On sets, functions and relations

Jeroen Goudsmit & Rosalie Iemhoff

A man ought to acquire wisdom by sharing it with others.

— Thomas Aquinas ("Sermon: Puer Iesus")

I hope I will not make it too difficult for you.
There will be some mathematics.

— Wim Veldman ("Perhaps perhaps")

October 23, 2012

Contents

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.

1 Sets

In this section the properties of sets will be studied. We start with the informal but intuitive notion of 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?

1.1 Notation

Sets will be denoted by latin capitals, often X, Y or A, B, the elements of sets by lower case letters. Fundamental to sets is the notion of "being an element of a given set", we write $x \in X$ to mean that x is an element of the set X. We write $x \notin X$ to say that x is not an element of X. Sets are completely determined by their elements. The only "observable" properties of sets are those pertaining to membership, so this makes it sensible to say that sets are extensional objects. To be a bit more precise, there is the axiom of extensionality (Extensionalitätsaxiom in German) which states that two sets are equal if and only if they have precisely the same elements. Symbolically, we can write this as

$$X = Y \quad \leftrightarrow \quad \forall a.\, a \in X \leftrightarrow a \in Y.$$

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. Due to extensionality the order in such a listing is wholly immaterial, and duplicates do not add anything new. That is to say, 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 $\{2, 1\}$.

It is important to note that the listing of elements may also be empty, in that there is a set with no elements at all. One could wonder whether there exist several such empty sets. The answer is an unequivocal no, and we prove this in Lemma 1 below. This ensures us that there is but one empty set, and we will denote this set $\emptyset$ from now on.

$\mathbb{N}$	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
$\mathbb{R} \setminus \mathbb{Q}$	the set of irrational numbers	de irrationale getallen
$\emptyset$	the empty set	de lege verzameling

Table 1.1: Commonly used sets.

1 Lemma
There exists precisely one set with no elements.

Proof. Suppose A and B are both sets without elements. This means that for any x we have $x \notin A$ and $x \notin B$. As a consequence, $x \in A$ holds if and only if $x \in B$, for indeed, both never hold. Extensionality now ensures us that $A = B$, proving the desired. ■

Given any specific object, there is a set having that object and that object alone as an element. We can describe such sets with but a single element in an easy manner as below.

1 Definition (Singleton)
A set X is called a singleton if there exists an a such that $x \in X$ if and only if $x = a$.

1 Example
The sets $\{0\}$ and $\{\emptyset\}$ are singletons.

2 Example
The set $\{1, 2\}$ is not a singleton. For suppose that it were, then there would be an a such that $x \in \{1, 2\}$ if and only $x = a$. Take such an a, then it must hold that $a = 1$ because $1 \in \{1, 2\}$. Likewise, we know that $a = 2$. It thus follows that $1 = 2$, which is blatantly false. We have arrived at a contradiction from the assumption that $\{1, 2\}$ is a singleton, so it is not a singleton.

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 exactly one element, but it is fairly difficult to compute. Sets given by descriptions are often denoted as follows:

$$\{\, n \in \mathbb{N} \mid n \text{ is an even number}\}\,, \quad \{\, p \in \mathbb{N} \mid p \text{ is a prime number}\}$$

Thus given a set X and some property φ, the set of elements of X for which φ holds is denoted as $\{\, x \in X \mid \varphi(x)\}$. Mnemonically, the symbol $\mid$ can be read as “for which”. Here φ is a property, which in a formal setting is given by a predicate formula and in an informal setting by a sentence. The set $\{\, x \in X \mid \varphi(x)\}$ can also be denoted as $\{\, x \mid x \in X, \varphi(x)\}$. Below follow some examples, see Table 1.1 for specific sets that one should know by heart.

3 Example
Both $\{\, n \in \mathbb{N} \mid n \text{ is odd }\}$ and $\{\, n \in \mathbb{N} \mid \ n = 2m + 1 \text{ for some } m \in \mathbb{N}\,\}$ are sets and contain precisely the odd numbers, hence they denote the very same set.

4 Example
Consider $\{ w \mid w$ is a sequence of 0's and 1's which sum equals 2 $\}$, which is a set. Moreover, it is equal to the set $\{ w \mid w$ is a sequence of 0's and 1's containing exactly two 1's $\}$.

5 Example
The set of true propositional formulae can be written as $\{ \varphi \mid \varphi$ is a propositional tautology$\}$.

6 Example (Solving Equations)
For any pair of real numbers $p, q \in \mathbb{R}$ we one can consider the set

$$S_{p,q} = \left\{ x \in \mathbb{R} \;\middle|\; x^2 - (p+q)x + p \cdot q = 0 \right\}$$

Using this construction we define $S = \{ S_{p,q} \mid p, q \in \mathbb{R}\}$, again a set. Is it the case that $\emptyset \in S$? It surely is not! For suppose that $\emptyset \in S$, then there would have to be $p, q \in \mathbb{R}$ such that $S_{p,q} = \emptyset$. Consider such $p, q \in \mathbb{R}$. Now see that $p \in S_{p,q}$, for we can easily compute

$$p^2 - (p+q) \cdot p + p \cdot q = p^2 - p^2 - q \cdot p + p \cdot q = 0.$$

Now as $p \in S_{p,q}$ and $S_{p,q} = \emptyset$ we have $p \in \emptyset$, but this is simply absurd. We have reached a contradiction from the assumption that $\emptyset \in S$, so we know $\emptyset \notin S$. Can you count the times we implicitly appealed to extensionality in this proof?

7 Example (Singletons)
Consider again the set $S_{p,q}$ of Example 6. For which $p, q \in \mathbb{R}$ is $S_{p,q}$ a singleton set? Recall that $S_{p,q}$ is a singleton if it has precisely one element. This means that for $S_{p,q}$ to be a singleton, there needs to be precisely one $x \in \mathbb{R}$ such that $x^2 - (p+q)x + p \cdot q = 0$. Realize that $(x-p)(x-q) = x^2 - (p+q)x + p \cdot q$, so if x is such that $x \in S_{p,q}$ then $x = p$ or $x = q$. It also follows that $p, q \in S_{p,q}$. From these two facts we can derive that $S_{p,q}$ is a singleton precisely if $p = q$.

