Foundations of Discrete Mathematics

Spring 2022

Tuomas Sahlsten
Based on Ragnar Freij-Hollanti's materials

Version 0.4 (February 21, 2022), first chapter included

Department of Mathematics and Systems Analysis, Aalto University

Contents

1 Sets and formal logic **3**

1.1 Sets . . . 3

1.1.1 Definition . . . 3

1.1.2 Equality and subsets . . . 5

1.1.3 Set operations . . . 5

1.1.4 Cartesian product . . . 7

1.1.5 Enumeration . . . 8

1.1.6 Indexing a family of sets and set operations . . . 9

1.1.7 Russel's paradox . . . 10

1.2 Formal logic . . . 12

1.2.1 Statements, closed- and open sentences . . . 12

1.2.2 Quantifiers . . . 13

1.2.3 Connectives and truth tables . . . 14

1.2.4 Tautologies . . . 15

1.2.5 Treasures example . . . 17

1.2.6 Negations of quantifiers . . . 18

1.2.7 Computing with logical symbols . . . 18

1.2.8 Sets and predicate logic . . . 18

1.3 Proof techniques . . . 19

1.3.1 Proof and overview of the proof techniques . . . 19

1.3.2 Direct proof . . . 20

1.3.3 Contrapositive proof . . . 20

1.3.4 Proof by contradiction . . . 21

1.3.5 Proof by cases . . . 21

1.3.6 Constructive existence proof . . . 22

1.3.7 Nonconstructive existence proof . . . 22

1.3.8 Induction proofs . . . 23

1.4 Relations . . . 25

1.4.1 Definition and different types of relations . . . 25

1.4.2 Equivalence relations 29
1.4.3 Partial orders 31
1.4.4 Hasse diagram 32
1.4.5 Linear extensions 33
1.5 Functions 34
1.5.1 Definition and graphs 35
1.5.2 Composition of functions 36
1.5.3 Injection, surjection, bijection 37
1.5.4 Inverse functions 37
1.6 Cardinalities 37
1.6.1 Infinite cardinalities 39

Welcome!

These are the lecture notes for the Foundations of Discrete Mathematics (MS-A0402) is given in Period IV on Spring 2022 in Aalto University. Discrete Mathematics is the mathematics of finite and countable structures, or loosely speaking the mathematics of sets where there is no notion of "convergence". Methods from discrete mathematics play a large role in many other subjects, in particular in computer engineering and data science. In this course we cover the foundations of discrete mathematics (graphs, enumeration, modular arithmetic) as well as as the foundations of all mathematics on university level (set logic and proof techniques). We also study some modern applications of the theory, in cryptography and networks theory.

Course content is roughly outlined as:

- Set theory and formal logic
- Relations and equivalence
- Enumerative combinatorics
- Graph theory
- Modular arithmetics

But more importantly:

- The fundamental notions and methods of mathematics (definition, theorem, proof, example...)

For learning, I recommend to look at the **Explorative exercises** (and additional exercises) from the assignment sheets: Updated on course homepage every Friday.

Here is some extra supporting literature for the course (in addition to these lecture notes, contain more details and proofs):

- Kenneth Rosen: *Discrete Mathematics and its Applications*, physical book
- Kenneth Bogart: *Combinatorics Through Guided Discovery.*, Freely available, `https://math.dartmouth.edu/news-resources/electronic/kpbogart/ComboNoteswHints11-06-04.pdf`
- Richard Hammack: *Book of Proof*, Freely available, `http://www.people.vcu.edu/%7Erhammack/BookOfProof/BookOfProof.pdf`

Good luck with the course!

- Tuomas

Chapter 1

Sets and formal logic

Set theory and formal logic form the foundation of all modern mathematics and the universal language used to describe and model phenomena. Here *sets* form some way to talk about collections of objects, where as *formal logic* gives us way to talk about logical implications. We learn formal logic:

- To define *precise* meanings of "and", "not", "or",...
- To transform complicated statements to equivalent but easier statements.
- Because it is the glue that holds mathematical statements together.

We do **not** learn it in order to:

- Write all mathematics using the symbols $\vee, \wedge, \forall, \exists, \cdots$

Formal logic is in the background of all mathematics, not the forefront.

1.1 Sets

1.1.1 Definition

All mathematical structures are sets, and all statements about them can be described in terms of sets.

Example 1.1

- $\mathbb{N} = \{0, 1, 2, 3, \dots\}$ is the set of natural numbers.
- $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$ is the set of integers.
- $\mathbb{Q} = \{\frac{p}{q} : p, q \in \mathbb{Z}, q \neq 0\}$ is the set of rational numbers.
- $\mathbb{R}$ is the set of real numbers.
- $\{\Delta ABC : A, B, C \in \mathbb{R}^2\}$ is the set of triangles in the plane.
- The members (*elements*) of a set can be whatever:

  $$A = \{\text{skateboard}, \text{paperclip}, 16, \pi, \text{infinity}\}$$

  is a set.

The most important notion in set theory is the symbol $\in$.

- $x \in A$ if "the element x belongs to the set A".
- $x \notin A$ if "the element x does not belong to the set A".

Example 1.2

- my car $\in \{\text{cars}\}$.
- $5 \in \mathbb{Z}$.
- $5 \in \mathbb{R}$.
- $5 \notin \mathbb{R}^2$.
- $\pi \in \mathbb{R}$.
- $\pi \notin \mathbb{Z}$.

We can *define the set* in the following ways:

- Listing elements: $\{2, 4, 5, 7\}$ is a set whose elements are 2, 4, 5, 7.
- Writing

  $$\{\texttt{expression} : \texttt{condition}\},$$

  which is a set containing all elements described by the `expression`, if the `condition` is satisfied.
  - $\{x^2 : x \in \mathbb{Z}, 2 < x < 10\} = \{9, 16, 25, 36, 49, 64, 81\}$.
  - $\{x \in \mathbb{R} : -1 \leq x \leq 1\} = [-1, 1]$.
- Futhermore, *empty set* $\emptyset = \{\}$ is a set that has no elements.

1.1.2 Equality and subsets

Definition 1.3 (Equality)

We say that two sets are the *same* $=$ if they contain the same elements.

Example 1.4

$\{2, 3, 4\} = \{4, 2, 4, 3\}$.

Sets do not have "order", nor "multiplicity". Thus, there is only one "empty set" $\emptyset$.

Definition 1.5 (Subsets)

We define $A \subseteq B$ ("A is a *subset* of B") if all elements of A are also in B.

Subsets can be visualised with a *Venn diagram:*

Example 1.6

- $$\emptyset \subseteq \{1, 2, 3\} \subseteq \mathbb{Z} \subseteq \mathbb{R}.$$
- $\emptyset$ is a subset of every set.
- Every set is a subset of itself.

Thus, $A = B$ if

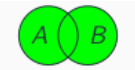
$$A \subseteq B \text{ and } B \subseteq A.$$

If $A \subseteq B$ and $A \neq B$, then A is a *proper* subset of B. Denoted $A \subsetneq B$, or sometimes $A \subset B$.

1.1.3 Set operations

In set theory we will commonly use the following set operations, which we can visualise with Venn diagrams.

- Union: $x \in A \cup B$ if $x \in A$ *or* $x \in B$.



- Intersection: $x \in A \cap B$ if $x \in A$ *and* $x \in B$.

- Set difference: $x \in A \setminus B$ if $x \in A$ but $x \notin B$.

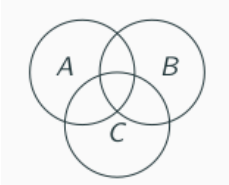
- Complement: $x \in A^c = \Omega \setminus A$ if $x \notin A$
  (but x is in the "universe" Ω, which is understood from context).

