cap (X \setminus N)$
t	**t**	**f**	**f**	**f**	**f**
t	**f**	**f**	**f**	**t**	**f**
f	**t**	**f**	**t**	**f**	**f**
f	**f**	**t**	**t**	**t**	**t**

One can see in above table that for all $x \in X$ we have

$$x \in X \setminus (M \cup N) \iff x \in (X \setminus M) \cap (X \setminus N).$$

This is exactly the definition of set equality. □

4.4 Cartesian Product

The *ordered pair* or *tuple* of two objects x, y is the object (x, y) with the property

$$(x, y) = (x', y') \iff x = x' \text{ and } y = y'.$$

In particular $(x, y) \neq (y, x)$ if $x \neq y$.

Formally one can define (x, y) as a set by setting

$$(x, y) := \{\{x\}, \{x, y\}\}.$$

One can show that then above property is satisfied.

Definition 4.4.1. The *cartesian product of two sets* M, N is the set

$$M \times N := \{(x, y) \mid x \in M \text{ and } y \in N\}.$$

Example 4.4.2. The set $\mathbb{N} \times \mathbb{N}$ consists of the pairs (a, b) with $a \in \mathbb{N}$ and $b \in \mathbb{N}$. So $\mathbb{N} \times \mathbb{N} = \{(1, 1), (1, 2), (2, 1), \dots\}$.

Definition 4.4.3. Let $n \geq 2$ be a natural number and $M_1, \dots, M_n$ be sets. The *cartesian product* of the sets $M_1, \dots, M_n$ is the set

$$M_1 \times \cdots \times M_n := \{(x_1, \dots, x_n) \mid x_1 \in M_1 \wedge \cdots \wedge x_n \in M_n\}.$$

For this we define the *n-tuple* $(x_1, \dots, x_n)$ recursively by setting

$$(x_1, \dots, x_n) := ((x_1, \dots, x_{n-1}), x_n).$$

Then we have

$$(x_1, \dots, x_n) = (y_1, \dots, y_n) \iff x_1 = y_1 \wedge \cdots \wedge x_n = y_n.$$

When $M = M_1 = \cdots = M_n$ we also write M^n instead of $M_1 \times \cdots \times M_n$.

Example 4.4.4. You are probably familiar with 3-dimensional euclidean space

$$\mathbb{R}^3 = \mathbb{R} \times \mathbb{R} \times \mathbb{R} = \{(x, y, z) \mid x, y, z \in \mathbb{R}\}.$$

One can identify this set with the points of space.

Theorem 4.4.5. *Let M_1, M_2, N be sets. Then we have*

(a) $(M_1 \cap M_2) \times N = (M_1 \times N) \cap (M_2 \times N)$.

(b) $(M_1 \cup M_2) \times N = (M_1 \times N) \cup (M_2 \times N)$.

Proof. Left as an exercise to the reader. □

5 Maps

A *map* or *function* f from a set M to a set N is a rule that assigns to each element $x \in M$ a unique element $y \in N$.
More precisely

Definition 5.0.1. Let M, N be sets and $R \subseteq M \times N$. We call the tuple

$$f = (M, N, R)$$

a *map* or *function* from M to N if for every $x \in M$ there is exactly one $y \in N$ with $(x, y) \in R$.
We call M the *domain* of f and N the *codomain* of f.
Instead of writing $(x, y) \in R$ we also write

$$y = f(x)$$

and call y the *image* of x under f.
Instead of writing $f = (M, N, R)$, we also write

$$f : M \to N, \quad x \mapsto f(x).$$

Example 5.0.2. Often we define maps in terms of (arithmetical) expressions, for example

$$f : \mathbb{N} \to \mathbb{N}, \quad z \mapsto z^2.$$

But there are also functions that can't be described that way:

$$g : \mathbb{N} \to \mathbb{N}, \quad n \mapsto \text{smallest prime greater than } n.$$

For the second example, it is not obvious if g even is a function, that is if every natural number can be assigned a unique value in the codomain. Is there a unique smallest prime number greater than n for every $n \in \mathbb{N}$? This question can be answered affirmatively if one knows that there are infinitely many prime numbers.