For any number n, $\mathbb{N}_{\geq n}$ denotes the set of natural numbers at least as large as n, in our notation this is the set $\{ m \in \mathbb{N} \mid m \geq n\}$. Likewise, we write $\mathbb{N}_{>n}$ for the set of all numbers strictly larger than n, that is to say, $\{ m \in \mathbb{N} \mid m > n\}$. Similar notation will be used for the other common sets of Table 1.1. Note that when n is a natural number we have that $\mathbb{N}_{\geq n} = \{n, n+1, \ldots\}$ and $\mathbb{N}_{>n} = n+1, n+2, \ldots$. The set $\mathbb{N}_{\geq 1}$, or equivalently $\mathbb{N}_{>0}$, is sometimes denoted by $\mathbb{N}^+$ and contains all positive natural numbers.

When we can exhaustively list all elements of a set, this set is finite. Of course this list can be taken to be duplicate-free, so the length of this list is the number of distinct elements the set has. It thus makes sense to call this number, the number of elements really, the size of the set. We will denote this size by $\mid X \mid$. A set whose elements can not be exhaustively listed is inifinite

8 Example
The set $\emptyset$ is finite, for it has no elements at all. We have $\mid \emptyset \mid = 0$.

9 Example
The set {1,2, ..., n} is finite for any $n \in \mathbb{N}$, but the set $\mathbb{N}$ is infinite. Of course $\mid \{1, 2, \ldots, n\} \mid = n$.

1.2 Careful

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

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

Thus R consists of the sets that are not an element of itself. Does R belong to this set (itself) or not? If it does, thus if $R \in R$, then, by definition of R, also $R \notin R$. This cannot be, and thus we conclude that $R \notin R$. But then, by the definition of R, also $R \in R$. This cannot be either. Our only conclusion can be that R 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.

1.3 Operations on sets

Given two sets one can take their union, intersection and difference. These operations are formally defined as follows, and illustrated in Fig. 1.1.

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

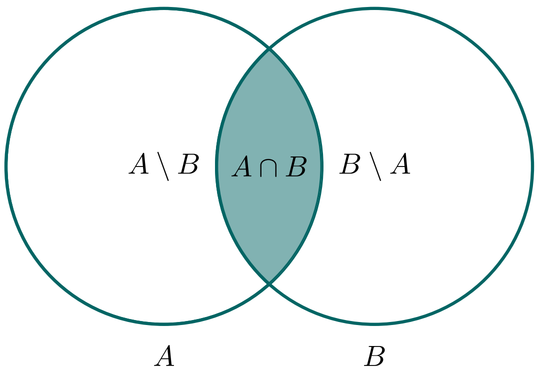

Figure 1.1: Sketch of set intersection and difference.

Two sets A and B are said to be disjoint if $A \cap B = \emptyset$. Given a set A one can form the union of all sets within A, defined as below. The operation of union defined above is actually a special case of this, as we will prove.

$$\bigcup A = \{\, x \mid \text{there exists an } a \in A \text{ such that } x \in a\}\,.$$

2 Lemma
Let A and B be sets. Now $A \cup B = \bigcup\{A, B\}$.

Proof. When we can show that for each x we have $x \in A \cup B$ if and only if $x \in \bigcup\{A, B\}$ then we are done by extensionality. First we unfold the left-hand definition, and note that $x \in A \cup B$ holds if and only if $x \in A$ or $x \in B$. Now to unfold the right hand definition, observe that $x \in \bigcup\{A, B\}$ if and only if there is an $y \in \{A, B\}$ such that $x \in y$. But the latter holds precisely if either $y = A$ or $y = B$. That is to say, $x \in \bigcup\{A, B\}$ if and only if $x \in A$ or $x \in B$, which we already know to be equivalent to $x \in A \cup B$. This finishes the proof. ∎

When we have an infinite $A = \{a_1, a_2, a_3, \dots\}$, one can see that $\bigcup A = a_1 \cup a_2 \cup \dots$, which is also written as $\bigcup A = \bigcup_{i=1}^{\infty} a_i$.

10 Example
Consider the set $N = \{\,\{n\} \mid n \in \mathbb{N}\}$. One can prove that

$$\bigcup_{i=0}^{\infty}\{i\} = \mathbb{N}.$$

Indeed, if $x \in \bigcup N$ then $x \in \{n\}$ for some $n \in \mathbb{N}$, and so $x = n$, which entails that $x \in \mathbb{N}$. Conversely, if $x \in \mathbb{N}$ then $x \in \{x\}$ and $\{x\} \in N$, so $x \in \bigcup N$.

1.4 Subsets

When each elements of the set X is an element of the set Y we say that X is a subset of Y, and denote this by $X \subseteq Y$. Thus $X \subseteq Y$ holds if and only if for all $x \in X$ we have $x \in Y$. Equality and being a subset are related to each other, in that $X = Y$ if and only if $X \subseteq Y$ and $Y \subseteq X$. Let us actually prove this.

3 Lemma
For any pair of sets X and Y, we have $X = Y$ if and only if $X \subseteq Y$ and $Y \subseteq X$.

Proof. First assume that $X = Y$. We now need to prove that $X \subseteq Y$, but this is not really hard. Assuming $x \in X$ of entails $x \in Y$, because $X = Y$ so X and Y have the same elements. By an analogous argument we see that $Y \subseteq X$ holds as well.

Now to prove the converse. Assume that $X \subseteq Y$ and $Y \subseteq X$. We want to show that $a \in X$ if and only if $a \in Y$. First, if $a \in X$ then $a \in Y$ by $X \subseteq Y$. The other way around, if $a \in Y$ then $a \in X$ follows from $Y \subseteq X$. This finishes the proof. ∎

Intuitively, subsets of a set at most as large as the original. It takes some doing to build up a sensible notion of size for all sets, we won't come to that until Chapter 3. At the moment we do have a notion of size for finite sets, as it was defined at the end of Section 1.1. We can validate whether our intuition holds up in this restricted case. To this end, let us first prove that size and union interact in the expected way.