Then the set operations satisfy the following *laws*

Theorem 1.7

- Commutative laws:
  - $A \cap B = B \cap A$
  - $A \cup B = B \cup A$
- Associative laws:
  - $(A \cap B) \cap C = A \cap (B \cap C)$
  - $(A \cup B) \cup C = A \cup (B \cup C)$
- Distributive law:
  - $(A \cup B) \cap C = (A \cap C) \cup (B \cap C)$
  - $(A \cap B) \cup C = (A \cup C) \cap (B \cup C)$

Proof
These can be proven using Venn diagrams:



□

1.1.4 Cartesian product

Cartesian products are used to construct "higher dimensional" sets from lower dimensions. For example, the Euclidean plane of vectors $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$:

Definition 1.8 (Cartesian product)

The *Cartesian product* $A \times B$ is the set of ordered pairs

$$\{(a, b) : a \in A, b \in B\}.$$

- $\{a, b, c\} \times \{1, 2\} = \{(a, 1), (a, 2), (b, 1), (b, 2), (c, 1), (c, 2)\}$.
- $\mathbb{R} \times \mathbb{R} = \mathbb{R}^2$ ("the xy-plane")

Definition 1.9 (Power set)

The *power set*: $P(A)$ is the set of all subsets of A.

Example 1.10

- $P(\{1, 2\}) = \{\emptyset, \{1\}, \{2\}, \{1, 2\}\}$.
- $P(\{a, b, c\}) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}$.
- $P(\emptyset) = \{\emptyset\} \neq \emptyset$.

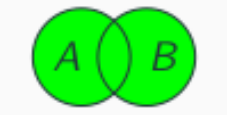
Definition 1.11 (Cardinality)

- $|A|$ denotes the number of elements in a finite set A.
- This is called the *cardinality* of A.
- If $S \subseteq T$, then $|S| \leq |T|$.

Example 1.12

- $|\emptyset| = 0$
- $|\{\emptyset\}| = 1$
- $|\{a, b, c\}| = |\{a, c, c, b, a, c, b, b, a\}| = 3$.

- If $|A| = 9$ and $|B| = 5$, what can we say about $|A \cup B|$?



  - $9 \leq |A \cup B|$.
  - $|A \cup B| \leq 14$.
  - $|A \cup B| \in \mathbb{N}$.
- In general, $|A \cup B| = |A| + |B| - |A \cap B|$.
- If $S \subseteq T$, then $|S| \leq |T|$.

Thus we have

Theorem 1.13

$$\max(|S|, |T|) \leq |S \cup T| \leq |S| + |T|.$$

1.1.5 Enumeration

Next we will go to the idea of *cardinality*, and counting the number of elements in a set. We will denote $|A|$ or $\sharp A$ as the number of elements in A.

- Let $|S| = n$ and $|T| = m$.
- An ordered pair (s, t), where $s \in S$ and $t \in T$, can be chosen in nm ways.
- So $|S \times T| = nm = |S| \cdot |T|$.

Theorem 1.14

Let $A_1, \ldots, A_k$ be finite sets. Then

$$|A_1 \times \cdots \times A_k| = |A_1| \cdot \cdots \cdot |A_k|.$$

- A subset A of $\{1, 2, \cdots, n\}$ is determined by, for each $1 \leq i \leq n$, whether or not $i \in A$.
- So a subset of $\{1, 2, \cdots, n\}$ can be described by a string of n symbols 0 ("out") and 1 ("in").
- Example: The string 001101 corresponds to the set

$$\{3, 4, 6\} \subseteq \{1, \ldots, 6\}.$$

- A subset of $\{1, 2, \cdots, n\}$ corresponds to a string of n symbols 0/1, which is the same as an element of
$$\{0,1\}^n = \underbrace{\{0,1\} \times \cdots \times \{0,1\}}_{n \text{ factors}}$$
- It follows that
$$|P(\{1,\ldots,n\})| = |\{0,1\}^n| = |\{0,1\}|^n = 2^n.$$

Theorem 1.15

Let A be a finite set. Then
$$|P(A)| = 2^{|A|}.$$

1.1.6 Indexing a family of sets and set operations

We can also have multiple sets, which we can index using some sets. Usually they are indexed with natural numbers (finite or infinite subsets), but they can be indexed over any set, like the reals.

Definition 1.16 (Indexed family of sets over finitely many indices)

Let $A_1, A_2, A_3, \cdots A_k \subseteq \Omega$ be sets. We say that
$$\{A_i : 1 \leq i \leq k\}$$
is an *indexed family of sets*. Then
$$\bigcup_{i=1}^{k} A_i = \{x \in \Omega : x \in A_i \text{ for some } 1 \leq i \leq k\}.$$
$$\bigcap_{i=1}^{k} A_i = \{x \in \Omega : x \in A_i \text{ for every } 1 \leq i \leq k\}.$$
This is union and intersection of more than two sets.

Example 1.17

Let $A_1 = \{0, 2, 5\}$, $A_2 = \{1, 2, 5\}$, $A_3 = \{2, 5, 7\}$.
$$\bigcup_{k=1}^{3} A_k = \{0, 1, 2, 5, 7\}.$$
$$\bigcap_{k=1}^{3} A_k = \{2, 5\}.$$

Definition 1.18 (Indexed family over countable index set)

We can do the same for infinitely large families of sets. Let $A_1, A_2, A_3, \cdots \subseteq \Omega$ be sets. We say that

$$\{A_i : i \geq 1\}$$

is an *indexed family of sets*. Then we can define the unions and intersections as follows:

$$\bigcup_{i=1}^{\infty} A_i = \{x \in \Omega : x \in A_i \text{ for some } i \in I\}.$$

$$\bigcap_{i=1}^{\infty} A_i = \{x \in \Omega : x \in A_i \text{ for every } i \in I\}.$$

Example 1.19

Let $\Omega = \mathbb{R}$, and let A_k be the closed interval $A_k = [0, \frac{1}{k}]$ for $k \geq 1$.

$$\bigcup_{k=1}^{\infty} A_k = [0, 1].$$

$$\bigcap_{k=1}^{\infty} A_k = \{0\}.$$

Definition 1.20 (Indexed family over general index set)

We can do the same for other indexing sets as well. Let I be a set. Let $A_i \subseteq \Omega$ be a set, for each $i \in I$. Then

$$\{A_i : i \in I\}$$

is an *indexed family of sets*. We can then define the unions and intersections over this family as follows:

$$\bigcup_{i \in I} A_i = \{x \in \Omega : x \in A_i \text{ for some } 1 \leq i\}.$$

$$\bigcap_{i \in I} A_i = \{x \in \Omega : x \in A_i \text{ for every } 1 \leq i\}.$$

1.1.7 Russel's paradox

"A male barber in the village shaves the beards of precisely those men, who do not shave their own beard."

Does the barber shave his own beard? Whether he does or does not, we get a contradiction. This is an instance of the problem of *self-reference* in set theory.

- For every man x in the village, there is a set S_x consisting of all the men whose beards he shaves.
- For the barber B,
$$S_B = \{x : x \notin S_x\}.$$
- In particular,
$$B \in S_B \Leftrightarrow B \notin S_B,$$
which is a contradiction! We are not allowed to use the set S in the formula that defines S!

For every "universe" Ω and every statement P (without self-reference),

$$\{x \in \Omega : P(x)\} \subseteq \Omega$$

is a set. Let Ω be "the set of all sets", and let

$$S = \{A \in \Omega : A \notin A\}.$$

Is S an element of itself? Again we get a contradiction.

To avoid this kind of contradictions, we decide:

- The "set of all sets" does not exist.
- No set is allowed to be an element of itself.
- All sets must be constructed from "safe and well-understood sets" (like $\mathbb{R}$) by taking
  - Subsets.
  - Cartesian products.
  - Power sets.
  - Unions.

