On sets, functions and relations

Rosalie Iemhoff

Contents

1 Introduction

Sets, functions and relations are some of the most fundamental objects in mathematics. They come in many disguises: the statement that 2+3=5 could be interpreted as saying that a set of two elements taken together with a set of three elements results in a set of five elements; it also means that the function +, when given the input 2 and 3, outputs the number 5; in saying that the probability of the number 2 is 1/6 when throwing a dice, one states that the set of outcomes of throwing a dice has six elements that occur with equal probability. In other settings the presence of sets, functions or relations is more evident: every polynomial is a function, in analysis one studies functions on the real numbers, in computer science functions play an essential role, as the notion of an algorithm is central in the field.

In these notes we will study some elementary properties of sets, functions and relations. Although this exposition will be mainly theoretical it is always instructive to keep in mind that through the study of these basic notions one obtains knowledge about the subjects in which these notions play a role, as e.g. in the examples above.

2 Sets

In this section the properties of sets will be studied. Interestingly, we have to start with an informal intuition about what a set is and what it means for an element to belong to a set, without describing it formally. This is not to say that one cannot approach the subject more precisely, but such an approach is related to many deep and complex problems in mathematics and its foundations, and therefore falls outside the scope of this exposition.

Taken that one has an intuition about what these two undefined notions set and membership are, one can, surprisingly enough, build all of mathematics on these two notions. That is, all the mathematical objects and methods can, at least in principle, be cast in terms of sets and membership, not using any other notions.

What is the intuition behind sets and their elements? In general, a set consists of elements that share a certain property: the set of tulips, the set of people who were born in July 1969, the set of stars in the universe, the set of real numbers, the set of all sets of real numbers. A special set is the empty set, that is the set that does not contain any elements. In contrast, do you think a set containing everything exists?

2.1 Notation

Sets are denoted by capitals, often X, Y or A, B, the elements of sets by lower case letters. $x \in X$ means that x is an element of the set X. Sets can be given by listing their elements: $\{0, 1, 2, 3, 4\}$ is the set consisting of the five elements

0, 1, 2, 3 and 4; $\{a, 7, 000\}$ consists of the elements a, 7, and 000. The elements of a set do not have to have an order and do not occur more than once in it: thus $\{1, 2, 1\}$ is the same set as $\{2, 1\}$.

Sometimes we cannot list the elements of a set and have to describe the set in another way. For example: the set of natural numbers; the set of all children born on July 12, 1969. Of course, the elements of the latter could be listed in principle, but it is much easier to describe the set in the mentioned way. Even sets of one element can be difficult to list, such as the set consisting of the 2^{1000}th digit of π. It has one elements, but we cannot compute it fast enough to know the answer before the end of time. Sets given by descriptions are often denoted as follows:

$$\{n \in \mathbb{N} \mid \ n \text{ is an even natural number}\},$$

$$\{p \in \mathbb{N} \mid \ p \text{ is a prime number}\}.$$

Thus given a set A

$$\{x \in A \mid \varphi(x)\}$$

denotes the set of elements of A for which φ holds. Thus the symbol $|$ can be read as "for which". Here φ is a property, which in a formal setting is given by a formula and in an informal setting by a sentence.

The set $\{x \in A \mid \varphi(x)\}$ can also be denoted as $\{x | x \in A, \varphi(x)\}$. I have a slight preference for the first option, but the second one is correct too.

Example 1

1. $\{n \in \mathbb{N} \mid \ n \text{ is odd }\}$ is the set of odd numbers, and whence is the same as the set $\{n \in \mathbb{N} \mid \exists m\, (n = 2m + 1)\}$.
2. $\{w \mid w \text{ is a sequence of 0's and 1's which sum is 2 }\}$ is a set, the same set as $\{w \mid w \text{ is a sequence of 0's and 1's containing exactly two 1's }\}$.
3. $\{\varphi \mid \varphi \text{ is a propositional tautology }\}$ is the set of propositional formulas that are true.

Some specific sets that one should know:

$\mathbb{N}$	the set of natural numbers $\{0, 1, 2, \dots\}$ (de natuurlijke getallen)
$\mathbb{Z}$	the set of integers $\{\dots, -2, -1, 0, 1, 2, \dots\}$ (de gehele getallen)
$\mathbb{Q}$	the set of rational numbers (de rationale getallen)
$\mathbb{R}$	the set of real numbers (de reële getallen)
$\mathbb{C}$	the set of complex numbers (de complexe getallen)
$\emptyset$	the empty set.

For any number n, $\mathbb{N}_{\geq n}$ denotes the set $\{n, n+1, \dots\}$, and $\mathbb{N}_{>n}$ denotes the set $\{n+1, \dots\}$, and similarly for the other sets in the list above. $\mathbb{N}_{\geq 1}$, or equivalently $\mathbb{N}_{>0}$, is sometimes denoted by $\mathbb{N}^{+}$. For a finite set X, $\mid X \mid$ denotes the number of elements of X. A set that consists of one element is called a *singleton*. Thus $\{0\}$ is a singleton, and so is $\{\emptyset\}$.

2.2 Careful

We have to be careful with the $\{\dots\}$-notation. Consider the object

$$N = \{x \mid x \text{ is a set}, x \notin x\}.$$

Thus N consists of the sets that are not an element of itself. Does N belong to this set (itself) or not? If it does, thus if $N \in N$, then, by definition of N, also $N \notin N$. This cannot be, and thus we conclude that $N \notin N$. But then, by the definition of N, also $N \in N$. This cannot be either. Our only conclusion can be that N itself is not a set! Intriguing as this example might be, we will in the following always remain on safe ground and not consider pathological cases like this one. In mathematics, in the field called *set theory*, the problem can be dealt with in a precise and satisfactory way.

2.3 Operations on sets

These are three standard operations on sets that often occur:

$A \cap B$	$=$	$\{x \mid x \in A \text{ and } x \in B\}$	intersection (doorsnede)
$A \cup B$	$=$	$\{x \mid x \in A \text{ or } x \in B\}$	union (vereniging)
$A \backslash B$	$=$	$\{x \in A \mid x \notin B\}$	difference (verschil)

2.4 Subsets

$X \subseteq Y$ means that X is a *subset* of Y, i.e. every element of X is an element of Y. Thus

$$X \subseteq Y \Leftrightarrow \forall x\,(x \in X \Rightarrow x \in Y).$$

We write $X \subset Y$ if $X \subseteq Y$ and $X \neq Y$. Thus $\{1,2\} \subset \{1,2,3,4\}$, and $\mathbb{N} \subset \mathbb{Z}$. There is another important operation on sets, namely the set of all subsets of a set, the so-called *powerset* of a set:

$$P(Y) = \{X \mid X \subseteq Y\}.$$

Thus $P(\{1,2\}) = \{\emptyset, \{1\}, \{2\}, \{1,2\}\}$, in words: $\{\emptyset, \{1\}, \{2\}, \{1,2\}\}$ is the powerset of $\{1,2\}$. $P(\mathbb{R})$ is the set of sets of real numbers. E.g. $\{1, \pi, -72\} \in P(\mathbb{R})$, but $\{1, \pi, -72\} \notin P(\mathbb{N})$. What do you think is $P(\emptyset)$?

Theorem 1 For finite sets X:

$$\mid P(X) \mid = 2^{|X|}.$$

Proof Consider a set X with n elements. Put the elements of X in a certain order, it does not matter which, say $X = \{x_1, \dots, x_n\}$. There is a correspondence between sequences of 0's and 1's of length n, and subsets of X. Given a sequence $i_1, \dots, i_n$ of 0's and 1's, let it correspond to the subset X consisting of exactly those x_{i_j} for which $i_j = 1$, for $1 \leq j \leq n$. Note that every sequence correponds to a unique subset of X and vice versa. There are 2^n such sequences, and thus as many subsets of X. $\heartsuit$

2.5 Exercises

1. Write in set-notation the set of numbers that are squares of natural numbers.
2. Write in set-notation the set of all vowel letters.
3. Give three set-notations for the set of non-negative integers divisable by 3.
4. Give the set-notation of the set consisting of (the name of) the present queen or king of the Netherlands. What is likely to be the set-notation for this set in the year 2015?
5. Describe in words the set $\{x \in \mathbb{Q} \mid 0 < x < 1\}$.
6. Describe in words the set $\{x \in \mathbb{R} \mid \exists y \in \mathbb{Q}(x = y^2)\}$.
7. Describe in words the set $\{x \in \mathbb{R} \mid \exists y \in \mathbb{R}(x = y^2 \ \wedge \ y > 2)\}$.
8. How many elements has the set $\{x \in \mathbb{R} \mid x^2 = x\}$? Give a different set-notation for the set.
9. Give an example of a set for which it is (at present) difficult to decide if it is empty or not.
10. Prove that $C \backslash (A \cap B) = (C \backslash A) \cup (C \backslash B)$.
11. Is $X \backslash Y$ equal to $Y \backslash X$? Explain your answer.
12. Is $\mathbb{N} \subseteq \mathbb{Z}$? And $\mathbb{R} \subseteq \mathbb{Q}$?
13. Give $P(\emptyset)$.
14. Given a set X, is $\emptyset$ an element of $P(X)$? And is $X \in P(X)$?
15. Show that $X \subseteq Y$ and $Y \subseteq Z$ implies $X \subseteq Z$.
16. Write down the subsets of $\{1, 2, 3, 4\}$.
17. How many subsets has $\{n \in \mathbb{N} \mid 0 \leq n \leq 5\}$? And $\mathbb{N}$?
18. Prove that if $X \neq Y$, then $P(X) \neq P(Y)$.

3 Relations

The elements of a set are not ordered. That is, $\{1, 2\}$ is the same set as $\{2, 1\}$. One sometimes calls such sets with two elements an *unordered pair*. In this section the notion of relation is introduced, which are sets with an order structure.

It is instructive to first consider the use of the word relation in daily speach. In the following sentences the word occurs explicitly: John has a relationship with Mary. Health and smoking are related. There is no relation between intelligence and gender. From these examples one can conclude that a relation, in many cases, is a "something" between two things. In these sentences the relation is implicit: John loves Mary, I have read Tolstoy's War and Peace. Here "to love" is a relation and so is "have read". These examples show that a relation is not necessarily symmetric: it might be that John loves Mary but she does not love him. You read these notes, but they do not read you.