4 Lemma
Given two finite sets X and Y we have $|\,X \cup Y\,| = |\,X\,| + |\,Y\,|$ when X and Y are disjoint.

Proof. Consider duplicate-free listings $x_1, \dots, x_n$ of X and $y_1, \dots, y_m$ of Y. Using these two listings we form $x_1, \dots, x_n, y_1, \dots, y_m$. Is this a duplicate-free listing of $X \cup Y$? Well, it certainly contains all elements of both X and Y, but the duplication freeness required further proof.

Suppose that the list contains a duplicate, that is to say, there are two elements on different positions in this listing that are actually the same. If these both come from the X-part of the listing, then the listing of X would have a duplicate, which it does not. Similarly, these items can not both come from the Y-part of the listing. This means that there are $i = 1, 2, \ldots, n$ and $j = 1, 2, \ldots, m$ such that $x_i = y_j$. But then we have that $x_i \in X$ and $x_i = y_j \in Y$, so $X \cap Y \neq \emptyset$. This contradicts the assumption that X and Y are disjoint, so there can not be a duplicate. We now have a duplicate-free listing of $X \cup Y$ of size $n + m$, proving the desired. ■

5 Lemma
Given two finite sets X and Y, if $X \subseteq Y$ then $|X| \leq |Y|$.

Proof. Consider some listing $y_1, \ldots, y_n$ of the elements of Y. We assume these listings to be duplicate free. Suppose that $X \subseteq Y$.

Note that for every $x \in X$ we have that $y \in Y$ so there is some $j = 1, 2, \ldots, n$ such that $x = y_j$. Now take some duplicate-free listing of X, say $x_1, \ldots, x_m$.

This gives us some sequence sequence $i_1, \ldots, i_m$ such that $x_j = y_{i_j}$ for all $j = 1, \ldots, m$. The sequence $i_1, \ldots, i_m$ is duplicate-free, and its length is equal to that of the given listing of X. Also note that the sequence $i_1, \ldots, i_m$ can have no more than n elements. This shows that $m \leq n$ as desired. ■

Does the converse of the above lemma always hold? Surely not, for $|\{3\}| \leq |\{1, 2\}|$, but $\{3\}$ is not a subset of $\{1, 2\}$ at all. When comparing numbers there is inequality and proper (or strict) inequality. We now define what it means to be a proper subset, which is to $\subseteq$ as $<$ is to $\leq$. This intuitive correspondence can also be made a bit more formal.

2 Definition
Given two sets X and Y, the former is said to be a proper subset of the latter, denoted $X \subset Y$, whenever $X \subseteq Y$ and $X \neq Y$.

When we have two finite sets X and Y such that $X \subseteq Y$ one can wonder whether $X \subset Y$. This follows immediately when $|X| < |Y|$. Indeed, if $X = Y$ were to hold then $|X| = |Y|$, which contradicts $|X| < |Y|$. Consequently, if $|X| < |Y|$ and $X \subseteq Y$ we know $X \subset Y$. The other direction, that is, from $X \subset Y$ follows $|X| < |Y|$ will Exercise 36.

There is another important operation on sets, namely forming the set of all subsets of a set, the so-called powerset (machtsverzameling in Dutch).

3 Definition (Powerset)
The powerset of a set X, denoted $\mathcal{P}(X)$, is defined as $\mathcal{P}(X) = \{ Y \mid Y \subseteq X \}$.

Let us first look at some examples of powersets.

11 Example (Singleton)
Is it always the case that the powerset of a singleton set has two elements? It surely is, and we can prove it. Suppose that X is any singleton set, this means that $X = \{a\}$ for some a. It is clear that $\emptyset \subseteq X$ and $X \subseteq X$, so $\emptyset \in \mathcal{P}(X)$ and $X \in \mathcal{P}(X)$ certainly both hold. From this we gather that $\{\emptyset, X\} \subseteq \mathcal{P}(X)$. To prove that $\mathcal{P}(X) = \{\emptyset, X\}$ we now only need to show that $\mathcal{P}(X) \subseteq \{\emptyset, X\}$ by Lemma 3.

So consider any $Y \in \mathcal{P}(X)$. By definition this means that $Y \subseteq X$. If $y \in Y$ then $y \in X$, so $y = a$ must follow. This means that either Y has no elements at all, in which case $Y = \emptyset$, or Y has an element, in which case it equals X. In both cases we see that $Y \in \{\emptyset, X\}$, proving the desired.

12 Example
The powerset of $\{1, 2\}$ is $\mathcal{P}(\{1, 2\}) = \{\emptyset, \{1\}, \{2\}, \{1, 2\}\}$.

13 Example
The powerset of the set of reals, $\mathcal{P}(\mathbb{R})$, is the set of sets of real numbers. E.g. $\{1, \pi, -72\} \in \mathcal{P}(\mathbb{R})$.

There are several intuitive truths about powersets. If Y is a subset of X, then the powerset of X ought to contain all subsets of Y as well. This we prove quite readily below.

1 Theorem
Let X and Y be sets such that $X \subseteq Y$, then $\mathcal{P}(X) \subseteq \mathcal{P}(Y)$.

Proof. Suppose that $X \subseteq Y$ and consider an element $x \in \mathcal{P}(X)$. By definition we know that $x \subseteq X$. But as $X \subseteq Y$ holds by assumption, we can deduce that $x \subseteq Y$. Hence $x \in \mathcal{P}(Y)$, proving the desired. ■

One can notice a regularity in the size of powersets of finite sets. If X is a finite set and w is some element not contained within X, then $Y = X \cup \{w\}$ is another set. One can compute that $|\,Y\,| = |\,X\,| + 1$, but this also follows from general theory, namely from Lemma 4. Any subset $A \subseteq X$ gives rise to two distinct subsets of Y, namely A itself, and $A \cup \{w\}$. Conversely, every subset $A \subseteq Y$ either contains A or it does not, and $A \setminus \{w\}$ is a subset of X. This counting argument shows that $|\,\mathcal{P}(Y)\,| = 2 \cdot |\,\mathcal{P}(X)\,|$.