1.2 Formal logic

1.2.1 Statements, closed- and open sentences

We will now move to the concept of formal logic to discuss about statements, their truth values and truth tables, and we will relate these to set theor.

Definition 1.21 (Statement)

A *statement* is a sentence that is either true or false.

Example 1.22

- Statements:
  - $2 \in \mathbb{Z}$
  - $2 = 5$
  - The millionth decimal of π is 7.
  - All mathematicians are bald.
- Not statements:
  - Is $2 + 2 = 4$?
  - This sentence is false.
  - x is an integer.
- Also not a statement:
  - This sentence is true.

Statements are also called *closed sentences*. An *open sentence* is a sentence containing a variable x, that *would have* a truth value of x had a given value. Open sentences are also called *predicates*.

Example 1.23

- Open sentences:
  - NN is the president of Finland.
  - $-1 \leq y \leq 1$.
  - The millionth decimal of π is n.
  - NN is bald.
  - x is an integer.
- Also an open sentence:
  - $1 \leq y \leq -1$.

- There are two ways to make a statement out of an open sentence (like "$-1 \leq y \leq 1$"):
- Assign a value to the variable.
  - "$-1 \leq 0 \leq 1$" is a TRUE statement.
  - "$-1 \leq 19 \leq 1$" is a FALSE statement.
- Quantify.
  - "There exists a real number y, such that $-1 \leq y \leq 1$" is a TRUE statement.
  - "For every real number y, $-1 \leq y \leq 1$" is a FALSE statement.

1.2.2 Quantifiers

Quantifiers are crucial way to discuss about existence and non-existence, and they relate closely to set theory. They are defined as follows

Definition 1.24 ($\forall$ and $\exists$ quantifiers)

- "For every $x \in A$, $P(x)$ holds" is denoted formally

$$\forall x \in A : P(x).$$

- "There is some $x \in A$, for which $P(x)$ holds" is denoted formally

$$\exists x \in A : P(x).$$

Example 1.25

- Which of the following statements are true?
  - $\forall x \in \mathbb{R} : x^2 > 0$.
  - $\exists a \in \mathbb{R} : \forall x \in \mathbb{R} : ax = x$.
  - $\forall n \in \mathbb{Z} : \exists m \in \mathbb{Z} : m = n + 5$.
  - $\exists n \in \mathbb{Z} : \forall m \in \mathbb{Z} : m = n + 5$.
  - On every party, there are two guests who know the same number of other guests.
- 2 and 3 are true, 1 and 4 are false.
- We will revisit 5 later in the course.

1.2.3 Connectives and truth tables

Statements can be connected by logical connectives:

negation	$\neg$	"not"
conjunction	$\wedge$	"and"
disjunction	$\vee$	"or"
implication	$\rightarrow$	"implies", "if ... then ..."
equivalence	$\leftrightarrow$	"if and only if"

- Statements can be quantified:

$\forall$	"for all"
$\exists$	"exists"

- Natural language has many more quantifiers: "many", "five", "infinitely many", "a few", "more than I thought"...

The meaning of connectives are *defined* via *truth tables*. In the following A and B denote statements, and T and F denote the truth values "True" and "False":

A	B	$A \wedge B$
T	T	T
T	F	F
F	T	F
F	F	F

A	B	$A \vee B$
T	T	T
T	F	T
F	T	T
F	F	F

A	$\neg A$
T	F
F	T

A	B	$A \leftrightarrow B$
T	T	T
T	F	F
F	T	F
F	F	T

The least intuitive connective is implication $\rightarrow$. $A \rightarrow B$ should certainly be False if A is True but B is False. What about the other rows?

A	B	$A \rightarrow B$
T	T	?
T	F	F
F	T	?
F	F	?

A statement like

$$(a > 3) \rightarrow (a^2 > 9)$$

"should be" True for any number a.If $a = 4$, this means that $T \rightarrow T$ should be True. If $a = 0$, this means that $F \rightarrow F$ should be True. If $a = -4$, this means that $F \rightarrow T$ should be True.

A	B	$A \rightarrow B$
T	T	T
T	F	F
F	T	T
F	F	T

We *define* the connective $\rightarrow$ by the truth table

A	B	$A \rightarrow B$
T	T	T
T	F	F
F	T	T
F	F	T

A False statement implies everything! For example,

$$\forall x \in \mathbb{R} : (x^2 < 0) \rightarrow (x = 23)$$

is a True statement. Silly, I know. But that's how it has to be. Live with it.

1.2.4 Tautologies

Definition 1.26

A *tautology* is a (composed) statement that is True regardless of the truth values of the elementary statements that it is composed of.

Example 1.27

The following statements are tautologies:

- $(\neg\neg P) \to P$ (double negation)
- $P \vee (\neg P)$ (excluded middle)
- $(P \to Q) \leftrightarrow (\neg Q \to \neg P)$ (contrapositive)
- $(P \leftrightarrow Q) \leftrightarrow ((P \to Q) \wedge (Q \to P))$ (equivalence law)
- These can be *proven* via truth tables.

If $A \to B$ is a tautology (where A and B are composed statements), then we write

$$A \Rightarrow B.$$

This gives us a way to "calculate" with statements. If $A \iff B$ (ie $A \leftrightarrow B$ is a tautology), then we can replace A by B everywhere in our logical reasoning. Often useful in math to replace an implication $P \to Q$ by its *contrapositive* $(\neg Q) \to (\neg P)$.

Example 1.28

- The contrapositive (for $x \in \mathbb{R}$) of

$$\text{if } x > 0 \text{ then } x^3 \neq 0$$

is

$$\text{if } x^3 = 0 \text{ then } x \leq 0.$$

1.2.5 Treasures example

Example 1.29

- Before you are three chests. They all have an inscription.
  - **Chest 1**: Here is no gold.
  - **Chest 2**: Here is no gold.
  - **Chest 3**: Chest 2 contains gold.

- We know that one of the inscriptions is true. The other two are false.
- If we can only open one chest, which one should we open?

Solution.

- **Axiom:** One of the inscriptions is true. The other two are false.
- Let P_i be the statement *"Chest i contains gold"*.
  - **Chest 1:** Here is no gold. $Q_1 := \neg P_1$
  - **Chest 2:** Here is no gold. $Q_2 := \neg P_2$
  - **Chest 3:** Chest 2 contains gold. $Q_3 := P_2$
- The axiom says

$$[Q_1 \wedge (\neg Q_2) \wedge (\neg Q_3)] \vee [(\neg Q_1) \wedge Q_2 \wedge (\neg Q_3)] \vee [(\neg Q_1) \wedge (\neg Q_2) \wedge Q_3]$$

$$\iff$$

$$[(\neg P_1) \wedge (\neg\neg P_2) \wedge (\neg P_2)] \vee [(\neg\neg P_1) \wedge (\neg P_2) \wedge (\neg P_2)] \vee [(\neg\neg P_1) \wedge (\neg\neg P_2) \wedge P_2]\,.$$

$$\iff$$

$$[\neg P_1 \wedge P_2 \wedge \neg P_2)] \vee [P_1 \wedge \neg P_2 \wedge \neg P_2] \vee [P_1 \wedge P_2 \wedge P_2]\,.$$

$$\iff$$

$$[P_1 \wedge \neg P_2] \vee [P_1 \wedge P_2]\,.$$

$$\iff$$

$$P_1$$

- The axiom "One of the inscriptions is true. The other two are false." $\iff$ *"Chest 1 contains gold"*.

- **Lesson 1**: Open the first chest.
- **Lesson 2**: Manipulating propositional statements (by the tautology rule) is "mechanical". Mathematical reasoning *without quantifiers* can be automated.