On a more formal level we define an *ordered pair* to be a pair of two elements, denoted by $\langle a, b\rangle$. We want to cast it in terms of sets, those being our building blocks for the other mathematical notions. Therefore, we define

$$\langle a, b\rangle =_{def} \{\{a\}, \{a, b\}\}.$$

Note that this is a definition. Thus one has to verify that it has the properties ones wishes an ordered pair to have. It does: from $\{\{a\}, \{a, b\}\}$ we can read of which element is the first of the ordered pair, a, and which is the second, b. And

$$\langle a, b\rangle = \langle c, d\rangle \Leftrightarrow (a = c \text{ and } b = d).$$

A *binary relation* is a set of ordered pairs. Often we leave out the word binary. Note that a relation is a set which elements are of a special form. Clearly, $\{\langle 1, 2\rangle, \langle 3, 4\rangle\}$ is a relation, a relation consisting of two pairs. And so is $\{\langle a, b\rangle, \langle b, a\rangle\}$. The relation

$$\{\langle i, j\rangle \mid i, j \in \mathbb{R}, i < j\}$$

consists of all pairs of real numbers for which the second element is larger than the first element. And

$$\{\langle i, j\rangle \mid i, j \in \mathbb{N}, \exists n \in \mathbb{N}(i^j = 2n)\}$$

is the relation consisting of all pairs of natural numbers such that the first number to the power of the second number is even. Unwinding the definition of ordered pair one readily sees that e.g. $\{\langle 1, 2\rangle, \langle 3, 4\rangle\}$ is short for

$$\{\langle 1, 2\rangle, \langle 3, 4\rangle\} = \{\{\{1\}, \{1, 2\}\}, \{\{3\}, \{3, 4\}\}\}.$$

(So it is clear why we stick to the $\langle\rangle$ notation ...) Note that a subset of a relation is also a relation. We sometimes write xRy for Rxy, and $xRyRz$ for xRy ánd yRz.

Here follow some definitions of important relations.

$$\leq_{\mathbb{N}} = \{\langle m,n\rangle \in \mathbb{N}^2 \mid m \leq n\} \qquad <_{\mathbb{N}} = \{\langle m,n\rangle \in \mathbb{N}^2 \mid m < n\}.$$

Similar notions we define for $\mathbb{Z}$, $\mathbb{Q}$, and $\mathbb{R}$. When R is a relation on a set A, i.e. $R \subseteq A \times A$, we sometimes denote it as (A, R) to stress that it is a relation on A. Thus $\leq_{\mathbb{N}}$ denotes the same relation as $(\mathbb{N}, \leq)$, etc.
Relations are everywhere. Here follow some examples.

Example 2

$\leq_{\mathbb{N}}$ is a relation.

The set $\{\langle a,b\rangle \mid$ a is the husband of b $\}$ is a relation on the set of human beings.

The set $\{\langle q,r\rangle \in \mathbb{Q}_{\geq 0} \times \mathbb{R} \mid \sqrt{q} = r\}$ is a relation.

The set $\{\langle q,r\rangle \in \mathbb{Q} \times \mathbb{R} \mid (q \geq 0$ and $\sqrt{q} = r)$ or $(q < 0$ and $r = 0)\}$ is a relation.

$\{\langle w,n\rangle \mid$ w is a sequence of n 0's and n 1's $\}$ is a relation.

$\{\langle \varphi,\psi\rangle \in \mathcal{P}^2 \mid \varphi$ is equivalent to $\psi\}$ is a relation on the set of propositional formulas $\mathcal{P}$.

Since $\{x\} \subseteq \{x,y\}$, $\{x\} \in P(\{x,y\})$. Also, $\{x,y\} \in P(\{x,y\})$. Thus

$$\{\{x\},\{x,y\}\} \subseteq P(\{x,y\}).$$

That is, $\langle x,y\rangle \subseteq P(\{x,y\})$. Whence

$$\langle x,y\rangle \in P(P(\{x,y\})).$$

3.1 Cartesian product

The *cartesian product* of two sets A and B is the set

$$A \times B =_{def} \{\langle a,b\rangle \mid a \in A, b \in B\}.$$

Note that the cartesian product of two sets is a relation.

Example 3

1. $\{1,2\} \times \{3,4\} = \{\langle 1,3\rangle, \langle 1,4\rangle, \langle 2,3\rangle, \langle 2,4\rangle\}$.
2. $\mathbb{R}^2 = \mathbb{R} \times R$ can be seen as the set of coordinates of points in the plane.
3. There is a correspondence between rational numbers and pairs of integers: n/m naturally corresponds to the pair $\langle n,m\rangle$ (for $m \neq 0$). One rational corresponds to more than one pair, e.g. 1 corresponds to all pairs $\langle n,n\rangle$.

3.2 Pictures

There is an elegant way of depicting relations on a set, i.e. relations $R \subseteq A^2$. We draw Rxy as

$$x \longrightarrow y$$

Thus the picture that corresponds to the relation $\{\langle 0,1\rangle, \langle 0,2\rangle, \langle 1,2\rangle\}$ is

$$\begin{tikzcd}
1 \arrow[rr] & & 2 \\
& 0 \arrow[ul] \arrow[ur] &
\end{tikzcd}$$

And $\{\langle 0,0\rangle, \langle 0,1\rangle, \langle 0,2\rangle, \langle 1,2\rangle, \langle 2,1\rangle\}$ corresponds to the picture

$$\begin{tikzcd}
1 \arrow[rr, bend left] & & 2 \arrow[ll, bend left] \\
& 0 \arrow[ul] \arrow[ur] \arrow[loop right] &
\end{tikzcd}$$

Using suggestive dots we can also draw infinite relations, e.g.

$$\{\langle 0,1\rangle, \langle 0,2\rangle, \langle 0,3\rangle, \dots\} \cup \{\langle 1,2\rangle, \langle 2,3\rangle, \langle 3,4\rangle, \dots\},$$

with picture

$$\begin{tikzcd}
1 \arrow[r] & 2 \arrow[r] & 3 \arrow[r] & {} \arrow[r, dotted] & \cdots \\
& 0 \arrow[ul] \arrow[u] \arrow[ur] \arrow[urr, dotted] \arrow[urrr, dotted] & & &
\end{tikzcd}$$

3.3 Properties of relations

Here follow the names and corresponding picture for some important properties of relations. Dotted arows denote the arrows that have to exist given the solid arrows.

reflexive $\quad \forall w(Rww)$

$$\begin{tikzcd} w \arrow[loop right] \end{tikzcd}$$

transitive $\quad \forall w \forall v \forall u(Rwv \wedge Rvu \to Rwu)$

$$\begin{tikzcd} w \arrow[r] \arrow[rr, dotted, bend right] & v \arrow[r] & u \end{tikzcd}$$

symmetric $\quad \forall w \forall v(Rwv \to Rvw)$

$$\begin{tikzcd} w \arrow[r, bend left] & v \arrow[l, dotted, bend left] \end{tikzcd}$$

euclidean $\quad \forall w \forall v \forall u(Rwv \wedge Rwu \to Rvu)$

$$\begin{tikzcd} v \arrow[rr, dotted] & & u \\ & w \arrow[ul] \arrow[ur] & \end{tikzcd}$$

dense $\quad \forall w \forall v(Rwv \to \exists u(Rwu \wedge Ruv))$

$$\begin{tikzcd} w \arrow[rr] \arrow[dr, dotted] & & v \\ & u \arrow[ur, dotted] & \end{tikzcd}$$

The following properties are a bit harder to draw. Therefore only their descriptions are given.

antisymmetric	$\forall x \forall y(Rxy \wedge Ryx \to x = y)$
weakly connected	$\forall x \forall y(Rxy \vee Ryx \vee x = y)$
partial order	reflexive, transitive and antisymmetric
total (linear) order	weakly connected partial order
equivalence relation	reflexive, transitive and symmetric

serial	$\forall x \exists y(Rxy)$
completely disconnected	$\forall x \forall y \neg(Rxy)$
well-founded	there is no infinite chain $Rx_2x_1 \wedge Rx_3x_2 \wedge Rx_4x_3 \ldots$

Thus in a well-founded frame this cannot occur:

$$\cdots \dashrightarrow x_4 \longrightarrow x_3 \longrightarrow x_2 \longrightarrow x_1$$

Although elements of (the pairs in) relations always range over sets, these sets are not always mentioned. For example, in the definitions given above all quantifiers should be restricted to sets, but we have not done so since these are in general clear from the context. For example, a relation R on a set A is reflexive if $\forall w \in A(Rww)$. A relation on the cartesian product $A \times B$ is serial if $\forall w \in A \exists v \in B(Rwv)$. And R is total on A if it is a partial order and $\forall x \in A \forall y \in B\,(Rxy \vee Ryx \vee x = y)$. Do you see what this implies for A and B?

It is instructive to see what the properties discussed above become when applied to a relation that is a cartesian product $A \times B$. For example, it is serial if $\forall a \in A \exists b \in B(\langle a, b\rangle \in A \times B)$, that is, if B is not empty. And it is symmetric if $A = B$. You will be asked to prove this in the exercises.

Example 4

1. $\leq_{\mathbb{N}}$ is a reflexive, transitive, linear, antisymmetric, and dense relation: $n \leq n$ (reflexivity); $k \leq n \leq m$ implies $k \leq m$ (transitivity); $n \leq m$ or $m \leq n$ or $n = m$ (linearity); $n \leq m \wedge m \leq n$ implies $m = n$ (antisymmetry); if $n \leq m$, then $n \leq n \leq m$ (dense).
2. Note that $<_{\mathbb{N}}$ has the same properties as $\leq_{\mathbb{N}}$ except that it is not reflexive (since not $n < n$) and not dense, since $1 < 2$ but there is no $n \in \mathbb{N}$ such that $1 < n < 2$.
3. $<_{\mathbb{R}}$ is dense, and so is $<_{\mathbb{Q}}$.
4. The relation “eat” has none of the above mentioned properties.
5. The relation “to meet” between human beings is symmetric.
6. The relation $\{\langle r, s\rangle \in \mathbb{R}^2 \mid x^2 = y\}$ is not linear.
7. $P(A)$ with the relation $\subseteq$ is a partial order. You will be asked to prove this in the exercises.