Futhermore, we can also show that $|\,\mathcal{P}(\emptyset)\,| = 1$. These two equations together suggest that $|\,\mathcal{P}(X)\,| = 2^{|\,X\,|}$ for any finite set X. Using mathematical induction one could prove that this equation is already entailed by the previous two. Let us prove it from scratch instead.

2 Theorem
For finite sets X we have $|\,\mathcal{P}(X)\,| = 2^{|\,X\,|}$.

Proof. Consider a set X with n elements. Put the elements of X in a certain order, it does not matter which, say $X = \{x_1, \ldots, x_n\}$. There is a correspondence between sequences of 0's and 1's of length n, and subsets of X. Given a sequence $i_1, \ldots, i_n$ 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 corresponds to a unique subset of X and vice versa. There are 2^n such sequences, and thus as many subsets of X. ■

1.5 The natural numbers

The set ω is the smallest set satisfying the following two properties:

$\emptyset \in \omega$,

if $x \in \omega$, then $(x \cup \{x\}) \in \omega$.

Thus the first four elements of ω are

$$\emptyset \quad \{\emptyset\} \quad \{\emptyset, \{\emptyset\}\} \quad \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}.$$

If we interpret $\emptyset$ as 0, and $x \cup \{x\}$ as $x + 1$, then we could view ω as a representation of $\mathbb{N}$ with $+$.

1.6 The Cantor set

Not all sets are easy to visualize. This is an example of an intriguing set: it is the result of the following process:

> start with the interval [0,1] and delete the open middle third $(\frac{1}{3}, \frac{2}{3})$,
>
> from the remaining line fragments delete the open middle third, and repeat this process indefinitely.

Thus after the first step the intervals $[0, \frac{1}{3}]$ and $[\frac{2}{3}, 1]$ remain. After the second step remain $[0, \frac{1}{9}]$ and $[\frac{2}{9}, \frac{3}{9}]$, $[\frac{6}{9}, \frac{7}{9}]$ and $[\frac{8}{9}, 1]$, and so on. The Cantor set has many special properties, which we will encounter in the next chapters. Which elements certainly belong to the set?

1.7 Exercises

1 Exercise (Set Notation)
Write in set-notation the set of:

(i) number that are squares of natural numbers;

(ii) all vowels.

2 Exercise (Divisibility)
Give three set-notations for the set of non-negative integers divisible by 3.

3 Exercise (More Set Notation)
Describe the following sets in plain words:

(i) $\{ x \in \mathbb{Q} \mid 0 < x < 1 \}$;

(ii) $\left\{ x \in \mathbb{R} \mid \exists y \in \mathbb{Q}.\, x = y^2 \right\}$;

(iii) $\left\{ x \in \mathbb{R} \mid \exists y \in \mathbb{R}.\, x = y^2 \text{ and } y > 2 \right\}$;

(iv) $\left\{ n \in \mathbb{N} \mid n^2 > n \right\}$.

4 Exercise (Difficulty Deciding)
Give an example of a set for which it is (at present) difficult to decide if it is empty or not.

5 Exercise (Squares)
How many elements does the set $\left\{ x \in \mathbb{R} \mid x^2 = x \right\}$ have? Give a different set-notation for the set.

6 Exercise (Elements & Counting)
Does $\{0\} \in \mathbb{N}$ hold? How many elements does $\{\{\mathbb{N}\}\}$ have?

7 Exercise

Does the equality below hold? Prove your answer.

$$\left\{ \{x, y\} \;\middle|\; x, y \in \mathbb{N}_{>0} \text{ and } \frac{x}{y} = \frac{y}{x} \right\} = \{ n \mid n \in \mathbb{N} \}$$

8 Exercise (Non-Empty)

Prove that for any set X, if $X \neq \emptyset$ then there is some x such that $x \in X$.

9 Exercise (Squares Again)

Does $\{ x \in \mathbb{R} \mid \exists y.\, x = y^2 \} = \mathbb{R}_{\geq 0}$ hold? What about $\{ x \in \mathbb{Q} \mid \exists y.\, x = y^2 \} = \mathbb{Q}_{\geq 0}$?

10 Exercise (Properties of Intersection)

Let X, Y and Z be arbitrary sets. Prove that:

(i) $X \cap X = X$;

(ii) $X \cap \emptyset = \emptyset$;

(iii) if $X \subseteq Y$ then $X \cap Y = X$;

(iv) if $X \subseteq Y$ and $Y \cap Z = \emptyset$ then $X \cap Z = \emptyset$.

(v) $X \cap Y \subseteq X$ and $X \cap Y \subseteq Y$;

(vi) if $Z \subset X$ and $Z \subseteq Y$ then $Z \subseteq X \cap Y$;

11 Exercise (Properties of Union)

Let X, Y and Z be arbitrary sets. Prove that:

(i) $X \cup X = X$;

(ii) $X \cup \emptyset = X$;

(iii) if $X \subseteq Y$ then $X \cup Y = Y$;

(iv) if $X \subseteq Y$ and $Y \cup Z = Y$ then $X \cup Z = Y$.

(v) $X \subseteq X \cup Y$ and $Y \subseteq X \cup Y$;

(vi) if $X \subseteq Z$ and $Y \subseteq Z$ then $X \cup Y \subseteq Z$.

12 Exercise (Distributive Laws)

The operations $\cap$ and $\cup$ relate to one another. Which of the following two equalities hold for all sets A, B, C? Do prove your answer.

$$\begin{aligned} (A \cap B) \cup C &= (A \cup C) \cap (B \cup C) \\ (A \cup B) \cap C &= (A \cap C) \cup (B \cap C) \end{aligned}$$

13 Exercise (Logic)

If you read $\vee$ for $\cup$ and $\wedge$ for $\cap$, and A, B, C are propositional formulas, are the equalities in Exercise 12 valid equivalences?