1.2.6 Negations of quantifiers

What is the negation (opposite) of

$$\forall x \in A : P(x)?$$

Example 1.30

- $A = \{\text{mathematicians}\}$, $P(x) =$"x is bald".
- $\forall x \in A : P(x)$ means "all mathematicians are bald".
- The opposite is "some mathematicians are not bald".

So

$$\neg \forall x \in A : P(x)$$

is equivalent to

$$\exists x \in A : \neg P(x).$$

1.2.7 Computing with logical symbols

We can perform computations with logical symbols, which have consequences also for number theory later on. For example, the first one here is a bit like $-(-1) = 1$:

$$\begin{aligned} (\neg\neg P) &\iff P \\ (P \to Q) &\iff (\neg Q \to \neg P) \\ \exists x \in \Omega : \neg P(x) &\iff \neg \forall x \in \Omega : P(x) \end{aligned}$$

In *constructive mathematics*, one only has the right implication

$$\exists x \in \Omega : \neg P(x) \Rightarrow \neg \forall x \in \Omega : P(x)$$

in the last line. This is philosophically interesting, and also interesting in some algorithmic applications, but will not be relevant in this course.

1.2.8 Sets and predicate logic

Finally we relate sets A and predicates $P(x)$ as follows:

- To any predicate $P(x)$ corresponds a set $\{x \in \Omega : P(x)\}$.

- To the set $S \subseteq \Omega$ corresponds the predicate $x \in S$.
- Sometimes mathematical statements are easier to think about in terms of sets, sometimes in terms of logical symbols.
- To any predicate $P(x)$ corresponds a set $S_P = \{x \in \Omega : P(x)\}$.
- To the predicate $P(x) \wedge Q(x)$ corresponds the set

$$\begin{aligned} S_{P \wedge Q} &= \{x \in \Omega : P(x) \text{ and } Q(x)\} \\ &= \{x \in \Omega : P(x)\} \cap \{x \in \Omega : Q(x)\} = S_P \cap S_Q. \end{aligned}$$

- To the predicate $P(x) \vee Q(x)$ corresponds the set

$$\begin{aligned} S_{P \vee Q} &= \{x \in \Omega : P(x) \text{ or } Q(x)\} \\ &= \{x \in \Omega : P(x)\} \cup \{x \in \Omega : Q(x)\} = S_P \cup S_Q. \end{aligned}$$

1.3 Proof techniques

In mathematics *proofs* are used to verify if a statement is true or not. In this section we will learn about various techniques to prove a statement. If you have not encountered proofs before, this can be quite challenging initially, and it is good to practise first with simple statements with the techniques presented here.

1.3.1 Proof and overview of the proof techniques

In the most abstract version, a mathematical theorem has an *axiom* (or conjunction of axioms) P, and a conclusion Q. A *proof* consists of a sequence of statements such that each row is either

- An axiom or a definition.
- Tautologically implied by the previous rows.
  if previous rows say $p_1, \ldots, p_k$, and $(p_1 \wedge \cdots \wedge p_k) \to q$
  is a tautology, then the next row may say q.
- Obtained from previous lines by "quantor calculus":

$$\begin{aligned} \forall x : \neg P(x) &\Leftrightarrow \neg \exists x : P(x) \\ \exists x : \neg P(x) &\Leftrightarrow \neg \forall x : P(x) \end{aligned}$$

- A special case of a previous row.
  if one row says $\forall x P(x)$, then the next row may say $P(c)$.
- An existential consequence of previous rows.
  if one row says $P(c)$, then the next row may say $\exists x : P(x)$.

Most mathematical proofs uses one of the following tautologies:

Definition 1.31 (Proof techniques)

- $(P \wedge (P \to Q)) \Rightarrow Q$ (Direct proof)
- $(P \wedge (\neg Q \to \neg P)) \Rightarrow Q$ (Contrapositive proof)
- $(P \wedge ((P \wedge \neg Q) \to False) \Rightarrow Q$ (Proof by contradiction)
- $((P_1 \vee P_2) \wedge (P_1 \to Q) \wedge (P_1 \to Q)) \Rightarrow Q$ (Proof by cases)

...and / or the following ways to prove existence:

- $P(c) \Rightarrow \exists x : P(x)$ (Constructive proof)
- $(\neg P(c) \to \exists x : P(x)) \Rightarrow \exists x : P(x)$ (Nonconstructive proof)

Next, we will see examples of all these proof techniques.

1.3.2 Direct proof

Example 1.32

For all odd integers n, then n^2 is also odd.

Proof

- Let n be an *arbitrary* odd integer.
- That means $n = 2k + 1$ for some integer k.
- Then
$$n^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$$
- Since $2k^2 + 2k$ is an integer, this means that n^2 is odd.

□

1.3.3 Contrapositive proof

Example 1.33

For all integers n, if n^2 is odd, then n is also odd.

Proof

- First attempt (direct proof):
- $n^2 = 2k + 1$ for some integer k.
- So $n = \pm\sqrt{2k+1}$, and n is an integer.
- No obvious way to write $n = 2\ell + 1$.

□

Example 1.34

For all integers n, if n^2 is odd, then n is also odd.

Proof
New attempt (contrapositive proof): Need to prove that if n is **not** odd, then n^2 is **not** odd. So assume $n = 2k$ even. Then $n^2 = 4k^2 = 2(2k^2)$ is even, so not odd. Thus, if n were odd, then n^2 must also be odd. □

1.3.4 Proof by contradiction

Example 1.35

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

Proof
Assume the claim was not true, so $\sqrt{2} \in \mathbb{Q}$. Then we could write $\sqrt{2} = \frac{p}{q}$, where p and q are integers with no common divisor. Then $2q^2 = p^2$, so p^2 is even. So p is even, and we can write $p = 2r$, $r \in \mathbb{Z}$ So $q^2 = \frac{p^2}{2} = 2r^2$ is even. Now p and q are both even. But this contradicts our assumption that they had no common divisor. Thus the assumption was false, so $\sqrt{2} \notin \mathbb{Q}$. □

1.3.5 Proof by cases

Recall:

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

Example 1.36

For all real numbers x, y, it holds that $|xy| = |x||y|$.

Proof

- Three cases:
  - Both numbers ≥ 0, so $xy \geq 0$: $|xy| = xy = |x||y|$.
  - Both numbers < 0, so $xy > 0$: $|xy| = xy = (-x)(-y) = |x||y|$.
  - The numbers have different sign, so $xy \leq 0$. Without loss of generality (WLOG) $x < 0 \leq y$:
$$|xy| = -xy = (-x)y = |x||y|.$$
- These cases cover all possibilities, so the claim is true for all $x, y \in \mathbb{R}$.

□

1.3.6 Constructive existence proof

Example 1.37

There exist integers that can be written as a sum of two cubes in more than one way.

Proof

$$12^3 + 1^3 = 1728 + 1 = 1729 = 1000 + 729 = 10^3 + 9^3$$

□

1.3.7 Nonconstructive existence proof

Example 1.38

There exist irrational numbers $x, y \notin \mathbb{Q}$ such that $x^y \in \mathbb{Q}$.

Proof

- The number $a = \sqrt{2}^{\sqrt{2}}$ is of the form x^y, where $x = y = \sqrt{2} \notin \mathbb{Q}$.
- If a is not rational, then $a^{\sqrt{2}}$ is also of the form x^y, where $x = a \notin \mathbb{Q}$ and $y = \sqrt{2} \notin \mathbb{Q}$.
- But
$$a^{\sqrt{2}} = (\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = \sqrt{2}^{(\sqrt{2}\cdot\sqrt{2})} = \sqrt{2}^2 = 2 \in \mathbb{Q}.$$
- So either $x = y = \sqrt{2}$ is an example of numbers with the desired property, or $x = a$, $y = \sqrt{2}$ is.
- So some irrational numbers with this desired property exist.