3.4 Equivalence relations

The rationals are a funny collection of numbers: $-5/8$ is a rational number, and so are $2/7$ and $4/14$, but although given by different expressions, the last two numbers $2/7$ and $4/14$ are considered to be “the same”, just like for example -1 and $-9/-9$. How can we express this sameness? Via an equivalence relation that in some sense collects all rationals that are the same in one set, the equivalence class of a rational. We first introduce equivalence relations in general, and then return to $\mathbb{Q}$.

Equivalence relations give rise to a partition of a set in the following way. If R is an equivalence relation on a set A, then we define the *equivalence class* of an element a as the set $\{b \in A \mid Rab\}$, and denote it by $[a]_R$, or by $[a]$, when R is clear from the context. Note that because R is symmetric, $[a]$ is the same set as $\{b \in A \mid Rba\}$. Because R is reflexive, $a \in [a]$. The set $\{[a] \mid a \in A\}$ is denoted by A/R.

Example 5 1. $\{\langle a, b\rangle \mid$ persons a and b have the same birthday $\}$ is an equivalence relation.

Theorem 2

$$\forall b \in [a] : \;\; [a] = [b].$$

Proof If $b \in [a]$ then Rab, and thus Rba since R is symmetric. We show that $[a] = [b]$. First, if $c \in [b]$, then Rbc. Since also Rab, Rac follows by transitivity, and thus $c \in [a]$. Second, if $c \in [a]$, then Rac. Since also Rba, Rbc follows by transitivity, and thus $c \in [b]$. This proves that $[a] = [b]$. ♡

Theorem 3

$$\forall b \notin [a] : \;\; [a] \cap [b] = \emptyset.$$

Proof If there would be a c in $[a] \cap [b]$, then Rac because $c \in [a]$ and Rcb because $c \in [b]$. Hence Rab by transitivity, and thus $b \in [a]$. ♡

From the two theorems above it follows that

Corollary 1 The set $\{[a] \mid a \in A\}$ is a partitioning of A into disjoint sets given by the equivalence classes.

3.4.1 The rational numbers

The beauty of all this is that we can define $\mathbb{Q}$ in terms of $\mathbb{Z}$ using the following equivalence relation on $\mathbb{Z} \times \mathbb{N}_{>0}$:

$$\langle x, y\rangle \sim \langle a, b\rangle \;\Leftrightarrow\; xb = ya.$$

In the exercises you will be asked to show that $\sim$ is indeed an equivalence relation. An instance of the relation is for example $\langle 2, 7\rangle \sim \langle 4, 14\rangle$, and a non instance is that not $\langle -5, 8\rangle \sim \langle 1, 1\rangle$. In terms of equivalence classes this reads: $[\langle 2, 7\rangle] = [\langle 4, 14\rangle]$ and $[\langle -5, 8\rangle] \neq [\langle 1, 1\rangle]$. Now we could define the rationals $\mathbb{Q}$ as

$$\mathbb{Z} \times \mathbb{N}_{>0} / \sim$$

and obtain a set that has precisely the properties of the rational numbers. We could do a similar thing for $\mathbb{R}$, i.e. define it in terms of simpler sets, but this falls outside the scope of these notes.

3.5 Relations of arbitrary arity

Above we saw relations between two elements. Of course, there are also relations between more than two elements. For example the relation "being the mother and the father of", i.e. the relation consisting of triples $\langle a, b, c\rangle$ such that a is the mother and b is the father of c. Or the relation $\{\langle n, m, k\rangle \in \mathbb{N} \mid n+m=k\}$, or the relation R of five-tuples $\langle a, b, c, d, e\rangle$ of letters such that *abcde* is a word in the Dutch language. Thus $\langle r, a, d, i, o\rangle$ belongs to R, and so does $\langle h, a, l, l, o\rangle$, but $\langle h, e, r, f, s\rangle$ does not. There are various ways to define relations of arbitrary arity in terms of sets, e.g.

$$\langle a, b, c\rangle =_{def} \langle a, \langle b, c\rangle\rangle \qquad \langle a, b, c, d\rangle =_{def} \langle a, \langle b, c, d\rangle\rangle,$$

etc. In the same way as above one can then show that

$$\langle a_1, \ldots, a_n\rangle = \langle b_1, \ldots, b_n\rangle \;\Leftrightarrow\; \forall i \leq n(a_i = b_i).$$

We will not return to this choice in what follows, but just assume that we have chosen a convenient way to define relations of arity > 2 (that of arity 2 being fixed already by the definition above) with the expected properties. We call expressions $\langle a_1, \ldots, a_n\rangle$ *n-tuples*. A set consisting of n-tuples we call an *n-ary relation*. As mentioned above, a set of pairs we also call a *binary* relation. $A^n = \{\langle a_1, \ldots, a_n\rangle \mid \forall i \leq n(a_i \in A)\}$.

Example 6

1. $\{\langle n, m, k\rangle \in \mathbb{N} \mid n \cdot m = k\}$ is a 3-ary relation.
2. $\{\langle a_1, \ldots, a_n\rangle \in \mathbb{R}^{n+1} \mid a_1 + a_2 + \ldots a_n = 0\}$ is a $(n+1)$-ary relation.

3.6 Exercises

1. Give a set-notation for the relation of pairs of reals for which the second element is the square of the first.
2. Write down the elements of $\{a, b\} \times \{a, c, d\}$.
3. Which subset of the plane $\mathbb{R}^2$ is the set $\{\langle x, y\rangle \in \mathbb{R}^2 \mid x = y\}$?
4. Is the relation $\{\langle r, s\rangle \in \mathbb{R}^2 \mid (r+s) \in \mathbb{Q}\}$ symmetric? Is it linear?
5. Is the relation $\{\langle n, m\rangle \in \mathbb{Z}^2 \mid n^2 = m\}$ dense?
6. Show that for euclidean relations $\forall x \forall y \forall x(Rxy \wedge Rxz \to Ryz \wedge Rzy)$ holds.
7. Write down in set notation the relation consisting of the 3-tuples $\langle x, y, z\rangle \in \mathbb{Z}^3$ such that $x^2 + y^2 = z^2$. Which arity has this relation? Give two elements of the relation.
8. Prove that the relation that is the cartesian product $A \times B$ of two sets is serial if and only if B is not empty. Prove that it is symmetric if $A = B$.

9. Prove that the relation $\{\langle x, y\rangle \in \mathbb{R}^2 \mid x^2 = y\}$ is not total on $\mathbb{R}$.

10. Given a relation $R \subseteq A^2$, $R_{\upharpoonright B}$ denotes the restriction of R to B: $R_{\upharpoonright B} = \{\langle x, y\rangle \mid \langle x, y\rangle \in R, x \in B, y \in B\}$. A property is called *subset-hereditary* if whenever R has a property, then so does $R_{\upharpoonright B}$ for all subsets B of A. Which of the properties given in Section 3.3 are subset-hereditary, and which are not? In the last case, provide counter examples.

11. Prove that $\langle a, b\rangle = \langle c, d\rangle$ if and only if $a = c$ and $b = d$.

12. Why would $\{a, b\}$ not be a useful definition for an ordered pair $\langle a, b\rangle$? What about the definition $\{\{a\}, \{b\}\}$?

13. Is $\{a\} \in \{\langle a, b\rangle\}$? Is $\{b\} \in \{\langle a, b\rangle\}$?

14. Is $\{\langle 1, 2\rangle\} \subseteq \mathbb{N}$? Is $\{\langle 1, 2\rangle\} \subseteq P(\mathbb{N})$?

15. Show that the relation $\sim$ on $\mathbb{Z} \times \mathbb{N}_{>0}$ given by

$$\langle x, y\rangle \sim \langle a, b\rangle \;\Leftrightarrow\; xb = ya,$$

that was used to construct $\mathbb{Q}$, is an equivalence relation.

16. Is the relation given by the picture euclidean?

$$\begin{tikzcd}
 & 3 & \\
1 \arrow[ur] \arrow[rr] & & 2 \\
 & 0 \arrow[ul] \arrow[ur] &
\end{tikzcd}$$

Which arrows have to be added to make it a transitive relation?

17. Is the following relation dense? Serial? Well-founded?

$$\begin{tikzcd}
a_1 \arrow[rr] \arrow[dr] & & a_2 \arrow[rr] \arrow[dr] & & a_3 \arrow[rr] \arrow[dr] & & a_4 & & \cdots \\
 & b_1 \arrow[ur] & & b_2 \arrow[ur] & & b_3 \arrow[ur] & & \cdots &
\end{tikzcd}$$

And the same questions for this relation:

$$\begin{tikzcd}
a_1 \arrow[rr] \arrow[dr] & & a_2 \arrow[rr] \arrow[dr] & & a_3 \arrow[rr] \arrow[dr] & & a_4 & & \cdots \\
 & b_1 \arrow[ur] \arrow[loop below] & & b_2 \arrow[ur] \arrow[loop below] & & b_3 \arrow[ur] \arrow[loop below] & & \cdots &
\end{tikzcd}$$

18. Which of $\leq_{\mathbb{N}}$, $\leq_{\mathbb{Z}}$, $\leq_{\mathbb{Q}}$, $\leq_{\mathbb{R}}$ is well-founded?

19. Show that the relation $\leftrightarrow$ on the set of propositional formulas is an equivalence relation.

20. Draw a diagram of the relation $\subseteq$ on $P(\{0,1,2\})$.

21. Prove that $(P(A), \subseteq)$ is a partial order for every set A. What about the set $(P(A), \subset)$?

22. How many elements has a set A at least if $(P(A), \subseteq)$ is not a total ordering?

23. Show that given a reflexive relation R, the relation S defined by

$$Sxy \;\Leftrightarrow\; Rxy \vee Ryx$$

is a reflexive symmetric relation.

4 Functions

In the previous section it has been explained how relations can be viewed as sets, namely as sets of ordered pairs. Functions can also be viewed as sets, or relations, but with certain additional properties.

A *function* $f : A \to B$ is a subset $f \subseteq A \times B$ such that for each $x \in A$ there exists exactly one $y \in B$ such that $\langle x, y\rangle \in f$. In formal notation: $f \subseteq A \times B$ is a function if

$$\forall x \in A \exists! y \in B\, (\langle x, y\rangle \in f).$$

($\exists! y$ means "there exists a unique y".) Functions are also called *maps* or *mappings*. When $A = B$ we also say that f is a function *on* A. We often write $f(x) = y$ for $\langle x, y\rangle \in f$.