14 Exercise (Symmetry)

Which of the following hold for all sets A and B? Prove your answer.

$$\begin{array}{rcl} A \cap B & = & B \cap A \\ A \cup B & = & B \cup A \\ A \setminus B & = & B \setminus A \end{array}$$

15 Exercise (Properties of Difference)

Let X and Y be arbitrary sets. Prove that:

(i) $X \setminus \emptyset = X$;

(ii) $X \setminus X = \emptyset$;

(iii) $X \setminus Y = \emptyset$ if and only if $X \subseteq Y$;

(iv) $X \setminus (X \setminus Y) = X \cap Y$;

(v) $X \cap (Y \setminus X) = \emptyset$;

16 Exercise (More Properties of Difference)

Let X and Y be sets such that $X \subseteq Y$. Prove that:

(i) $X \cup (Y \setminus X) = Y$;

(ii) $Y \setminus (Y \setminus X) = X$;

17 Exercise

Recall Exercise 10. In this exercise we will re-prove parts of that exercise, using earlier established "structural properties" of intersection.

(i) Prove Exercise 10.(i) from (v), (vi) of the same exercise and Lemma 3.

(ii) Prove that for any set X we have $X \subseteq \emptyset$ if and only if $X = \emptyset$.
Hint: This question is partially covered by Exercise 22.

(iii) Use the above item together with Lemma 3.(v) to prove Lemma 3.(ii).

18 Exercise

In Exercise 17 we investigated Exercise 10. Perform a similar analysis of Exercise 11. That is to say, prove (i), (iii), (iv) of Exercise 11 using (v) and (vi). Can you use these two items to prove (ii) too?

19 Exercise (More Distributive Laws)
As in Exercise 12, we look at the relation between several of the common set-operations. Which of the following two equalities hold for all sets A, B, C? Prove your answer.

$$\begin{array}{rcl} C \setminus (A \cap B) & = & (C \setminus A) \cup (C \setminus B) \\ C \setminus (A \cup B) & = & (C \setminus A) \cap (C \setminus B) \end{array}$$

20 Exercise (Some More Distributivity)
Prove that for any pair of sets A and B the following holds:

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

21 Exercise (Symmetric Difference)
Given two sets A and B we can define the symmetric difference as $A \oplus B = (A \setminus B) \cup (B \setminus A)$. Which of the following equalities hold for all sets A, B and C? Prove your answer.

$$\begin{array}{rcl} A \oplus B & = & B \oplus A \\ A \oplus A & = & \emptyset \\ A \oplus \emptyset & = & A \\ A \oplus (B \cup C) & = & (A \oplus B) \cup (A \oplus C) \end{array}$$

22 Exercise (Empty Subset)
Given any set A, is $\emptyset$ a subset of A?

23 Exercise (Powerset of Empty Set)
Give $\mathcal{P}(\emptyset)$. How many elements does it have?

24 Exercise (Describing the Powerset)
What are the subsets of $\{\text{appel}, \text{moes}\}$? How many are there?

25 Exercise (Subsets)
Write down all subsets of $\{1, 2, 3, 4\}$. How many do you expect to get?

26 Exercise (Elements of the Powerset)
Given a set X, is $\emptyset$ an element of $\mathcal{P}(X)$? And is $X \in \mathcal{P}(X)$?

27 Exercise
Let X and Y be finite sets. Prove that $|X \cup Y| = |X| + |Y| - |X \cap Y|$.
Hint: For inspiration, look at the proof of Lemma 4.

28 Exercise
For which of the following sets do there exist real numbers r, s such that $r < s$ and the interval $[r, s]$ is a subset of that set? Prove your answer.

(i) $\mathbb{R} \setminus \mathbb{Q}$;

(ii) $\mathbb{R} \setminus \{ x \in \mathbb{R} \mid \text{the decimal expansion of } x \text{ does not contain the string } 11\}$;

29 Exercise
Give an argument that in some sense shows that the sets $\big\{ \{n\} \bigm| n \in \mathbb{N} \big\}$ and $\mathbb{N}$ have "the same size".

30 Exercise
Describe $\bigcup \omega$.

31 Exercise
Does there exist a subset of the natural numbers X for which $X \in X$? And are there sets of real numbers A and B such that $\{A\} \in B$ and $B \subseteq A$?

32 Exercise (Sequences of Sets)
Consider a sequence of sets $A_1, A_2, A_3, \ldots$.

(i) Is there such a sequence such that $A_i \subset A_{i+1}$ for all i?

(ii) Suppose that $A_i \in \{A_{i+1}\}$ for all i, what can you now say about this sequence?

(iii) Now suppose that $A_1 = \{1\}$ and $A_{i+1} = \{A_1, \ldots, A_i\}$. Does the following hold: for every $x \in y \in A_{i+1}$, either $x = 1$ or $x \in A_i$? Prove your answer.

33 Exercise
How many subsets does $\{ n \in \mathbb{N} \mid 0 \leq n \leq 5\}$ have? And $\mathbb{N}$?

34 Exercise
What are the elements of $\mathcal{P}(\mathbb{R} \setminus \mathbb{Q})$? And what are the elements of $\mathcal{P}(\mathbb{R}) \setminus \mathbb{Q}$?

35 Exercise (Inequality Reflected in Powerset)
Prove that if $X \neq Y$, then $\mathcal{P}(X) \neq \mathcal{P}(Y)$.

36 Exercise (Size and Subsets)
Let X and Y be finite sets and assume that $X \subseteq Y$.

(i) Prove that $X = Y$ if and only if $|X| = |Y|$.
Hint: Use Lemma 5.

(ii) Prove that $X \subset Y$ if and only if $|X| < |Y|$.

37 Exercise (Intersections)
Let X be any non-empty set. Now define

$$\bigcap X = \{ a \mid \text{for all } x \in X, a \in x\}$$

Prove the following:

(i) given any pair of sets X and Y it holds that $X \cap Y = \bigcap\{X, Y\}$;

(ii) given sets X and Y we have $Y \cup \bigcap X = \bigcap\{\, x \cup Y \mid x \in X \}$ whenever X is non-empty;

Hint: By Lemma 3 it suffices to prove that

$$Y \cup \bigcap X \subseteq \bigcap\{\, x \cup Y \mid x \in X \} \text{ and } \bigcap\{\, x \cup Y \mid x \in X \} \subseteq Y \cup \bigcap X.$$

The former can be shown directly. The latter is easier proven by contraposition. That is to say, prove that for any a the assumption $a \notin Y \cup \bigcap X$ yields $a \notin \bigcap\{\, x \cup Y \mid x \in X \}$. Show that this proves $\bigcap\{\, x \cup Y \mid x \in X \} \subseteq Y \cup \bigcap X$.