□

1.3.8 Induction proofs

This proof technique is very useful for number sequences (but also in many other parts of mathematics)

- **Goal:** Prove a statement $P(n)$ for all natural numbers $n \in \mathbb{N}$.
- **Technique:**
  - First (base case) prove the first case $P(0)$.
  - Then (induction step) prove that, for an arbitrary $m \in \mathbb{N}$,
    IF $P(m)$ holds, THEN $P(m+1)$ also holds.
  - These two steps together prove that the statement $P(n)$ holds for any $n \in \mathbb{N}$.

$$P(0) \Rightarrow P(1) \Rightarrow P(2) \Rightarrow P(3) \Rightarrow P(4) \Rightarrow \cdots .$$

Example 1.39

Let a_n be recursively defined by $a_0 = 0$ and $a_{n+1} = 2a_n + 1$. Then $a_n = 2^n - 1$ for all $n \in \mathbb{N}$.

Proof

- Base case: $a_0 = 0 = 1 - 1 = 2^0 - 1$, so the statement is true for $n = 0$.
- Induction step: Assume (*induction hypothesis*) that $a_m = 2^m - 1$. Then

$$a_{m+1} \overset{def}{=} 2a_m + 1 \overset{IH}{=} 2 \cdot (2^m - 1) + 1 = 2^{m+1} - 2 + 1 = 2^{m+1} - 1,$$

  so the statement is also true for $n = m + 1$.
- It follows that the statement $a_n = 2^n - 1$ is true for all $n \in \mathbb{N}$.

□

Example 1.40

Prove that, for every $n \in \mathbb{N}$,

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

Proof

- Base case ($n = 0$):

$$\sum_{i=1}^{0}(2i-1) = \sum_{i\in\emptyset}(2i-1) = 0 = 0^2.$$

- Induction step: Assume (*IH*) that $\sum_{i=1}^{m}(2i-1) = m^2$. Then

$$\begin{aligned}\sum_{i=1}^{m+1}(2i-1) &\overset{def}{=} (2(m+1)-1) + \sum_{i=1}^{m}(2i-1)\\ &\overset{IH}{=} m^2 + 2(m+1) - 1 = m^2 + 2m + 1 = (m+1)^2,\end{aligned}$$

  so the statement is also true for $n = m + 1$.

□

There is also a more general version of the induction proof, which can be useful for certain situations that involve e.g. sequences. The goal is the same:

- **Goal:** Prove a statement $P(n)$ for all natural numbers $n \in \mathbb{N}$.
- **More general technique:**
  - First (base case) prove the k first cases $P(0), \ldots, P(k)$.
  - Then (induction step) prove that, for an arbitrary $m \in \mathbb{N}$,
    IF $P(m-k), \ldots, P(m)$ holds, THEN $P(m+1)$ also holds.
  - These two steps together prove that the statement $P(n)$ holds for any $n \in \mathbb{N}$.

    $$(P(0) \wedge \cdots \wedge P(k)) \Rightarrow (P(1) \wedge \cdots \wedge P(k+1)) \Rightarrow (P(2) \wedge \cdots \wedge P(k+2)) \Rightarrow \cdots .$$

  - How large k needs to be, may depend on the problem.

Example 1.41

The Fibonacci numbers are defined by $f_0 = 0$, $f_1 = 1$ and $f_n = f_{n-1} + f_{n-2}$. For all $n \in \mathbb{N}$ holds $f_n < 2^n$.

Proof

- Base case: $f_0 = 0 < 1 = 2^0$ and $f_1 = 1 < 2 = 2^1$.
- Induction step: Assume (*induction hypothesis*) that $f_m < 2^m$ and $f_{m-1} < 2^{m-1}$. Then

$$f_{m+1} \overset{def}{=} f_m + f_{m-1} \overset{IH}{<} 2^m + 2^{m-1} < 2 \cdot 2^m = 2^{m+1},$$

  so the statement is also true for $n = m + 1$.
- It follows that the statement $f_n < 2^n$ is true for all $n \in \mathbb{N}$.

□

1.4 Relations

Next, we will move to the topic of *relations*. Relations are used in all parts of mathematics, and we can consider them as generalisations of *functions* $f : A \to B$ you may have seen before (we will talk about functions specifically a bit later!), but also have important applications outside of mathematics: Relational databases, automated translation,...

Example 1.42

• $y = x^2$.	$x, y \in \mathbb{R}$.
• $S \subseteq T$.	$S, T \in P(\Omega)$.
• $5 \mid x - y$, *i.e.* $x \equiv y \mod 5$.	$x, y \in \mathbb{Z}$.
• x and y are siblings.	$x, y \in \{\text{humans}\}$.
• $x \leq y$.	$x, y \in \mathbb{R}$.
• $x \mid y$, *i.e.* y is divisible by x.	$x, y \in \mathbb{Z}$.

1.4.1 Definition and different types of relations

Definition 1.43

A *relation* can be defined in any of two different ways (which we will use interchangably):

- A relation on a set A is a subset $R \subseteq A \times A$.
- A relation is an open statement $R(x, y)$ that has a truth value for every $x, y \in A$.

Recall: To the *predicate* $R(x, y)$ corresponds the *set*

$$\{(x, y) \in A^2 : R(x, y)\}.$$

This set is sometimes also denoted R.

Example 1.44

- Let $A = \{1, 2, 3, 4\}$.
- The equality relation $x = y$ on A is given by the set

$$\{(1,1), (2,2), (3,3), (4,4)\} \subseteq A^2.$$

- The order relation $x < y$ on A is given by the set

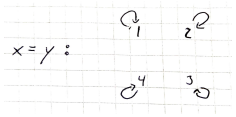
$$\{(1,2), (1,3), (1,4), (2,3), (2,4), (3,4)\} \subseteq A^2.$$

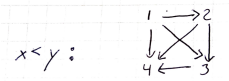
- The divisibility relation $x|y$ on A is given by the set

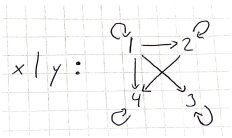
$$\{(1,1), (1,2), (1,3), (1,4), (2,2), (2,4), (3,3), (4,4)\} \subseteq A^2.$$

A relation R on A can also be represented by a *directed graph*.

- *Nodes* corresponding to the elements $x \in A$.
- *Arcs* $x \to y$ if $R(x, y)$ holds.







Example 1.45

If

$$|A| = n,$$

how many relations are there on A? Recall a relation on a set A is a subset $R \subseteq A^2 = A \times A$.

Answer: $|P(A^2)| = 2^{|A \times A|} = 2^{|A| \cdot |A|} = 2^{n^2}$ different relations.

- We can also define a relation "from a set A to a set B":
  - As a subset $R \subseteq A \times B$.
  - As an open statement $R(x, y)$ that has a truth value for every $x \in A, y \in B$.

Example 1.46

- $x \in S$. $x \in \Omega$, $S \in P(\Omega)$.
- x has shoes in size y. $x \in \{\text{humans}\}$, $y \in \mathbb{R}$.
- x is born in year n. $x \in \{\text{humans}\}$, $n \in \mathbb{N}$.