This view on functions is not a natural one in that f is not viewed as an operation or algorithm that on input x provides an outcome $f(x)$, like e.g. the function $\mathrm{ggd}(x, y)$ that outputs the greatest common divisor of numbers x and y. What we gain by this unnatural view is the insight that functions can defined in terms of sets, and whence everything we know about sets holds for functions as well. The intuitive notion of a function $f : A \to B$ is *intensional*, it is considered to be given by a rule or computation that associates an element in B with every element in A. Thus it might be that $f(x)$ and $g(x)$ are the same for all values x, although they are different in that they are given by a different computations. This intuition we lose in the set-theoretic view, which, on the other hand, has advantages as well; having more than one point of view can be useful. Functions in the set-theoretic setting are *extensional*: when $f(x) = g(x)$ for all x, then $f = g$, as the sets $f = \{\langle x, y\rangle \mid f(x) = y\}$ and $g = \{\langle x, y\rangle \mid g(x) = y\}$ are equal, and there is no reference to the processes underlying f and g which might distinguish them.

Example 7

1. The function $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = 2x$ is equal to the set $\{\langle x, y\rangle \in \mathbb{R}^2 \mid 2x = y\}$.
2. The identity function id_A on a set A is given by the set $\{\langle x, y\rangle \in A^2 \mid x = y\}$. Thus $id_A(x) = x$.

4.1 Domain and range

The *domain* of a function $f : A \to B$ is A. The *range* of the function is the set $\{y \in B \mid \exists x \in A\, f(x) = y\}$. The domain of f is denoted by $\mathrm{dom}(f)$, and its range by $\mathrm{rng}(f)$. If $f(x) = y$, then y is called the *image* of x under f. Given a set $X \subseteq A$, $f[X]$ denotes the set $\{f(x) \mid x \in X\}$ and is called the *image* of X under f. Thus $f[A]$ is the set of elements in B that can be reached from A via f. For $Y \subseteq B$, the set $\{x \in A \mid f(x) \in Y\}$ is denoted by $f^{-1}[Y]$.

The set of *all* functions from A to B is denoted by B^A.

Example 8 1. The domain of the function $f : \mathbb{N} \to \mathbb{Z}$ given by $f(n) = -n$ is $\mathbb{N}$, and the range is $\mathbb{Z}_{\leq 0}$ (all negative integers plus 0). $f[\{n \in \mathbb{N} \mid n < 7\}] = \{n \in \mathbb{Z}_{\leq 0} \mid n > -7\}$.

2. The domain of the function $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = x^2$ is $\mathbb{R}$ and its range is $R_{\geq 0}$ (all positive reals). $f^{-1}[\{4, 9\}] = \{2, -2, 3, -3\}$.

$$f^{-1}[\mathbb{R}_{\geq 25}] = \{x \in \mathbb{R} \mid x \geq 5\} \cup \{x \in \mathbb{R} | x \leq -5\}.$$

3. For the function sgn: $\{0, 1\} \to \{0, 1\}$ with sgn(0)=1 and sgn(1) $= 0$, domain and range are $\{0, 1\}$. $f[0] = \{1\}$ and $f^{-1}[0] = \{1\}$.

4. Let $\mathcal{P}$ be the set of propositional formulas. Then $f(\varphi) = \neg\varphi$ is the function on $\mathcal{P}$ that maps formulas to their negation.

5. $\mathbb{R}^{\mathbb{R}}$ is the set of all the functions on the reals. $\{0, 1\}^{\mathbb{N}}$ is the set of all functions from the natural numbers to $\{0, 1\}$, which can also be viewed as the set of infinite sequences of zeros and ones.

Theorem 4 For finite sets X and Y the number of functions from X to Y is $|Y|^{|X|}$.

Proof You will be asked to prove this in the exercises. ♡

4.2 Composition

Given two functions, one can *compose* them, that is, apply the one after the other. For example, the composition of the function $f(x) = x^2$ with the function $g(x) = x - 5$ is the function $h(x) = g(f(x)) = x^2 - 5$, while the composition of g with f is $f(g(x)) = (x - 5)^2$.

More formally, given two functions $f : A \to B$ and $g : B \to C$, the *composition* of f and g is denoted by $f \circ g$ and is the function defined by

$$(g \circ f)(x) = g\big(f(x)\big).$$

Of course, the notion $g \circ f$ onlay makes sense when the range of f is part of the domain of g: rng(f)⊆dom(g). E.g. for $f : \mathbb{N} \to \mathbb{Z}$ with $f(n) = -n$ and $g : \mathbb{N} \to \mathbb{N}$ with $g(n) = 2n$ the composition $g \circ f$ is not well-defined, since e.g. $f(2) = -2$, but $g(-2)$ is not defined. On the other hand, the composition $f \circ g$ is defined, since indeed rng(g)⊆dom(f). Note that this also shows that $f \circ g$ is in general different from $g \circ f$.

We can repeat this process and, given functions $f_1, \dots f_n$ where $f_i : A_i \to B_i$ and $B_i \subseteq A_{i+1}$, we can define $f_n \circ \dots \circ f_1$ as

$$f_n \circ \dots \circ f_1(x) = f_n(f_{n-1}(\dots(f_2(f_1(x))\dots).$$

Example 9 1. For $f, g : \mathbb{R}_{\geq 0} \to \mathbb{R}$ with $f(x) = x + 2$ and $g(x) = \sqrt{x}$, the composition $g \circ f$ maps x to $\sqrt{(x + 2)}$, and $f \circ g$ maps x to $\sqrt{x} + 2$.

2. Let $\mathcal{P}$ be the set of propositional formulas, and $f, g \in \mathcal{P}^{\mathcal{P}}$ defined by $f(\varphi) = \neg\varphi$ and $g(\varphi) = \varphi \vee p$. Then $(g \circ f)(\varphi) = \neg\varphi \vee p$ and $(f \circ g)(\varphi) = \neg(\varphi \vee p)$.

3. Given $f, g, h : \mathbb{N} \to \mathbb{N}$ with $f(n) = (n + 2)$, $g(n) = 2n$ and $h(n) = n^2$, then $h \circ g \circ f = (2(n + 2))^2$.

4. Given $f, g, h : \mathbb{R}_{\geq 0} \to \mathbb{R}$ with $f(x) = x^2$, $g(x) = \sqrt{x}$ and $h(x) = x^2$, then $h \circ g \circ f = (\sqrt{x^2})^2$, and thus $h \circ g \circ f = f$.

The following theorem is simple, but its proof is a nice example of a formal and precise proof.

Theorem 5 If f, g, h are functions such that $\mathrm{rng}(f) \subseteq \mathrm{dom}(g)$ and $\mathrm{rng}(g) \subseteq \mathrm{dom}(h)$, then

$$h \circ (g \circ f) = (h \circ g) \circ f.$$

This property says that composition is *associative*.

Proof Let $f : A \to B$, $g : B \to C$ and $h : C \to D$. We have to show that for all $x \in A$ we have $(h \circ (g \circ f))(x) = ((h \circ g) \circ f)(x)$. We prove this by applying the definitions of composition:

$$\begin{array}{rcl} (h \circ (g \circ f))(x) & = & h\big((g \circ f)(x)\big) \\ & = & h\big(g\big(f(x)\big)\big) \\ & = & (h \circ g)\big(f(x)\big) \\ & = & \big((h \circ g) \circ f\big)(x) \end{array}$$

♡

4.3 Injections, surjections and bijections

There are function that do not map two different elements to the same element. For example, the function $f : \mathbb{N} \to \mathbb{N}$ with $f(n) = n + 1$. Such functions are called *injections*. A function $f : A \to B$ is *injective* if

$$\forall x, y \in A\ (x \neq y \to f(x) \neq f(y)).$$

Note that this is equivalent to

$$\forall x \forall y \in A (f(x) = f(y) \to x = y).$$

Example 10 1. The identity function is injective.

2. $f : \mathbb{R} \to \mathbb{R}$ such that $f(x) = x^2$ is not injective: $f(-2) = 4 = f(2)$. If we consider the same function, but now as a function on $R_{\geq 0}$ then it is injective.

You will be asked to prove the following observation in the exercises.

Theorem 6 The composition of two injective functions $f : A \to B$ and $g : B \to C$ is injective.

There are functions $f : A \to B$ that do not reach all elements in B, that is, the range of f is a real subset of B. The function $f : \mathbb{N} \to \mathbb{N}$ that maps all numbers to 0, $f(n) = 0$ for all n, is an example of this since rng(f)=$\{0\} \subset \mathbb{N}$. Functions that do reach *all* of B are called surjective. A function $f : A \to B$ is *surjective* if $f[A] = B$, in other words if

$$\forall y \in B \exists x \in A \; f(x) = y.$$

Example 11

1. The identity function is surjective.
2. $f : \mathbb{Z} \to \mathbb{Q}$ with $f(n) = 1/n$ is not surjective, as $2 \notin f[\mathbb{Z}]$. It is injective.
3. $f : \{\{a, b\}, \{c\}, \{d\}\} \to \{0, 1, 2\}$ given by $f(\{a, b\}) = 0$ and $f(\{c\}) = f(\{d\}) = 2$, is not injective since $\{c\}$ and $\{d\}$ are mapped to the same element. Neither is it surjective, as there is no x such that $f(x) = 1$.

Observe that the surjectivity of a function depends on the way the function is presented to us. For example, the function $f : \mathbb{N} \to \{0\}$ given by $f(n) = 0$ is surjective, but the same function, $f(n) = 0$, considered as a function $f : \mathbb{N} \to \mathbb{N}$ is not.

A function is *bijective* if it is both injective and surjective. Sometimes, bijections are called *1-1 functions*.

Example 12

1. The function $f(x) = x - 1$ on the reals is bijective.
2. The function $f : \mathbb{N} \to \mathbb{N}$ given by $f(n) = n + 7$ is not bijective, as it is not surjective.

Intuitively, a bijection between sets A and B associates with every element in A a unique element in B and vice versa. Thus it can be seen as a correspondence between the sets A and B. Because of this, bijections have a natural inverse, which is the function "turned around". That is, if $f : A \to B$ is a bijection, then we can define the function $g : B \to A$ such that for all $x \in B$, $g(y) = x$ if $f(x) = y$. Note that then

$$(g \circ f)(x) = g\big(f(x)\big) = x.$$

E.g. for the bijection $f(x) = x + 2$ on the reals, g would be $g(y) = y - 2$. And indeed, $g\big(f(x)\big) = g(x+2) = (x+2)-2 = x$. This is the content of the following theorem.