(iii) for any set X and $A \in X$ we have $\bigcap X \subseteq A$.

2 Relations

The elements of a set are not ordered. That is, $\{1, 2\}$ is the same set as $\{2, 1\}$. One sometimes calls sets with two elements an unordered pair. In this section we will encode ordering in sets, and use this to describe relations using sets.

It is instructive to first consider the use of the word relation in daily speech. In the following sentences the word occurs explicitly: "John has a relationship with Mary." "There is a relation between mass and force." 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 with a specific order, denoted by $\langle\, a, b\,\rangle$. We want to cast it in terms of sets. Therefore, we define

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

Note that this is a definition, a mere coding of an intuitive notion. We have to verify that this coding has the properties ones wishes an ordered pair to have.

This coding does satisfy these properties. Indeed, from $\{\{a\}, \{a, b\}\}$ we can read of which element is the first of the ordered pair, a, and which is the second, b. Moreover, we see that $\langle\, a, b\,\rangle = \langle\, c, d\,\rangle$ if and only if $a = c$ and $b = d$.

Before we go on to define a relation, let us first inspect a bit the set of all ordered pairs one can construct from two sets. We will give this set a name, and look at some of its properties.

4 Definition (Cartesian Product)
The cartisian product of two sets A and B, denoted $A \times B$, is the set of all ordered pairs $\langle\, a, b\,\rangle$ where $a \in A$ and $b \in B$.

14 Example
The cartesian product of the set $\{1, 2\}$ with $\{a, b, c\}$ is given by the following set of ordered pairs.

$$\{\, \langle\, 1, a\,\rangle, \langle\, 1, b\,\rangle, \langle\, 1, c\,\rangle, \langle\, 2, a\,\rangle, \langle\, 2, b\,\rangle, \langle\, 2, c\,\rangle, \,\}\,.$$

To make abundantly clear the beauty of writing $\langle\, a, b\,\rangle$ for $\{\{a\}, \{a, b\}\}$, the above set comes down to the following when we do away with this abbreviation.

$$\Big\{\, \{\{1\}, \{1, a\}\}\,, \{\{1\}, \{1, b\}\}\,, \{\{1\}, \{1, c\}\}\,, \{\{2\}, \{2, a\}\}\,, \{\{2\}, \{2, b\}\}\,, \{\{2\}, \{2, c\}\}\,\Big\}\,.$$

There are many sensible questions one could ask about this product. First of all, can one actually think of this as a product? The product of natural numbers, dear to us all, satisfies some properties, and for this so-called product to "piggyback" on that intuition it had better satisfy these properties too. Unfortunately we need some more technical machinery to ask these questions in a more appropriate manner, but the basic idea is this: the product acts akin to the product of natural numbers concerning the size of the sets involved. In this setting, the empty set is similar to zero and any singleton set is similar to one. Let us put all these, admittedly vague, claims to test.

6 Lemma

Let X be any set. Now $X \times \emptyset = \emptyset$.

Proof. We know that $a \in X \times \emptyset$ when $a = \langle x, y \rangle$ for $x \in X$ and $y \in \emptyset$. But there can never be such a y, hence no such a exists. This proves that $X \times \emptyset \subseteq \emptyset$, whence the desired follows. ∎

7 Lemma

Let X and Y be finite sets. Now $|X \times Y| = |X| \cdot |Y|$.

Proof. Pick any listing $x_1, \ldots, x_n$ of X and $y_1, \ldots, y_m$ of y. A listing of the set $X \times Y$ can now be given as in Table 2.1. One can readily see that this listing has $n \cdot m$ elements, proving the desired. ∎

	x_1	x_2	$\ldots$	x_n
y_1	$\langle x_1, x_2 \rangle$	$\langle x_2, y_1 \rangle$	$\ldots$	$\langle x_n, y_1 \rangle$
y_1	$\langle x_1, y_1 \rangle$	$\langle x_2, y_2 \rangle$	$\ldots$	$\langle x_n, y_2 \rangle$
$\vdots$	$\vdots$		$\ddots$	
y_m	$\langle x_1, y_m \rangle$	$\langle x_2, y_m \rangle$	$\ldots$	$\langle x_n, y_m \rangle$

Table 2.1: Listing of all elements of X on the horizontal axis, Y on the vertical axis, and the filled-out square is a listing of $X \times Y$.

1 Corollary

Let X be any finite set and let Y be a singleton set. Now $|X \times Y| = |X|$.

Proof. By Lemma 7 we know that $|X \times Y| = |X| \times |Y|$. But Y was assumed to be a singleton set, so $|Y| = 1$. This immediately proves the desired. ∎

Equipped with a coding of ordered pairs, we can now code relations. Let us give a formal definiton.

5 Definition

A binary relation between the sets A and B is a subset of $A \times B$.

The word "binary" in this definition refers to this pertaining to a relation between two things. We will often omit this word from the nomenclature. We also will often omit the "ambient" sets A and B between which the relation occurs, and leave it up to the reader to infer this from context. This is a somewhat dangerous affair, for some relation properties to be discussed in Section 2.3 need this ambient data. In such settings we will be a bit more explicit.

To emphasize that we are dealing with relations we will often use R to refer to a relation. We also write $x \; R \; y$ to mean $\langle x, y \rangle \in R$. When R is a relation between A and A, we will say that R is a relation on A.

15 Example
The set $\{\langle 1, 2\rangle, \langle 3, 4\rangle\}$ is a relation, a relation consisting of two pairs.

16 Example
The set $\{\langle a, b\rangle, \langle b, a\rangle\}$ is a relation too.

17 Example (Order)
The set $\{\langle x, y\rangle \mid x, y \in \mathbb{R} \text{ and } x < y\}$ is a relation, and it relates a real number to every real number greater than it. From now on we will interpret the symbols $<$, $>$, $\leq$, $\geq$, all symbols that intuitively denote relations on the common sets of Table 1.1, as the relations they represent.