Definition 1.47

A relation $\sim$ on A is called:

- *reflexive* if
$$\forall x \in A : x \sim x.$$
- *symmetric* if
$$\forall x, y \in A : x \sim y \leftrightarrow y \sim x.$$
- *antisymmeric* if
$$\forall x, y \in A : (x \sim y \wedge y \sim x) \rightarrow x = y.$$
- *transitive* if
$$\forall x, y, z \in A : (x \sim y \wedge y \sim z) \rightarrow x \sim z.$$

Definition 1.48

A relation $\sim$ on A is called:

- *reflexive* if
$$\forall x \in A : x \sim x.$$

Example 1.49

- $x \leq y$ on $\mathbb{R}$
- $x|y$ on $\mathbb{Z}$
- $x = y$ on any set
- $x \equiv y \mod n$ on $\mathbb{Z}$
- NOT reflexive: $x < y$ on $\mathbb{R}$
- NOT reflexive: x is a father of y on $\{\text{humans}\}$

Definition 1.50

A relation $\sim$ on A is called:

- *symmetric* if
$$\forall x, y \in A : x \sim y \leftrightarrow y \sim x.$$

Example 1.51

- x and y are siblings — on {humans}
- $|x - y| \leq 1$ — on $\mathbb{R}$
- NOT symmetric: $x - y \leq 1$ — on $\mathbb{R}$

Definition 1.52

A relation $\sim$ on A is called:

- *antisymmeric* if
$$\forall x, y \in A : (x \sim y \wedge y \sim x) \rightarrow x = y.$$

Example 1.53

- $x \leq y$ — $x, y \in \mathbb{R}$
- $S \subseteq T$ — $S, T \in P(\Omega)$

Definition 1.54

A relation $\sim$ on A is called:

- *transitive* if
$$\forall x, y, z \in A : (x \sim y \wedge y \sim z) \rightarrow x \sim z.$$

Example 1.55

- $x - y \in \mathbb{Z}$ — $x, y \in \mathbb{R}$
- $x \leq y$ — $x, y \in \mathbb{R}$
- NOT transitive: x and y have a parent in common.
$x, y \in$ {Humans}.

1.4.2 Equivalence relations

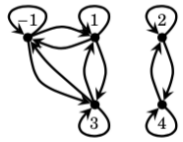
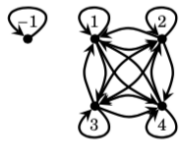
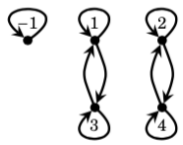
An equivalence relation usually describes "sameness" in some sense.

Definition 1.56

A relation $\sim$ is an *equivalence relation* if it is reflexive, symmetric, and transitive.

Example 1.57

- $x = y$ on any set.
- $x \equiv y \mod n$ $x, y \in \mathbb{Z}$.
- $x - y \in \mathbb{Z}$ $x, y \in \mathbb{R}$.
- $|S| = |T|$ $S, T \in P(\Omega)$.
- x and y have the same biological mother $x, y \in \{\text{Humans}\}$.
- NOT an equivalence relation: $x \leq y$ $x, y \in \mathbb{R}$.
- NOT an equivalence relation: $|x - y| \leq 1$. $x, y \in \mathbb{R}$.

Relation R	Diagram	Equivalence classes (see next page)
"is equal to" (=) $R_1 = \{(-1,-1),(1,1),(2,2),(3,3),(4,4)\}$		$\{-1\}$, $\{1\}$, $\{2\}$, $\{3\}$, $\{4\}$
"has same parity as" $R_2 = \{(-1,-1),(1,1),(2,2),(3,3),(4,4),$ $(-1,1),(1,-1),(-1,3),(3,-1),$ $(1,3),(3,1),(2,4),(4,2)\}$		$\{-1,1,3\}$, $\{2,4\}$
"has same sign as" $R_3 = \{(-1,-1),(1,1),(2,2),(3,3),(4,4),$ $(1,2),(2,1),(1,3),(3,1),(1,4),(4,1),(3,4),$ $(4,3),(2,3),(3,2),(2,4),(4,2),(1,3),(3,1)\}$		$\{-1\}$, $\{1,2,3,4\}$
"has same parity and sign as" $R_4 = \{(-1,-1),(1,1),(2,2),(3,3),(4,4),$ $(1,3),(3,1),(2,4),(4,2)\}$		$\{-1\}$, $\{1,3\}$, $\{2,4\}$

Every equivalence relation on A divides A into disjoint *equivalence classes* of elements that are "same".

Definition 1.58 (Equivalence classes)

- Let $\sim$ be an equivalence relation on A.
- The equivalence class of $a \in A$ is

$$[a] = [a]_\sim = \{x \in A : x \sim a\}.$$

Example 1.59

- Let $\sim$ be congruence modulo 2, on $\mathbb{Z}$.
- $x \equiv y$ if $2|x - y$.
- Then

$$[0] = \{\dots, -4, -2, 0, 2, 4, \dots\} \text{ and } [1] = \{\dots, -3, -1, 1, 3, \dots\}.$$

Theorem 1.60

- Let $\sim$ be an equivalence relation on A, and let $x, y \in A$.
- If $x \sim y$, then $[x] = [y]$.
- If $x \not\sim y$, then $[x] \cap [y] = \emptyset$.

This shows that the equivalence classes form a *partition* of A: Every element in A is in exactly one equivalence class.

Definition 1.61

A partition of a set A is a collection of subsets $A_i \subseteq A$, $i \in I$ such that:

- $A = \bigcup_{i \in I} A_i$.
- $A_i \cap A_j = \emptyset$ for all $i \neq j$.

How many equivalence relations are there on a set with n elements? This is the *Bell number* B_n. (outside the scope of this course). The first few Bell numbers are

$$B_0 = 1, B_1 = 1, B_2 = 2, B_3 = 5, B_4 = 15, B_5 = 52, B_6 = 203, B_7 = 877.$$

The numbers can be computed recursively in a *Bell triangle*. No "closed formula" known.

1.4.3 Partial orders

Remember that in real line, we can talk about some numbers being bigger than others, like $2 < 5$, $2 \leq 2$ or $3 < \pi < 4$. This idea can be introduced as a structure to sets as well, as a relation:

Definition 1.62 (Partial order)

A relation $\preceq$ on A is an *order relation* if it is reflexive, antisymmetric, and transitive.

Example 1.63

- $x \leq y$ on $\mathbb{R}$
- $x|y$ on $\mathbb{N}$
- $S \subseteq T$ on $P(\Omega)$.

An order relation is sometimes called a *partial order*. If $a \preceq b$ and $a \neq b$, then we write $a \prec b$.

Definition 1.64 (Covering relation)

- Let $\preceq$ be an order relation on A.
- Let $a, b \in A$ be elements such that:
  - $a \prec b$
  - $\neg\exists x \in A : a \prec x \prec b$.
- Then we say that b *covers* a, written $a \lessdot b$.

Example 1.65

- $18 \lessdot 19$ in the order $(\mathbb{Z}, \leq)$.
- $3 \lessdot 6$ in the order $(\mathbb{Z}, |)$.
- $\{a, b, c\} \lessdot \{a, b, c, d\}$ in the order $(P(\Omega), \subseteq)$.
- In the order $(\mathbb{R}, \leq)$, there are no covering pairs $a \lessdot b$.

Theorem 1.66

- Let $\preceq$ be an order relation on a *finite* set A, $a, b \in A$.
- $a \prec b$ if and only if there exist $a_1, a_2, \ldots, a_n \in A$ such that

$$a \lessdot a_1 \lessdot a_2 \lessdot \cdots \lessdot a_n \lessdot b.$$

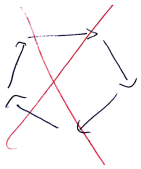
In other words, the order relation is uniquely defined if we know the corresponding covering relation. Note: This is not true if A is infinite.