Theorem 7 A function $f : A \to B$ is bijective if and only if there exists a function $g : B \to A$ such that $(f \circ g) = id_B$ and $(g \circ f) = id_A$. g is called the *inverse* of f and denoted by f^{-1}.

Proof An if and only if statement has to directions: from left to right and from right to left, which we denote by $\Rightarrow$ and $\Leftarrow$.

$\Rightarrow$: in the direction from left to right we have to show that if f is bijective, then such a function g as in the theorem exists. Thus suppose that f is bijective. A explained above, sets are considered to be set of pairs, $f \subseteq A \times B$. But then we define g according to the intuition of "turning f around":

$$g = \{\langle y, x\rangle \mid \langle x, y\rangle \in f\} = \{\langle y, x\rangle \mid f(x) = y\}.$$

We have to show that g is a function from B to A and that $(f \circ g) = id_B$ and $(g \circ f) = id_A$. You will be asked to prove this in the exercises below.

$\Leftarrow$: in the direction from right to left we have to show that if there is a $g : B \to A$ such that $(f \circ g) = id_B$ and $(g \circ f) = id_A$, then f is a bijection. Thus we have to show that f is injective and surjective.

First, we show that f is injective by showing that if $f(x) = f(y)$, then $x = y$. So suppose $f(x) = f(y)$ for two elements x and y. Since $(g \circ f) = id_A$ it follows that $g(f(x)) = (g \circ f)(x) = id_A(x) = x$. Similarly, $g(f(y)) = (g \circ f)(y) = id_A(y) = y$. But since $f(x) = f(y)$, also $g(f(x)) = g(f(y))$, and thus $x = y$.

Second, we show that f is surjective. Consider an $y \in B$. We have to find an $x \in A$ such that $f(x) = y$. Now take $x = g(y)$. Indeed, $x \in A$. Also, since $(f \circ g) = id_B$ it follows that $f(x) = f(g(y)) = y$, and we are done.

Note that in $\Rightarrow$ we used that $(g \circ f) = id_A$, and in $\Leftarrow$ we used $(f \circ g) = id_B$. ♡

Example 13

1. $id_A^{-1} = id_A$.
2. For the function $f : \mathbb{N} \to \{n \in \mathbb{N} \mid \exists m \in \mathbb{N}\, (2m = n)\}$ given by $f(x) = 2x$, $f^{-1} : \{n \in \mathbb{N} \mid \exists m \in \mathbb{N}\, (2m = n)\} \to \mathbb{N}$ is given by $f^{-1}(n) = n/2$.
3. The inverse of the function $\sqrt{x}$ on the positive reals $\mathbb{R}_{\geq 0}$ is the function x^2.
4. All bijections on $\{0, 1\}$, i.e. all bijective functions $f : \{0, 1\} \to \{0, 1\}$, are $\{\langle 0, 0\rangle, \langle 1, 1\rangle\}$, $\{\langle 0, 1\rangle, \langle 1, 0\rangle\}$. Note that there are in this case no injections except the bijections.
5. The unique fucntion from $\{a\}$ to $\{b\}$ is a bijection.

4.4 Fixed points

The identity function maps every element to itself. There are functions that only map some elements to themselves, like the real-valued function $f(x) = x^2$ that is the identity on 0 and 1 but not so on any of the other elements in $\mathbb{R}$. Clearly, there are functions that map no element to itself, for example the function $f(n) = n + 1$.

Given a function $f : A \to B$, an element $x \in A$ is called a *fixed point of* f if $f(x) = x$. Thus 0 and 1 are fixed points of the function $f(x)$ given by $f(x) = x^2$.

The famous Dutch mathematician L.E.J. Brouwer (1881 - 1966) has proved the *fixed point theorem*: every continuous function on the unit ball has a fixed point.

4.5 Isomorphisms

The existence of a bijection between two sets indicates a certain similarity between them. For example, for finite sets the existence of a bijection implies that they have the same number of elements. When the sets are endowed with certain structure (like relations) the notion of bijection can be extended to the notion of isomorphism, such that the existence of the latter guarantees that also on the structural level the two sets are similar. The definition runs as follows. Given two orders $R \subseteq A \times A$ and $S \subseteq B \times B$, a function $f : A \to B$ is an *isomorphism* if it is a bijection and

$$\forall x \in A \forall y \in A : \ xRy \ \Leftrightarrow \ f(x)Sf(y).$$

In this case (A, R) and (B, S) are called *isomorphic*.

Example 14

1. $(\mathbb{N}, \leq)$ is isomorphic to $(\{n \in \mathbb{Z} \mid n \leq 0\}, \geq)$.
2. The sets $(\{1, 2, \ldots, 5\}, <)$ and $(\{a, b, e, d, c\}, R)$, where xRy holds if x comes before y in the Dutch alphabet, are isomorphic.

4.6 Notation

The definition of a function can be given in many ways. In words, in set-notation, or by a formula, like this:

f is the function on the integers that multiplies a number by 7

$$f = \{\langle n, m\rangle \in \mathbb{Z}^2 \mid m = 7n\}$$

$$f : \mathbb{Z} \to \mathbb{Z} \text{ given by } f(n) = 7n.$$

Sometimes more complex notation is needed: $F : \mathbb{R} \to \mathbb{R}$ and

$$f(x) = \begin{cases} \sqrt{x} & \text{if } x \geq 0 \\ 1 & \text{if } x < 0 \end{cases}$$

describes the function that maps positive reals to their square root and negative reals to 1. We call such a definition a *definition by case distinction* or a *definition by cases*. Such definitions are often used in programming languages.

4.7 Exercises

1. Give a set-notation for the function that maps real numbers m to their inverse, except when $m = 0$, in which case it is mappped to 0. What are the domain and range of this function?
2. What is the domain and what is the range of the function $f(n) = 7n$ on the natural numbers?

3. Given the function $f(x) = \sqrt{x}$ on the positive reals, write down its set-notation. What is $f[\mathbb{R}_{\geq 4}]$? And what is $f^{-1}[\mathbb{R}_{\leq 4}]$?

4. List the elements of the set $\{0, 1, 2\}^{\{0\}}$.

5. Show that the number of functions from $\{0, 1\}$ to $\{0, 1\}$, i.e. the size of $\{0, 1\}^{\{0,1\}}$, is 2^2.

6. Given $f, g : \mathbb{R}_{\geq 0} \to \mathbb{R}$ with $f(x) = \sqrt{x}$, $g(x) = x^3$, which function is $f \circ g$? And which $g \circ f$?

7. Let $\mathcal{P}$ be the set of propositional formulas, and consider the function $f(\varphi) = \varphi \to p$ and $g(\varphi) = p \to \varphi$. Describe $f \circ g$ and $g \circ f$. Are there φ for which $(f \circ g)(\varphi) \leftrightarrow (g \circ f)(\varphi)$?

8. Prove for the f and g in the proof of Theorem 7 that g is a function from B to A, and that $(f \circ g) = id_B$ and $(g \circ f) = id_A$.

9. Prove Theorem 4.

10. Is the function $f : \mathbb{Z} \to \mathbb{Z}$ with $f(n) = n + 1$ surjective? Is it surjective when considered as a function on the natural numbers? Explain your answer.

11. Is the exponentation function $f : \mathbb{R} \to \mathbb{R}$ given by $f(x) = 2^x$ injective? And surjective? Describe the set $f[\{x \in \mathbb{R} \mid -2 \leq x \leq 2\}]$ and the set $f^{-1}[\{x \in \mathbb{R} \mid 4 \leq x \leq 16\}]$.

12. Prove that the composition of two injective functions is injective.

13. Are the sinus and cosinus functions on the real numbers injective? And surjective?

14. Prove that all functions from a nonempty set to a singleton (a set with one element) are surjective, i.e. all $f : A \to \{a\}$, with $A \neq \emptyset$, are surjective. In which cases are they also injective?

15. Given finite sets A and B, give a condition under which there are no injections from A to B.

16. Show that for any injective function $f : A \to B$, the function f as considered from A to $f[A]$ is a bijection.

17. Let $\mathcal{P}$ be the set of propositional formulas, and consider the function $f(\varphi) = \neg\varphi$. Does f have a fixed point? Are there ψ such that $f(\psi) \leftrightarrow \psi$? If $f(\psi) \leftrightarrow \psi$, does this imply that ψ is a fixed point of f?

18. Show that if $f : A \to A$ has a fixed point x, then also $f^n(x)$ (f composed with itself n times) is a fixed point of f and equal to x.

19. Give a definition by cases of the function $f : \mathbb{R} \to \mathbb{R}$ that maps all reals between 0 and 1 to 0, that maps 0 and 1 to 1, and that maps all other rationals to -1.

20. Given two finite sets A and B, how many injections are there from A to B?

21. Show that for a function f, $\{\langle x, y\rangle \mid f(x) = f(y)\}$ is an equivalence relation.

22. Show that for a function $f : A \to B$, for $R = \{\langle x, y\rangle \mid f(x) = f(y)\}$, there is an injection from A/R to B.

23. Show that for finite A there is no surjection from A to $P(A)$.

24. Is $(\mathbb{N}, \leq)$ isomorphic $(\mathbb{Z}_{\leq 0}, \leq)$?

25. Is $(\mathbb{N}, \leq)$ isomorphic to $(\mathbb{Z}, \leq)$?

5 Counting the infinite

It is easy to count the elements of a finite set. For infinite sets we just say they have infinitely many elements. But there is much more to that: in this section we are going to show that some infinite sets are much more infinite than others. First we reconsider the notion of a finite set, and define it in a way that can easily be extended to the infinite case.

A set A is called *finite* if for some natural number n there is a bijection

$$f : \{1, 2, \ldots, n\} \to A.$$

We call n the number of elements of A. Observe that this definition captures the intuitive idea of finiteness perfectly.

For sets A and B we write $|A| \leq |B|$ if there is an injection from A to B. We write $|A| = |B|$ if there is a bijection between A and B. We write $|A| < |B|$ if there is an injection from A to B but no bijection.

Note that for a finite set A, the definition of $|A|$ can be taken to be the number of elements of A, because the number of elements in A is $\leq$ the number of elements in B if and only if there is an injection from A to B, i.e. $|A| \leq |B|$.