18 Example (More Squares)
We can relate each natural number to its square, $\left\{\langle n, m\rangle \,\middle|\, n, m \in \mathbb{N} \text{ and } n^2 = m\right\}$. This is a relation on the natural numbers.

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

20 Example
The set $\left\{\langle q, r\rangle \in \mathbb{Q}_{\geq 0} \times \mathbb{R} \,\middle|\, \sqrt{q} = r\right\}$ is a relation between rational numbers at least as large as zero and real numbers.

21 Example
Continuous the above Example 20, we can relate a rational number q to a real number r when either q is negative and $r = 0$ or q and r are related by the relation in Example 20. This gives us the set $\left\{\langle p, q\rangle \in \mathbb{Q} \times \mathbb{R} \,\middle|\, (q \geq 0 \text{ and } \sqrt{q} = r) \text{ or } (q < 0 \text{ and } r = 0)\right\}$.

22 Example
The set $\{\langle w, n\rangle \mid w \text{ is a sequence of } n \text{ 0's and } n \text{ 1's}\}$ is a relation between sequences (of ones and zeroes) and their length.

23 Example
The set $\{\langle \varphi, \psi\rangle \in \mathcal{L}_{\mathsf{PROP}} \times \mathcal{L}_{\mathsf{PROP}} \mid \varphi \leftrightarrow \psi \text{ is a tautology}\}$ is a relation on the set of propositional formulas $\mathcal{L}_{\mathsf{PROP}}$.

24 Example (Lines in the Plane)
A straight line in the real plane can be seen as a specific kind of subset of $\mathbb{R}^2$. For the moment, let us be a little bit vague and simply define

$$\mathbb{L} = \left\{ L \in \mathcal{P}(\mathbb{R}^2) \,\middle|\, L \text{ is a line} \right\}.$$

We can define a relation R on $\mathbb{L}$ by setting $L\ R\ K$ if and only if $L \cap K$ is non-empty. That is to say, R relates lines that intersect in at least one point.

Let us again revisit the coding of ordered pairs. First note that $\langle x, y\rangle = \{\{x\}, \{x, y\}\} \in \mathcal{P}(\{x, y\})$ for any $x \in X$ and $y \in Y$. In turn, $\{x, y\}$ is a subset of $X \cup Y$. This means that $X \times Y$ is in fact a subset of $\mathcal{P}(\mathcal{P}(X \cup Y))$.

Given two sets X and Y we may want to join X and Y together, without loosing tack of which element came from which set. This can be done by taking the disjoint union.

6 **Definition (Disjoint Union)**
The disjoint union of sets X and Y, denoted $X+Y$, is the set

$$\{\langle x,0\rangle \mid x\in X\}\cup\{\langle y,1\rangle \mid y\in Y\}.$$

The disjoint union behaves like a sum concerning size, just like the cartesian product behaves like a product. One also calls the disjoint union the disjoint sum of coproduct. Given an element $a\in X+Y$ one can determine whether a comes from X or Y, because when $a=\langle v,w\rangle$ and $w=0$ we know $v\in X$, and if $w=1$ then $v\in Y$.

25 **Example**
The disjoint union of $\mathbb{N}$ and $\mathbb{N}$ is the set $\{\langle n,m\rangle\in\mathbb{N}\times\mathbb{N}\mid m=0 \text{ or } m=1\}$.

8 **Lemma**
Let X and Y be finite sets. Now $|X+Y|=|X|+|Y|$.

Proof. This is immediate from Lemma 4. ■

2.1 Relations of arbitrary arity

Above we saw relations between two elements. Examples of relations of arity greater than two are: "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; the relation $\{\langle n,m,k\rangle\in\mathbb{N}\times\mathbb{N}\times\mathbb{N}\mid n+m=k\}$; 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 ($\langle r,a,d,i,o\rangle$ 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.

$$\begin{aligned}\langle a,b,c\rangle &=_{def} \langle a,\langle b,c\rangle\rangle\\ \langle a,b,c,d\rangle &=_{def} \langle a,\langle b,c,d\rangle\rangle\end{aligned}$$

etc. We define relations of arity n inductively as follows

$$\langle a_1,\dots,a_{n+1}\rangle =_{def} \langle a_1,\langle a_2,\dots,a_{n+1}\rangle\rangle.$$

In the same way as above one can then show that

$$\langle a_1,\dots,a_n\rangle=\langle b_1,\dots,b_n\rangle \;\Leftrightarrow\; \forall i\le n.\, a_i=b_i.$$

Expressions $\langle a_1,\dots,a_n\rangle$ are called n-tuples. A set consisting of n-tuples is an n-ary relation. As mentioned above, a set of pairs we also call a binary relation. We define

$$A^n=\{\langle a_1,\dots,a_n\rangle \mid \forall i\le n(a_i\in A)\}.$$

26 **Example (Multiplication)**
The set $X=\{\langle n,m,k\rangle\mid n,m,k\in\mathbb{N} \text{ and } n\cdot m=k\}$ is a 3-ary (ternary) relation on natural numbers. We have that $\langle 1,n\rangle n\in X$ for all $n\in\mathbb{N}$, and one can also prove that if $\langle n,m,k\rangle\in X$ then $\langle m,n,k\rangle\in X$.

27 **Example**
For each natural number $n\in\mathbb{N}$ we can consider the set

$$\left\{\langle a_1,\dots,a_n\rangle\in\mathbb{R}^{n+1}\;\middle|\; a_1+a_2+\dots a_n=0\right\}.$$

This is a n-ary relation.

28 **Example**
The set $\left\{\langle\varphi,\psi,\chi\rangle\in\mathcal{L}^3_{\mathsf{PROP}}\;\middle|\;\varphi\wedge\psi\to\chi \text{ is a tautology}\right\}$ is a 3-ary relation.