Because two tuples are equal if and only if they are equal in every entry, we get

Definition 5.0.3 (Equality of functions)**.** Let $f_1 = (M_1, N_1, R_1)$ and $f_2 = (M_2, N_2, R_2)$ be maps. Then we have $f_1 = f_2$ if and only if

- $M_1 = M_2$ and
- $N_1 = N_2$ and
- $R_1 = R_2$.

Or formulated differently:
Two maps f_1 and f_2 are equal if and only if their domains and codomains are equal and for all elements x of the domain we always have $f_1(x) = f_2(x)$.

Example 5.0.4. Consider the maps

$$f\colon \mathbb{N} \to \mathbb{N},\ z \mapsto 2z, \quad g\colon \mathbb{N} \to 2\mathbb{N},\ z \mapsto 2z$$

and

$$h\colon \mathbb{N} \to \mathbb{N}, h(z) \coloneqq \text{number of elements in the set } \{z+1, z+2, \ldots, 3z\}.$$

Even though we have $f(z) = g(z)$ for all $z \in \mathbb{N}$, we have $f \neq g$. On the other hand the maps f and h are equal.

5.1 Image and preimage

We introduce a number of important concepts:

Definition 5.1.1. (a) The *graph* of a map $f\colon M \to N$ is the set

$$\Gamma_f \coloneqq \{(x, f(x)) \mid x \in M\} \subseteq M \times N.$$

The graph of f is therefore precisely the set R given in the definition of map.

(b) The *image* of a subset $A \subseteq M$ under $f\colon M \to N$ is the set

$$f(A) \coloneqq \{f(x) \mid x \in A\} \subseteq N.$$

We also call $f(M)$ the *image* of f.

(c) The *preimage* of a set $B \subseteq N$ is the set

$$f^{-1}(B) \coloneqq \{x \in M \mid f(x) \in B\} \subseteq M.$$

(d) Let A be a subset of M. Then we call

$$f|_A : A \to N, \quad x \mapsto f(x)$$

the *restriction* of f to A.

Example 5.1.2. Consider

$$f\colon \mathbb{N} \to \mathbb{N}, \quad n \mapsto \begin{cases} 1 & \text{if } n \geq 4, \\ n^2 & \text{if } n < 4. \end{cases}$$

(a) The image of $\mathbb{P}$ under f is $f(\mathbb{P}) = \{1, 4, 9\}$, because $f(2) = 4$, $f(3) = 9$ and $f(n) = 1$ for all $n \in \mathbb{P}$ with $n \geq 4$.

(b) The preimage of $\mathbb{P} \subseteq \mathbb{N}$ under f is $f^{-1}(\mathbb{P}) = \varnothing$, because there is no $n \in \mathbb{N}$ such that $f(n)$ is prime.

Example 5.1.3. The graph Γ of a function $\mathbb{R} \to \mathbb{R}$ is a subset of $\mathbb{R}^2$. When identifying the elements of Γ with points of $\mathbb{R}^2$, one can draw them in a coordinate system and thus obtain a graphical representation of f.

The following statements are important.

Theorem 5.1.4. *For every map $f : M \to N$ and subsets $A, A_1, A_2 \subseteq M$ and $B_1, B_2 \subseteq N$ we have:*