5.1 Countable sets

We call a set A *countable* if there is a surjection from $\mathbb{N}$ to A. We call a set *uncountable* when it is not countable. From this definition it is clear that:

Theorem 8 Every finite set is countable. $\mathbb{N}$ is countable.

Proof If A is finite, there is, by definition, a bijection $f : \{1, 2, \ldots, n\} \to A$, for some n. But then there clearly is a surjection from $\mathbb{N}$ to A. For example, the function $g : \mathbb{N} \to A$ defined as follows:

$$g(i) = \begin{cases} f(i) & \text{if } 1 \leq i \leq n \\ f(1) & i = 0 \text{ or } i > n \end{cases}$$

This g is a surjection, as f is a bijection: for all $a \in A$, there is a i such that $1 \leq i \leq n$ and $f(i) = a$. But then $g(i) = f(i) = a$. This shows that for every $a \in A$ there exists a $i \in \mathbb{N}$ such that $g(i) = a$, and that is precisely the definition of a surjective function.

That $\mathbb{N}$ is countable is clear: the identity function is a surjection from $\mathbb{N}$ to $\mathbb{N}$. $\heartsuit$

Less trivial are the following observations.

Theorem 9 $\mathbb{Z}$ is countable. Every subset of $\mathbb{N}$ is countable.

Proof That every subset A of $\mathbb{N}$ is countable is easy to see. We let the surjection $f : \mathbb{N} \to A$ be the identity on elements is A, and let it map all other elements of A to one particular element of A, say a:

$$f(i) = \begin{cases} i & \text{if } i \in A \\ a & i \notin A \end{cases}$$

Check for yourself that f indeed is a surjection.

To see that $\mathbb{Z}$ is countable we cannot use the previous argument as $\mathbb{Z}$ is not a subset of $\mathbb{N}$. In this case we construct the surjection $f : \mathbb{N} \to \mathbb{Z}$ as follows

$$f(i) = \begin{cases} 0 & \text{if } i = 0 \\ n & \text{if } i = 2n \text{ and } n > 0 \\ -n & \text{if } i = 2n-1 \text{ and } n > 0 \end{cases}$$

Thus $f(0) = 0$, $f(2) = 1$, $f(4) = 2$, $f(6) = 3$, ..., and $f(1) = -1$, $f(3) = -2$, $f(5) = -3$, ... ♡

Given an infinite countable set A with a surjection f from $\mathbb{N}$ to A, there is a natural way to enumerate the infinitely many elements of A, namely as $f(0), f(1), f(2), \ldots$. For example for $\mathbb{Z}$, the surjection given above results in the enumeration $0, -1, 1, -2, 2, -3, 3, \ldots$. Because of the surjectivity of f every element of A occurs in this list. However, it is not excluded that an element of A appears twice in it. For any countable set we can construct a list in which no element occurs twice. Although this is intuitively clear (just skip the duplicates), the proof of this fact is elegant and not completely trivial. It is a corollary of the following two theorems.

Theorem 10 If A is an infinite set, there is an injection from $\mathbb{N}$ to A. For every infinite set $A \subseteq \mathbb{N}$ there is a bijection between $\mathbb{N}$ and A.

Proof Suppose A is infinite. We construct the injection $f : \mathbb{N} \to A$ in stages. Pick an $a_0 \in A$, and put $f(0) = a_0$. Then pick an $a_1 \in A\backslash\{f(0)\}$, and put $f(1) = a_1$, etc. Thus at the n-th stage we pick an $a_n \in A\backslash\{f(0), \ldots, f(n-1)\}$, and put $f(n) = a_n$. The process never stops because A is infinite. It is easy to see that f is an injection.

Suppose $A \subseteq \mathbb{N}$ is an infinite set. We construct a bijection $g : \mathbb{N} \to A$ as follows. Given a set $X \subseteq \mathbb{N}$ define $\min(X)$ as the smallest element in X. We define g as follows: $g(0) = \min(A)$, and for $n > 0$

$$g(n) = \min(A\backslash\{g(0), g(1), \ldots, g(n-1)\}).$$

It is easy to see that g is an injection. That it is a surjection, and thus a bijection, can be seen as follows. Given $n \in A$, there are only $(n-1)$ elements smaller than n. Even if they are all in A, $g(n)$ will be equal to n, if they are not all in A, there will be an $m < n$ such that $g(m) = n$. ♡

Theorem 11 For every infinite countable set A there exists a bijection between $\mathbb{N}$ and A.

Proof For $A \subseteq \mathbb{N}$, the statement is proved via the previous theorem. Therefore, consider an arbitrairy infinite countable set, and its surjection $f : \mathbb{N} \to A$. Consider the set

$$B = \{n \in \mathbb{N} \mid f(n) \notin \{f(0), \dots, f(n-1)\}\ \}.$$

First we prove that $f : B \to A$, the restriction of f to B, is a bijection. Intuitively, f on B skips the duplicates of elements appearing earlier in the list. That $f : B \to A$ is injective can be seen as follows. If $n \neq m$, then $n < m$ or $m < n$. Suppose that for $n, m \in B$ the first holds, the latter case is similar. Since $m \in B$, $f(m) \notin \{f(0), \dots, f(m-1)\}$, but $f(n) \in \{f(0), \dots, f(m-1)\}$, as $n < m$. Therefore, $f(n) \neq f(m)$. Next we show that f is surjective by induction. We know that $f : \mathbb{N} \to A$ is surjective, i.e. that for all $a \in A$ there exists a $n \in \mathbb{N}$ such that $f(n) = a$. Thus we have shown that $f : B \to A$ is surjective if we have shown that for all $n \in \mathbb{N}$, $f(n) \in f[B]$, i.e. there exists a $m \in B$ such that $f(m) = f(n)$. We prove this by induction on $\mathbb{N}$. Proofs by induction will be treated in the last section, so the reader not familiar with this concept could postpone the following argument till later.

For $n = 0$, $0 \in B$, thus $f(0) \in f[B]$. Assume $f(0), \dots, f(n) \in B$. Either $f(n) \in \{f(0), \dots, f(n-1)\}$, and then clearly $f(n) \in B$, or $f(n) \notin \{f(0), \dots, f(n-1)\}$, and then $n \in B$, thus $f(n) \in f[B]$. Thus we have proved that $f : B \to A$ is a bijection. Thus B is infinite. Since also $B \subseteq \mathbb{N}$, it follows by the previous theorem that there is a bijection $g : \mathbb{N} \to B$. Then the composition $f \circ g$ is a bijection from $\mathbb{N}$ to A, and we are done. ♡

Finally we reach the conclusion that we mentioned above: if A is an infinite countable set, there is an enumeration $a_1, a_2, \dots$ of A in which no element occurs twice. Namely, given the bijection f from $\mathbb{N}$ to A, we take for a_n the element $f(n)$. We call the $a_1, a_2, \dots$ an *enumeration* of A. Conversely, given an enumeration $a_1, a_2, \dots$ in which no element occurs twice, a bijection between A and $\mathbb{N}$ is given by $f(n) = a_n$. We will use these two notions, enumeration and bijection with $\mathbb{N}$, interchangeably.

Theorem 12 If $|A| \leq |B|$ and B is countable, then A is countable. If $|A| \leq |B|$ and A is uncountable, then B is uncountable.

Proof You will be asked to prove this in the exercises. ♡

Theorem 13 If A and B are countable, then so is $A \times B$.

Proof Let $a_1, a_2, \dots$ be an enumeration of A, and $b_1, b_2, \dots$ an enumeration of B. The following is an enumeration of $A \times B$:

$$\langle a_1, b_1 \rangle, \langle a_1, b_2 \rangle, \langle a_2, b_1 \rangle, \langle a_1, b_2 \rangle, \langle a_1, b_3 \rangle, \langle a_2, b_2 \rangle, \dots$$

Thus, first all pairs for which the sum of the indices is 2 are listed, then the pairs which sum of the indices is 3, etc. If we let $f(n)$ be the n-th element in the enumeration we have constructed the desired bijection. ♡

In the exercises you will be asked to show that $|\mathbb{Q}| \leq |\mathbb{Z} \times \mathbb{Z}|$. Thus it follows from the previous two theorems that

Corollary 2 $\mathbb{Q}$ is countable.

5.2 The Cantor-Schroder-Berstein theorem

The following theorem is extremely useful in showing the existence of bijections between sets.

Theorem 14 (Cantor-Schroder-Bernstein theorem) If there is an injection from A to B and an injection from B to A, then there is a bijection between A and B. That is,

$$|A| \leq |B| \wedge |B| \leq |A| \;\Rightarrow\; |A| = |B|.$$

Proof Let $f : A \to B$ and $g : A \to B$ be the injections. We construct the bijection $h : A \to B$ in stages.
If A and B are finite, the statement follows directly, as $|A| \leq |B|$ implies that the number of elements in A is $\leq$ the number of elements in B, and $|B| \leq |A|$ vice versa, thus the number of elements in A and B are equal, and whence $|A| = |B|$.
Therefore, suppose A and B are infinite. We define

$$g^{-1} : \{a \in A \mid \exists b \in B(g(b) = a)\} \to B.$$

as the function that maps $a \in \{x \in A \mid \exists b \in B(g(b) = x)\}$ to a $b \in B$ such that $g(b) = a$. We inductively define sets $C_1, C_2, \ldots$ as follows:

$$C_1 = A \backslash g[B] \qquad C_{n+1} = g(f(C_n)) \qquad C = \bigcup_i C_i.$$

We define

$$h(a) = \begin{cases} f(a) & \text{if } a \in C \\ g^{-1}(a) & \text{if } a \notin C \end{cases}$$

This h is the desired bijection. ♡

5.3 The real numbers

The set of real numbers $\mathbb{R}$ naturally corresponds to the set $\mathbb{Z} \times I$, where

$$I = \{f \in \{0, 1, \ldots 9\}^{\mathbb{N}} \mid \; f(i) \neq 9 \text{ for infinitely many } f\}.$$

Recall that $\{0, 1, \ldots 9\}^{\mathbb{N}}$ is the set of functions from $\mathbb{N}$ to $\{0, 1, \ldots 9\}$. We can view these as infinite sequences $f(0), f(1), \ldots$. Then the view on $\mathbb{R}$ will be clear: a real number is an integer followed by a infinite sequence of decimals. The extra condition on I that $f(i)$ must be distinct from 9 for infinitely many i

stems from the fact that e.g. $0,999\cdots = 1,000\ldots$, and we do not want to have two different representations of a single number in the set.