1.4.4 Hasse diagram

So we can represent a finite order relation $(A, \preceq)$ as a directed graph where we only draw the arcs corresponding to covering pairs:

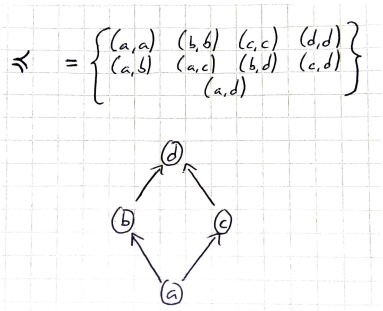
- Nodes are elements of A.
- Arc $a \to b$ if $a \lessdot b$.

Because of antisymmetry, this graph has no *directed cycles*:



When there are no directed cycles, we can draw the directed graph so that all arcs point upwards. This representation of a finite order relation is called its *Hasse diagram*.

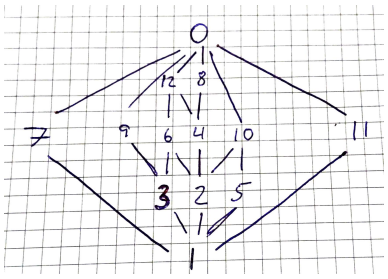
Example 1.67



The head of the arcs are usually not drawn in the Hasse diagram, as we already know that the arcs point upwards.

Example 1.68

The divisibility relation on $\{0, 1, 2, \ldots, 12\}$.



1.4.5 Linear extensions

Definition 1.69 (Linear relations and chains)

An order relation is called *linear*, or *total*, if for every x, y holds that $x \leq y$ or $y \leq x$. A totally ordered set is also called a *chain*.

Example 1.70

- The ordinary order relation $(\mathbb{N}, \leq)$ is linear, because for every two integers, if they are not the same, then one is smaller than the other.
- The divisibility relation $(\mathbb{N}, |)$ is not linear, because (for example) $5 \not| 7$ and $7 \not| 5$.

Definition 1.71 (Compatible linear relations)

A linear relation $\leq$ on a set P is *compatible* with a partial order $\preceq$ on the same set, if for every $x, y \in P$ such that $x \preceq y$, also holds that $x \leq y$. We say that $\leq$ is a *linear extension* of $\preceq$

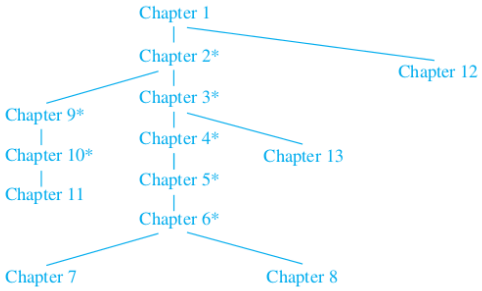
Example 1.72

- The ordinary order relation on $\{1, 2, 3, 4\}$ is a linear extension of the partial order
$$1 \preceq 2, 1 \preceq 3, 1 \preceq 4, 2 \preceq 4, 3 \preceq 4.$$
- Another linear extension of the same partially ordered set would be
$$1 \leq 3 \leq 2 \leq 4.$$

Example 1.73

- The ordinary order relation on $\mathbb{N} \setminus \{0\} = \{1, 2, 3, 4, \dots\}$ is a linear extension of the divisibility relation.
  - A positive integer can never be divisible by any larger integer
- The ordinary order relation on $\mathbb{N} = \{0, 1, 2, 3, \dots\}$ is **not** a linear extension of the divisibility relation.
- Zero is divisible by any positive integer n (because $0 = 0 \cdot n$), although $0 \leq n$.

A partial order $\preceq$ can describe the dependencies of tasks. (Task T $\preceq$ Task S if the outcome of S is needed in order to begin T.) Then, a linear extension of $\preceq$ is an order in which the tasks can be performed.



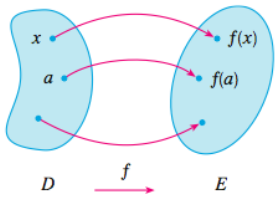
1.5 Functions

Functions are a special class of relations that describe a rule how an element is mapped into another element.

1.5.1 Definition and graphs

Definition 1.74 (Functions)

A *function* $f : A \to B$ is a relation "$f(x) = y$", such that for each element $a \in A$, there is a *unique* element $b \in B$ for which $f(a) = b$ holds.

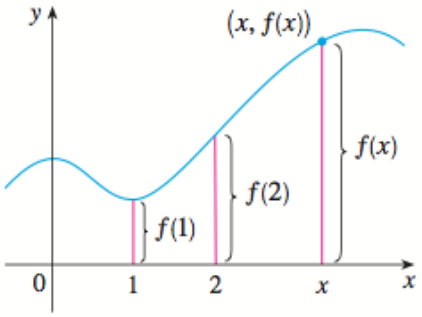


The set A is the *domain* of the function, and B is the *codomain*. The *range* of f is the set $f(A) \stackrel{\text{def}}{=} \{f(x) : x \in A\} \subseteq B$.

Functions can thus be seen as a special case of relations: Every element in the domain is related with some element in the codomain. A function f from A to B is compactly denoted $f : A \to B$. Sometimes a function does not need a name; in such case we write $a \mapsto b$ ("a maps to b") rather than $f(a) = b$. When considering a relation as a subset of $D \times E$, the set corresponding to f is its *graph*

$$\{(x, f(x)) : x \in D\} \subseteq D \times E.$$

A function is often represented geometrically by its graph, especially when the domain and codomain are both (subsets of) $\mathbb{R}$.



Example 1.75

The function

$$\begin{aligned} f :&\mathbb{Z} \to \mathbb{Z} \\ &x \mapsto 4x + 5 \end{aligned}$$

(also written $f(x) = 4x + 5$) has:

- Domain (*määrittelyjoukko*) $\mathbb{Z}$.
- Codomain (*maalijoukko*) $\mathbb{Z}$.
- Range (*arvojoukko*)

$$\{4x + 5 : x \in \mathbb{Z}\} = \{\dots, -7, -3, 1, 5, 9, \dots\}.$$

- Graph (*kuvaaja*)

$$\{(x, y) : y = 4x + 5\} \subseteq \mathbb{Z}^2.$$

1.5.2 Composition of functions

Two functions $f : A \to B$ and $g : B \to C$ can be *composed* into a function $g \circ f : A \to C$, $g \circ f(x) = g(f(x))$.

Example 1.76

The function $h(x) = 2^{x^2+1}$ can be written as $g \circ f$, where $g(y) = 2^y$ and $f(x) = x^2 + 1$.

Example 1.77

- The function $h(x) = 2^{x^2+1}$ can be written as $g \circ f$, where $g(y) = 2^y$ and $f(x) = x^2 + 1$.
- $$x \overset{f}{\longmapsto} x^2 + 1 \overset{g}{\longmapsto} 2^{x^2+1}.$$
- This is **not** the same as the composition $f \circ g$:

$$x \overset{g}{\longmapsto} 2^x \overset{g}{\longmapsto} (2^x)^2 + 1 = 4^x + 1.$$

1.5.3 Injection, surjection, bijection

Next we will discuss three important notions of functions, which we will use later for example in checking whether two sets have same number of elements or not.

Definition 1.78

A function $f : A \to B$ is called

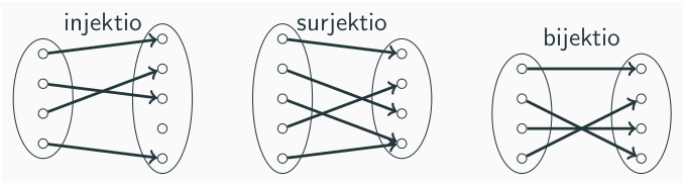
- *Injective* (or one-to-one) if

$$\forall x, y \in A : f(x) = f(y) \Rightarrow x = y.$$

- *Surjective* (or onto) if

$$\forall b \in B : \exists a \in A : f(a) = b.$$

- *Bijective* (or invertible) if it is injective and surjective.



injektio = injection, surjektio = surjection, bijektio = bijection

1.5.4 Inverse functions

Definition 1.79

The *inverse* of the bijective function $f : A \to B$ is the function $g = f^{-1} : B \to A$ such that

$$f(a) = b \iff g(b) = a.$$

This defines the inverse function f^{-1} uniquely. If $f : A \to B$ is not bijective, then it can not have an inverse $B \to A$. Warning: Do not mistake the *function* f^{-1} for the *number* $f(x)^{-1} = \frac{1}{f(x)}$.