(a)
$$f^{-1}(B_1 \cup B_2) = f^{-1}(B_1) \cup f^{-1}(B_2),$$

(b)
$$f^{-1}(B_1 \cap B_2) = f^{-1}(B_1) \cap f^{-1}(B_2),$$

(c)
$$f(A_1 \cup A_2) = f(A_1) \cup f(A_2),$$

(d)
$$f(A_1 \cap A_2) \subseteq f(A_1) \cap f(A_2),$$

(e)
$$A \subseteq f^{-1}(f(A)).$$

Proof. We only show (a). The other proofs are similar and left as an exercise to the reader. In particular the reader should think about why equality does not hold in general in (d) and (e) and construct suitable counterexamples.
"$f^{-1}(B_1 \cup B_2) \subseteq f^{-1}(B_1) \cup f^{-1}(B_2)$":
Suppose $x \in f^{-1}(B_1 \cup B_2)$. Then $f(x) \in B_1 \cup B_2$. Therefore $f(x)$ is in B_1 or in B_2. Thus x is in $f^{-1}(B_1)$ or in $f^{-1}(B_2)$, so

$$x \in f^{-1}(B_1) \cup f^{-1}(B_2).$$

"$f^{-1}(B_1 \cup B_2) \supseteq f^{-1}(B_1) \cup f^{-1}(B_2)$":
Suppose $x \in f^{-1}(B_1) \cup f^{-1}(B_2)$. Then $x \in f^{-1}(B_1)$ or $x \in f^{-1}(B_2)$. This shows that $f(x) \in B_1$ or $f(x) \in B_2$, therefore $f(x) \in B_1 \cup B_2$. It follows that

$$x \in f^{-1}(B_1 \cup B_2).$$

□

5.2 Injectivity, surjectivity and bijectivity

Definition 5.2.1 (Surjectivity)**.** A function $f : X \to Y$ is called *surjective* if $f(X) = Y$.

Theorem 5.2.2. *For a function $f : X \to Y$ the following are equivalent:*

(a) f is surjective.

(b) $f(X) = Y$.

(c) *Codomain and image of the function are equal.*

(d) *Every element of the codomain has* at least one *preimage.*

Example 5.2.3. A function $f : \mathbb{R} \to \mathbb{R}$ is surjective if and only if every parallel to the x-axis intersects the graph of the function at least once.

Definition 5.2.4 (Injectivity)**.** A map $f : X \to Y$ is called *injective* if for all $x_1, x_2 \in M$ we have

$$x_1 \neq x_2 \implies f(x_1) \neq f(x_2).$$

Theorem 5.2.5. *For a function $f : X \to Y$ the following are equivalent:*

(a) *f is injective.*

(b) $\forall x_1, x_2 \in X : x_1 \neq x_2 \implies f(x_1) \neq f(x_2)$.

(c) $\forall x_1, x_2 \in X : f(x_1) = f(x_2) \implies x_1 = x_2$.
In other words: If $y \in Y$ has a preimage, it must be unique.

(d) *Every $y \in Y$ has* at most one *preimage.*

Example 5.2.6. A function $f : \mathbb{R} \to \mathbb{R}$ is injective if and only if every parallel to the x-axis intesects the graph in not more than a single point.

Definition 5.2.7 (Bijectivity)**.** A function $f : X \to Y$ is called *bijective* if it is surjective and injective. The map f is therefore bijective if and only if every $y \in Y$ has *exactly one* preimage $x \in X$.

Because for a bijective function every element in the codomain has exactly one preimage, we are able to define a new function:

Definition 5.2.8 (Inverse function)**.** Let $f : X \to Y$ be bijective. Then

$$g : Y \to X, \quad y \mapsto \text{unique preimage of } y \text{ under } f$$

is a function as well. We call it the *inverse function* or *inverse map* of f and denote it by f^{-1}.

Theorem 5.2.9. *A function f is bijective if and only if it has an inverse function. The inverse function is uniquely determined by f.*

Example 5.2.10. (a) Consider the maps

$$f : \mathbb{Z} \to \mathbb{Z},\ z \mapsto z^2 \text{ and } g : \mathbb{N} \to \mathbb{N},\ z \mapsto z^2.$$

The map f is not surjective, because there are elements in the codomain that do not have a preimage, for example -1. We have

$$f(\mathbb{Z}) \subset \mathbb{Z}.$$

The map f is also not injective, because the elements 1 and -1 in the domain both have the same image

$$f(1) = 1 = f(-1).$$

Likewise g is not surjective as well, because $2 \in \mathbb{N}$ does not have a preimage under g. But g is injective, because for every $x_1, x_2 \in \mathbb{N}$ with $g(x_1) = g(x_2)$ we have

$$g(x_1) = g(x_2) \implies x_1^2 = x_2^2 \implies |x_1| = |x_2| \overset{x_i \text{ is positive}}{\implies} x_1 = x_2.$$

An element in the image of g therefore has a unique preimage.