Here follows the famous theorem of Cantor that implies that there are "different" infinities. Recall that we call a set uncountable when it is not countable.

Theorem 15 (Cantor) $\mathbb{R}$ is uncountable.

Proof The proof is by contradiction. Assume that $\mathbb{R}$ is countable and let $f : \mathbb{N} \to \mathbb{R}$ be a surjection. We construct a real number for which there is no $n \in \mathbb{N}$ such that $f(n) = r$, and then we have arrived at a contradiction. We define r as $r = 0, r_0 r_1 r_2 \ldots$, where

$$r_n = \begin{cases} 0 & \text{if the } n\text{-th digit from } f(n) \text{ is not } 0 \\ 1 & \text{otherwise} \end{cases}$$

Now this number r differs from any number in the list, as it differs in the n-th digit with the real number $f(n)$. Thus r does not appear in $f[\mathbb{N}]$, and whence f is not surjective, contradicting the hypothesis. ♡

The argument above is called a *diagonalization argument*, as it uses a diagonal: if we list the $f(0), f(1), \ldots$ below one another, the choice of r is based on the values on the diagonal.

Here follow some examples of sets A for which $|A| = |\mathbb{R}|$, and which are thus other examples of uncountable sets. Recall that for $x, y \in \mathbb{R}$, (x, y) denotes the interval $\{r \in \mathbb{R} \mid x < r < y\}$, and $\mathbb{R}_{>x}$ denotes the set $\{r \in \mathbb{R} \mid x < r\}$.

Theorem 16 For every $x \in \mathbb{R}$, $|\mathbb{R}| = |\mathbb{R}_{>x}|$.

Proof Pick an $x \in \mathbb{R}$. That $|\mathbb{R}_{>x}| \leq |\mathbb{R}|$ is easy to see. We show that $|\mathbb{R}| \leq |\mathbb{R}_{>x}|$. The Cantor-Schroder-Bernstein theorem then implies that $|\mathbb{R}| = |\mathbb{R}_{>x}|$. Consider the function $f : \mathbb{R} \to \mathbb{R}_{>x}$, defined as $f(r) = 2^r + x$. It is not difficult to see that this is an injection ($r \neq s \Rightarrow f(r) \neq f(s)$) from $\mathbb{R}$ into $\mathbb{R}_{>x}$. And this proves $|\mathbb{R}| \leq |\mathbb{R}_{>x}|$. ♡

Theorem 17 For every $x, y \in \mathbb{R}$ with $x \neq y$, $|\mathbb{R}| = |(x, y)|$.

Proof We first prove that $|\mathbb{R}_{>1}| = |(0, 1)|$. That $|(0, 1)| \leq |\mathbb{R}_{>1}|$ is clear. Thus if we show that $|\mathbb{R}_{>1}| \leq |(0, 1)|$, the Cantor-Schroder-Bernstein theorem and the previous theorem imply that $|\mathbb{R}| = |(0, 1)|$. Consider $f : \mathbb{R}_{>1} \to (0, 1)$ defined as $f(x) = 1/x$. This clearly is an injection from $\mathbb{R}_{>1}$ to $(0, 1)$, and thus proves $|\mathbb{R}_{>1}| \leq |(0, 1)|$.

It is easy to see that $|(0, 1)| = |(x, y)|$ for any distinct real numbers x and y: the function $g : (0, 1) \to (x, y)$ defined as $g(r) = x + (y - x) \cdot r$ is the desired bijection. ♡

Theorem 18 $|\mathbb{R} \times \mathbb{R}| = |\mathbb{R}|$.

Proof That $|\mathbb{R}| \leq |\mathbb{R} \times \mathbb{R}|$ is clear. Thus by the Cantor-Schroder-Bernstein theorem we only have to show that $|\mathbb{R} \times \mathbb{R}| \leq |\mathbb{R}|$. Recall the definition of $\mathbb{R}$ as $\mathbb{Z} \times I$. We define a function $f : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$, where for two reals $r = r_1, r_2r_3\ldots$ and $s = s_1, s_2s_3\ldots$, $f(\langle r, s\rangle)$ is the real number (in decimal notation, like an element of $\mathbb{Z} \times I$) $t_1, t_2t_3t_4\ldots$, where $t_{2n} = r_n$ and $t_{2n+1} = s_n$. For example, for $r = 0,222\ldots$ and $1,333\ldots$, $f(\langle r, s\rangle) = 0,1232323\ldots$. Thus f "merges" numbers. It is not difficult to see that f is an injective function. ♡

5.4 Infinitely many infinities

We have have seen that

$$|\mathbb{N}| < |\mathbb{R}|.$$

A question that immediately comes to mind: are there more infinities, or are these the only two? The following theorem shows that there are more infinities, infinitely many more.

Theorem 19 (Cantor) For every set A, $|A| < |P(A)|$.

Proof Note that for finite sets the statement is easily seen to be true. Suppose A is infinite. That there is an injection from A to $P(A)$ is not difficult to see: take the function $f(a) = \{a\}$. To see that there is no surjection from A to $P(A)$, we have to show that for every $g : A \to P(A)$ there exists a $X \in P(A)$ such that $X \notin g[A]$. Consider the set

$$X = \{b \in A \mid b \notin g(b)\}.$$

Note that this definition makes sense, as $g(b) \in P(A)$, and thus $g(b) \subseteq A$. Since $X \subseteq A$ we have $X \in P(A)$. We show that there is no $a \in A$ such that $g(a) = X$. Suppose there is such an element a. If $a \in X$, then $a \notin g(a)$. But $g(a) = X$, thus $a \in X$ and $a \notin X$, which cannot be. But if $a \notin X$, then $a \in g(a)$. As $g(a) = X$, again $a \in X$ and $a \notin X$. Thus such a an element a cannot exist. ♡

From this theorem we obtain our infinitely many infinities:

$$|A| < |P(A)| < |P(P(A))| < |P(P(P(A)))| < \ldots$$

The question whether there are infinities strictly between $\mathbb{N}$ and $\mathbb{R}$ is an open problem in an essential way: it can be shown that it is not solvable by the mathematical methods we use today.

5.5 Exercises

1. Show that $\mathbb{Z} \times \mathbb{Z}$ is countable by providing a bijection between $\mathbb{Z} \times \mathbb{Z}$ and $\mathbb{N}$.

2. Give an injection from $\mathbb{Q}$ to $\mathbb{Z} \times \mathbb{Z}$. Use the definition of $\mathbb{Q}$ given in Section 3.4.1.

3. Show that $\mathbb{Q} \times \mathbb{Q}$ is countable by constructing a surjection from $\mathbb{N}$ to it. Use the definition of $\mathbb{Q}$ given in Section 3.4.1.
4. Show that $\mathbb{Z}^n = \{\langle x_1, \ldots, x_n \rangle \mid \forall i \leq n\, (x_i \in \mathbb{Z})\}$ is countable.
5. Show that $\mathbb{Z} \cup \{\langle 0, n \rangle \mid n \in \mathbb{Z}\}$ is countable.
6. Show that $\mathbb{Q} \cup \{\langle 0, q \rangle \mid q \in \mathbb{Q}\}$ is countable.
7. Given an equivalence relation R on a set A, show that $|A/R| \leq |A|$.
8. Give an example of a finite set A and equivalence relations R and S such that $|A| = |A/R|$ and $|A/S| < |A|$. The same but then for an infinite A.
9. Prove that $\mathbb{R}_{\geq 0}$ is uncountable.
10. Prove that every subset of a countable set is countable.
11. Prove that the cartesian product of a countable and an uncountable set is uncountable.
12. Prove Theorem 12.
13. Prove that the set of finite words of 0's and 1's is countable.
14. Prove that the set of propositional formulas in the propositional variables $p_1, p_2, \ldots$ is countable.
15. Pick your favorite programming language and prove that the set of programs in this language is countable.

6 Induction

In the previous sections we considered infinite sets and their relations to each other in terms of functions, in particular bijections. In this section we consider one specific way of defining certain infinite sets, the *inductive definition*, and a certain method of proof appliciable to such sets, the *proof by induction*. We start with inductive definitions.

6.1 Inductive definitions

The sets to which induction arguments apply are in general sets that can be defined in an *inductive way*. An *inductive definition* is a definition in which the elements are defined/build up from below. We do not give a formal definition but treat some examples.

Example 15 Formulas can be defined inductively:

1. propositional variables are formulas,
2. if φ and ψ are formulas, then so are $\neg\varphi$, $(\varphi \wedge \psi)$, $(\varphi \vee \psi)$ and $(\varphi \to \psi)$,
3. only expressions obtained by application of 1. and 2. are formulas.

Observe that we include the brackets in this definition, as they are formally there. The fact that we write $\varphi \wedge \psi \to \phi$ for $((\varphi \wedge \psi) \to \phi)$ is just a convention. Note that the last requirement is a closure requirement. It is often left out. When one defines: mamals are those animals that breast-feed their children, then one implicitly means that no other "things" are mamals.

Example 16 Given addition, the natural numbers could be defined inductively:

1. 0 is a natural number,
2. if n is a natural number, then so is $(n + 1)$.

Example 17 Here we inductively define the notion of sequences of 0's and 1's that are palindromes (reading the word from back to front gives the same word):

1. 0 and 00 are palindromes,
2. 1 and 11 are palindromes,
3. if n is palindrome, then so are $0n0$ and $1n1$.

Also, the syntax of most programming languages are defined in a inductive way.

6.2 Proofs by induction

Every inductively defined set comes with a certain method called a *proof by induction*, that can be used to show that all the elements of the set share a certain property.

When we have to show for a finite number of elements that they all have a certain property, we can show this by treating every element seperately. For example, the proof that 2, 5 and 11 are prime just consists of the proofs that 2 is prime, that 5 is prime, and that 11 is prime. When we have to show for infinitely many elements that they have a certain property, we have to use other means to convince ourselves of the thruth of the statement, as we can not treat the elements one by one. For inductively defined sets there is a certain proof method, proofs by *induction*, that can be a useful tool in these settings. The method of proofs mirrors exactly the inductive definition of the set in question.