1.6 Cardinalities

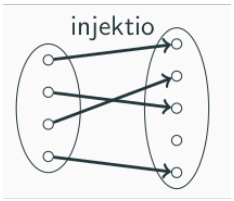
Next, we will apply the idea of injections, surjections and bijections to talk about *cardinalities* again and we can use them to formally define the cardinality of any set by using functions:

Theorem 1.80

Let A and B be finite sets. Then $A \to B$ injective $\Rightarrow n = |A| \leq |B|$.

Proof

If there is an injection $A = \{a_1, \ldots, a_n\} \to B$, then $f(a_1), \ldots, f(a_n)$ are all *different* elements of B.



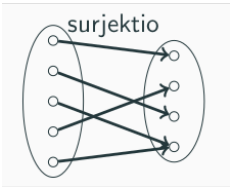
□

Theorem 1.81

Let A and B be finite sets. Then $A \to B$ surjective $|A| \geq |B| = m$.

Proof

If there is a surjection $A \to B = \{b_1, \ldots, b_m\}$, then there are *different* elements $a_1, \ldots a_m \in A$ such that $f(a_i) = b_i$ for $i = 1, \ldots, m$.



□

For finite sets, there is an injective map $A \to B$ precisely if B has at least as many elements as A. For general sets, we take this as the *definition* of cardinality (i.e. "number of elements")

Definition 1.82

Let A and B be sets. We say that:

- $|A| = |B|$ if there exists a bijection $A \to B$.
- $|A| \leq |B|$ if there exists an injection $A \to B$.

Fact (from exploratory exercises): There is a surjection $B \to A$ if and only if there is an injection $A \to B$. Assuming a technical axiom about sets, called the axiom of choice. Do not worry about this.

Definition 1.83 (Finite, countable and uncountable sets)

Note that $|A| = n$ if there is a bijection $A \to \{1, 2, \ldots, n\}$. The set A is *finite* if $|A| = n$ for some $n \in \mathbb{N}$. Otherwise it is *infinite*. For any infinite set A, there is an injection $\mathbb{N} \to A$. So $|\mathbb{N}| = \aleph_0$ is "the smallest infinite cardinality". The set A is *countable* if $|A| = |\mathbb{N}|$. If $|A| > |\mathbb{N}|$, then we say that A is *uncountable*.

Theorem 1.84

$|\mathbb{N}| = |\{0, 2, 4, 6, 8, \ldots\}|$

Proof

- Define $f : \mathbb{N} \to \{0, 2, 4, 6, 8, \ldots\}$ by $f(n) = 2n$ for all $n \in \mathbb{N}$.
- Then f is a bijection.
- Inverse function $m \mapsto \frac{m}{2} \in \mathbb{N}$ for $m \in \{0, 2, 4, 6, 8, \ldots\}$.

□

Note: for infinite sets A, B, it is very possible that $|A| = |B|$ even when $A \subsetneq B$.

1.6.1 Infinite cardinalities

Example 1.85 (Hilbert's hotel)

- David Hilbert is checking in to a hotel with infinitely many rooms (numbered $0, 1, 2, \ldots$)
- Unfortunately, every room is already occupied.
- Solution: All guests move rooms: The guest who used to stay in room k moves to room $k + 1$ for all $i \in \mathbb{N}$.
- Now, Hilbert can move into room 0.

Example 1.86 (Hilbert's hotel, infinitely many new guests)

- The next day a bus arrives to the hotel, bringing infinitely (but countably) many new guests.
- Unfortunately, every room is already occupied.
- Solution: All guests move rooms: The guest who used to stay in room k moves to room $2k$ for all $i \in \mathbb{N}$.
- Now, the bus tourists can move into all odd numbered rooms.

Example 1.87 (Hilbert's hotel, infinite number of new buses!)

- The next day, **infinitely** many buses (numbered $1, 2, 3, \dots$) arrive to the hotel, all bringing infinitely (but countably) many new guests.
- Solution: All previous guests move to odd numbered rooms.
- Now, the passengers on bus number k can move into rooms numbered $2^k, 2^k \cdot 3, 2^k \cdot 5, 2^k \cdot 7, \dots$.

Theorem 1.88

The relation $|A| = |B|$ (between pairs of sets) is an equivalence relation (on $P(\Omega)$).

Proof

- Reflexivity: The identity map $\iota : A \to A$ is a bijection.
- Symmetry: If $f : A \to B$ is a bijection, then $f^{-1} : B \to A$ is a bijection.
- Transitivity: If $f : A \to B$ and $g : B \to C$ are bijections, then $g \circ f : A \to C$ is a bijection.

□

Theorem 1.89

- $|\mathbb{N}| = |\mathbb{Z}|$

Proof

- Define $f : \mathbb{N} \to \mathbb{Z}$ by

$$f(0) = 0, f(2k) = k \text{ and } f(2k-1) = -k \text{ for } k \geq 1.$$

- Then f is a bijection.

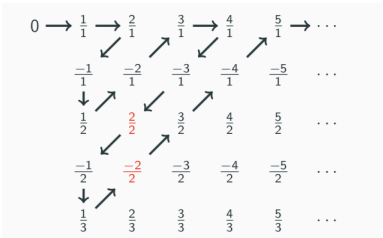
□

Theorem 1.90

- $|\mathbb{N}| = |\mathbb{Q}|$

Proof

- Order the numbers $\frac{p}{q}$, $p, q \in \mathbb{Z}$, $q > 0$, as in the figure:



- Let $f(n)$ be the n^{th} "new" number in the sequence, for $n \in \mathbb{N}$.
- Then $f : \mathbb{N} \to \mathbb{Q}$ is a bijection.

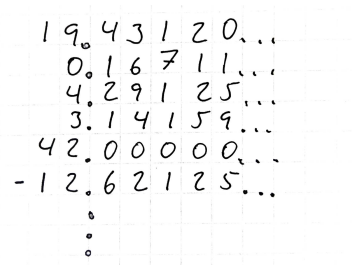
□

Theorem 1.91

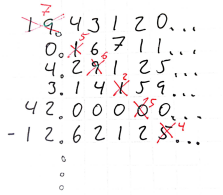
- $|\mathbb{N}| \neq |\mathbb{R}|$

Proof

- Assume for a contradiction that we can "list" the real numbers as in the figure



- Change the i^{th} decimal digit of the i^{th} number, in any way you want.



- The "diagonal number" (in the example $7.56254\ldots$) was not in the original list.
- Contradiction, so $|\mathbb{N}| \neq |\mathbb{R}|$.

□

Recall: $|A| \leq |B|$ if there exists an injection $A \to B$.

Theorem 1.92

- $|A| \leq |B| \leq |C| \implies |A| \leq |C|$.

Proof

- If $f : A \to B$ and $g : B \to C$ are injections, then $g \circ f : A \to C$ is an injection.

□

Theorem 1.93 (Not proved in this course)

- If $|A| \leq |B|$ and $|B| \leq |A|$, then $|A| = |B|$.
  - This is a nice and challenging problem - Try it at home!
- For any sets A and B holds that $|A| \leq |B|$ or $|B| \leq |A|$.
  - This is a deep fact, and not true in *constructive mathematics* - Do not try it at home!