(b) The function

$$f\colon \mathbb{N} \to 2\mathbb{N},\ n \mapsto 2n$$

is bijective. Its inverse function is

$$f^{-1}\colon 2\mathbb{N} \to \mathbb{N},\ n \mapsto \frac{1}{2}n.$$

Definition 5.2.11 (Composition)**.** Let $f\colon X \to Y$ and $g\colon Y \to Z$ be maps. The map $g \circ f$ (read: "g after f") is then defined as

$$g \circ f\colon X \to Z,\ x \mapsto g(f(x)).$$

We call $g \circ f$ the *composition of f with g*.

To be able to form the composition $g \circ f$, it is required that the codomain of f is a subset of the domain of g.

Example 5.2.12. (a) Consider

$$f\colon \mathbb{N} \to \mathbb{N},\ n \mapsto 3n \text{ and } g\colon \mathbb{N} \to \mathbb{N},\ n \mapsto n^2.$$

We are able to form both compositions $f \circ g$ and $g \circ f$. For $n \in \mathbb{N}$ we have

$$(g \circ f)(n) = g(f(n)) = g(3n) = 9n^2, \text{ and therefore } g \circ f\colon \mathbb{N} \to \mathbb{N},\ n \mapsto 9n^2.$$

Analogously we obtain

$$f \circ g\colon \mathbb{N} \to \mathbb{N},\ n \mapsto 3n^2.$$

We have $f \circ g \neq g \circ f$.

(b) Let $f\colon X \to Y$ be bijective. Then we have for all $x \in X$

$$f^{-1}(f(x)) = x.$$

Additionally we have for all $y \in Y$

$$f(f^{-1}(y)) = y.$$

Definition 5.2.13. The map

$$\mathrm{id}_X \colon X \to X,\ x \mapsto x$$

is called the *identity on* X. It is bijective with $\mathrm{id}_X^{-1} = \mathrm{id}_X$.

Theorem 5.2.14. *The map $f \colon X \to Y$ is bijective if and only if there exists a map $g \colon Y \to X$ such that*

$$g \circ f = \mathrm{id}_X \ \text{ and } \ f \circ g = \mathrm{id}_Y.$$

Proof. The map g is precisely the inverse map of f. □

Remark 5.2.15. An inverse map f^{-1} is only defined for bijective maps, but the preimage $f^{-1}(A)$ exists for every map $f \colon X \to Y$ and every subset $A \subseteq X$. Here we (unfortunately) use the same notation for two different things.

Theorem 5.2.16. *Let $f \colon X \to Y$ and $g \colon Y \to Z$ be maps. Then*

(a) If f and g are both injective, then $g \circ f$ is injective.

(b) If f and g are both surjective, then $g \circ f$ is surjective.

(c) If f and g are both bijective, then $g \circ f$ is bijective. In this case we have

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

Proof. We only prove statement (a) and leave the others as an exercise.
Let f and g be injective. We have to show: For $x_1, x_2 \in X$ and $(g \circ f)(x_1) = (g \circ f)(x_2)$ it follows that $x_1 = x_2$.

So suppose $(g \circ f)(x_1) = (g \circ f)(x_2)$. Then

$$\begin{aligned}(g \circ f)(x_1) = (g \circ f)(x_2) &\iff g(f(x_1)) = g(f(x_2)) \\ &\overset{g \text{ injective}}{\implies} f(x_1) = f(x_2) \\ &\overset{f \text{ injective}}{\implies} x_1 = x_2.\end{aligned}$$

This proves the claim. □