6.2.1 Natural numbers

Let us start by recalling one of the most famous instances of a proof by induction, by showing that for all natural numbers n, it holds that $\Sigma_{k=0}^{n} k = n(n+1)/2$. For this, it suffices to show that

1. the statement holds for $n = 0$,
2. if the statement holds for n (the *induction hypothesis*), it holds for $(n+1)$ too. In other words, assuming that the statement holds for n, it can be shown to hold for $(n+1)$ too.

Thus if we write $\varphi(n)$ for $\Sigma_{k=0}^{n} k = n(n+1)/2$, then we have to show that

1. $\varphi(0)$,
2. $\varphi(n)$ implies $\varphi(n+1)$. ($\varphi(n)$ is called the *induction hypothesis*.)

Thus, in this particular case we have to show that

1. $\Sigma_{k=0}^{0} k = 0(0+1)/2$,
2. if $\Sigma_{k=0}^{n} k = n(n+1)/2$, then it follows that $\Sigma_{k=0}^{n+1} k = (n+1)(n+2)/2$.

1. amounts to 0=0, and is therefore clearly true. The argument for 2. runs as follows. Suppose $\Sigma_{k=0}^{n} k = n(n+1)/2$ (the induction hypothesis). Since $\Sigma_{k=0}^{n+1} k = (n+1) + \Sigma_{i=0}^{n} k$, and by the induction hypothesis, the right side of the equality is equal to $(n+1) + n(n+1)/2$, we have $\Sigma_{k=0}^{n+1} k = (n+1) + n(n+1)/2$. Since

$$(n+1) + n(n+1)/2 = 2(n+1)/2 + n(n+1)/2 = (n+2)(n+1)/2,$$

$\Sigma_{k=0}^{n+1} k = (n+2)(n+1)/2$ follows. And that is what we had to show.

The reason that these arguments suffice to show that for all natural numbers n, $\Sigma_{k=0}^{n} k = n(n+1)/2$ is true, is the following. Given an arbitrary natural number, say 27, one can show that $\Sigma_{k=0}^{27} k = 27 \cdot 28/2$, i.e. $\varphi(27)$, as follows. First one shows $\varphi(0)$, but this is 1. above. Now, an instance of 2. reads: if $\varphi(0)$, then $\varphi(1)$. Since we had $\varphi(0)$, $\varphi(1)$ follows. Now, another instance of 2. reads: if $\varphi(1)$, then $\varphi(2)$. Since we have just proved $\varphi(1)$, $\varphi(2)$ follows. We repeat this process until we reach $n = 27$, and then we are done. What is required for this argument is that we can reach every natural number after a finite number of steps, starting from 0. One can view the repeated use of 2. as calls on the same algorithm but with different input.

Example 18 As another example, let us show $\Sigma_{k=0}^{n} 2^k = 2^{n+1} - 1$. Here, when writing $\psi(n)$ for the statement $\Sigma_{k=0}^{n} 2^k = 2^{n+1}$, to prove the statement it suffices to show that

1. $\psi(0)$,
2. $\psi(n)$ implies $\psi(n+1)$.

We prove 1. and 2. For 1., since $\Sigma_{k=0}^{0} 2^0 = 1$, and $2^1 - 1 = 1$, we have shown that $\psi(0)$ holds. The argument for 2. runs as follows. Suppose $\psi(n)$, that is, $\Sigma_{k=0}^{n} 2^k = 2^{n+1} - 1$ holds. Then, using the induction hypothesis, i.e. the assumption that $\psi(n)$ holds,

$$\Sigma_{k=0}^{n+1} 2^k = 2^{n+1} + \Sigma_{k=0}^{n} 2^k = 2^{n+1} + 2^{n+1} - 1 = 2 \cdot 2^{n+1} - 1 = 2^{n+2} - 1.$$

This proves $\psi(n+1)$. Thus we have shown that $\psi(n)$ implies $\psi(n+1)$, and thereby 2. is proved to be true.

6.2.2 Formulas

Natural numbers are not the only infinite sets to which proofs by induction apply. The arguments above suggest that this method of proof might be applicable to many sets that are defined inductively, e.g. to the set of propositional formulas $\mathcal{P}$. If we would wish to show that a certain property Θ holds for all formulas one could succeed by showing that

1. the statement holds for the propositional variables, i.e. $\Theta(p)$ holds for all propositional variables p,
2. if the statement holds for the formulas φ and ψ (the *induction hypothesis*), then it holds for $\neg\varphi$, $(\varphi \wedge \psi)$, $(\varphi \vee \psi)$ and $(\varphi \to \psi)$. In other words, if $\Theta(\varphi)$ and $\Theta(\psi)$ hold, then so do $\Theta(\neg\varphi)$, $\Theta(\varphi \wedge \psi)$, $\Theta(\varphi \vee \psi)$ and $\Theta(\varphi \to \psi)$.

Example 19 For example, let us show that in every formula the number of propositional formulas is at most one more than the number of connectives in it. For a formula φ, let $c(\varphi)$ denote the number of connectives in it, and $v(\varphi)$ the number of propositional variables in it. In this particular case we have to show that

1. for every formula that is a propositional variable, say p, $v(p) \leq c(p) + 1$,

2. if $v(\varphi) \leq c(\varphi) + 1$ and $v(\psi) \leq c(\psi) + 1$, then this also holds for $\neg\varphi$, $\varphi \wedge \psi$, $\varphi \vee \psi$ and $\varphi \rightarrow \psi$.

1. follows immediately: in the formula p, where p is a propositional formula, the number of atoms in it is 1 ($v(p) = 1$), and that is at most one more as the number of connectives in it, which is 0 ($c(p) = 0$). For 2., assume that $v(\varphi) \leq c(\varphi) + 1$ and $v(\psi) \leq c(\psi) + 1$. We have to treat the four mentioned formulas.

First, we show that $v(\neg\varphi) \leq c(\neg\varphi) + 1$. Observe that $v(\neg\varphi) = v(\varphi)$, and that $c(\neg\varphi) = c(\varphi) + 1$. Since by the induction hypothesis $v(\varphi) \leq c(\varphi) + 1$, it follows that $v(\neg\varphi) = v(\varphi) \leq c(\varphi)+1 = c(\neg\varphi) \leq c(\neg\varphi)+1$, and thus $v(\neg\varphi) \leq c(\neg\varphi)+1$.

Next we treat conjunction. We have to show that $v(\varphi \wedge \psi) \leq c(\varphi \wedge \psi) + 1$. Observe that $v(\varphi \wedge \psi) = v(\varphi) + v(\psi)$ and that $c(\varphi \wedge \psi) = c(\varphi) + c(\psi) + 1$. By the induction hypothesis this gives

$$v(\varphi\wedge\psi) = v(\varphi)+v(\psi) \leq c(\varphi)+1+c(\psi)+1 = \big(c(\varphi)+c(\psi)+1\big)+1 = c(\varphi\wedge\psi)+1.$$

And thus indeed $v(\varphi\wedge\psi) \leq c(\varphi\wedge\psi)+1$. The argument for $\vee$ and $\rightarrow$ are similar, because also in these cases $v(\varphi\vee\psi) = v(\varphi)+v(\psi)$ and $c(\varphi\vee\psi) = c(\varphi)+c(\psi)+1$, and $v(\varphi \rightarrow \psi) = v(\varphi) + v(\psi)$ and $c(\varphi \rightarrow \psi) = c(\varphi) + c(\psi) + 1$.

Again, let us see why these arguments suffice to show that for all formulas $v(\varphi) \leq c(\varphi) + 1$. For take an arbitray formula, say $\neg(p \wedge q)$. First, we use 1. to establish that $v(p) \leq c(p) + 1$ and $v(q) \leq c(q) + 1$. An instance of 2. reads: if $v(p) \leq c(p) + 1$ and $v(q) \leq c(q) + 1$, then $v(p \wedge q) \leq c(p \wedge q) + 1$. Thus we have established $v(p \wedge q) \leq c(p \wedge q) + 1$. Another instance of 2. reads: if $v(p\wedge q) \leq c(p\wedge q)+1$, then $v(\neg(p\wedge q)) \leq c(\neg(p\wedge q))+1$. And since we have already established $v(p\wedge q) \leq c(p\wedge q)+1$, we have arrived at $v(\neg(p\wedge q)) \leq c(\neg(p\wedge q))+1$, and that is what we had to show.

Example 20 We show by induction that every propositional formula is equivalent to one in which only negations and disjunctions occur. Thus we show

1. every atom is equivalent to a formula in which only negations and disjunctions occur,

2. if φ and ψ are equivalent to formulas in which only negations and disjunctions occur, then this also holds for $\neg\varphi$, $\varphi \wedge \psi$, $\varphi \vee \psi$ and $\varphi \rightarrow \psi$.

1. is clear. For 2. suppose φ and ψ are equivalent to formulas in which only negations and disjunctions occur, and let us call these formulas φ' and ψ'. Now $\neg\varphi$ is then equivalent to $\neg\varphi'$, and the latter clearly contains only negations and disjunctions. This treats the negation case. For $\varphi \vee \psi$, this is equivalent to $\varphi' \vee \psi'$, and this formula contains only negations and disjunctions, so we are done in the disjunction case too. For $\varphi \wedge \psi$, this formula is equivalent to $\neg(\neg\varphi' \vee \neg\psi')$, and this formula contains only negations and disjunctions, so done. For $\varphi \rightarrow \psi$, this is equivalent to $\neg\varphi' \vee \psi'$, done too.

6.3 Exercises

1. Give an inductive definition of the set of formulas in which the only connectives are negations and implications.
2. Given an inductive definition of the binairy words in which the number of 0's is even.
3. Give an inductive defintion of the binairy words for which the sum of their elements is odd.
4. Show by induction that $\Sigma_{k=0}^{n} k^2 = n(n+1)(2n+1)/6$.
5. Show by induction that $\Sigma_{k=0}^{n} k^3 = n^2(n+1)^2/4$.
6. Show by induction that that $\Sigma_{k=0}^{n} 3^k = (3^{n+1} - 1)/2$.
7. Show by induction that that $\Sigma_{k=0}^{n} 4^k = (4^{n+1} - 1)/3$.
8. Show by induction that the number of brackets in a formula is even.
9. Show by induction that every formula is equivalent to one in which only negations and conjunctions occur.
10. Show by induction that every formula is equivalent to one in which only negations and implications occur.
11. Show by induction that every formula in which the only connectives are negations contains one propositional variable.
12. Prove by induction that in each palindrome the number of 0's or the number of 1's is even.