2.2 Pictures

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

$$x \longrightarrow y$$

If both $x \; R \; y$ and $y \; R \; x$ hold we draw in one of the three following ways:

$$\begin{tikzcd} x \arrow[r, bend left] & y \arrow[l, bend left] \end{tikzcd} \qquad \begin{tikzcd} x \arrow[r, leftrightarrow] & y \end{tikzcd} \qquad \begin{tikzcd} x \arrow[r, dash] & y \end{tikzcd}$$

Below two figures, the left-hand side corresponds to the relation $\{\langle 0, 1 \rangle, \langle 0, 2 \rangle, \langle 1, 2 \rangle\}$ and the right-hand side figure corresponds to $\{\langle 0, 0 \rangle, \langle 0, 1 \rangle, \langle 0, 2 \rangle, \langle 1, 2 \rangle, \langle 2, 1 \rangle\}$.

$$\begin{tikzcd} 0 \arrow[r] \arrow[dr] & 1 \arrow[d] \\ & 2 \end{tikzcd} \qquad\qquad \begin{tikzcd} 0 \arrow[loop left] \arrow[r] \arrow[dr] & 1 \arrow[d, bend left] \\ & 2 \arrow[u, bend left] \end{tikzcd}$$

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

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

with picture

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

The relation $\{0, 1, 2\}^2 \setminus \{\, \langle x, x \rangle \mid x \in \{0, 1, 2\}\}$ corresponds to this picture:

$$\begin{tikzcd} 0 \arrow[r, dash] \arrow[dr, dash] & 1 \arrow[d, dash] \\ & 2 \end{tikzcd}$$

2.3 Properties of relations

In this section we focus on relations on a set. Many of the relations we are already familiar with are of this form, for instance the orders on the common sets. Such relations can have several interesting properties. We introduce a few of the properties here, and give several examples. In Fig. 2.5, we graphically illustrate some of these properties. It may be helpful to look at these pictures while reading the formal definition. Let us now go through some properties, rougly in increasing order of complexity.

7 **Definition (Reflexive)**
A relation R on X is said to be reflexive when for each $x \in X$ we have $x \; R \; x$.

29 Example
The relation $\subseteq$ on $\mathcal{P}(X)$ for any set X is reflexive. Indeed, $Y \subseteq Y$ always holds.

30 Example
The relation $\leq$ on natural numbers is reflexive, because any $x \in \mathbb{N}$ is less than or equal to x. Similarly, the same relation on the other common sets, such as the integers, rational numbers, real numbers and irrational numbers are all reflexive.

31 Example
Contrary to $\leq$, the relation $<$ on the natural number is not reflexive. It is easy to see that $0 < 0$ is not true at all. In fact, there is no natural number $x \in \mathbb{N}$ for which $x < x$ hold. The same goes for the less-than order on any of the common sets.

32 Example
Consider the relation $R = \{ \langle x, y \rangle \in \mathbb{Z} \times \mathbb{Z} \mid x + y \text{ is even}\}$. This relation is reflexive, because $x + x = 2 \cdot x$ is always even.

33 Example (Empty Relations are usually not Reflexive)
The relation $R = \emptyset$ on $\emptyset$ is reflexive, because for each $x \in \emptyset$ we have $x \ R \ x$. But the empty relation $R = \emptyset$ on any set $X \neq \emptyset$ is not reflexive, and we can prove this. For suppose that R were reflexive. Then $x \ R \ x$ would hold for all $x \in X$. Because $X \neq \emptyset$ we know that $x \in X$ holds for some x, as you were asked to prove in Exercise 8. Now $x \ R \ x$ must hold, so $\langle x, x \rangle \in R = \emptyset$. This is of course utter nonsense, so the assumption that R is reflexive is false. We have now proven what we set out to prove.

34 Example (Divisibility)
Consider the relation $\mid$ of divisibility on the natural numbers, defined as

$$n \mid m \text{ if and only if there exists a } k \in \mathbb{N} \text{ such that } nk = m.$$

Pronounce $n \mid m$ as "n is a divisor of m". This relation is reflexive, because $n \cdot 1 = n$.

35 Example
Recall the relation R from Example 32 and $\mid$ from Example 34. Realize that R actually satisfies the following equality.

$$R = \left\{ \langle x, y \rangle \;\middle|\; 2 \mid (x + y) \right\}$$

We can generalize this definition by replacing 2 by an arbitrary other natural number. Let us define $R_n = \left\{ \langle x, y \rangle \;\middle|\; n \mid (x + y) \right\}$, and for the moment think about R_3. Is the relation R_3 reflexive too? It most certainly is not! We quite readily can compute that $1 + 1 = 2$, but $3 \mid 2$ does not hold.

8 Definition (Symmetric)
A relation R on X is said to be symmetric when for each $a, b \in X$ we have $a \ R \ b$ whenever $b \ R \ a$.

Note that in the definition of symmetry we might as well have said that $a \ R \ b$ holds if and only if $b \ R \ a$.

36 Example (Lines Again)
Recall the set $\mathbb{L}$ and the relation R from Example 24. This relation R is symmetric, and we can prove this. For suppose that $L \ R \ S$, then $L \cap S$ is non-empty. In Exercise 14 you were asked to see whether $L \cap S = S \cap L$. This is indeed the case, and due to this, $S \cap L$ is non-empty as well. Consequently, $S \ R \ L$ as desired.

37 Example (Anti-Symmetry)
The relation $\leq$ on natural numbers is not symmetric. In fact, it is even called anti-symmetric, another interesting property of relations we visit in Definition 13. One can see that if $n \leq m$ and $m \leq n$ both were to hold, then $n = m$ follows for any $n, m \in \mathbb{N}$. Now see that $1 \neq 2$, so from the above reasoning we know that $1 \leq 2$ and $2 \leq 1$ can not both hold. Of course, we already know that $2 \leq 1$ does not hold due to intuitive reasons, but it never hurts to have several compelling arguments around.

9 Definition (Transitive)
A relation R on X is said to be transitive when for each $a, b, c \in X$ we have that if $a \ R \ b$ and $b \ R \ c$ then $a \ R \ c$.

38 Example
Let X be any set. The relation $R = X \times X$ is transitive by virtue of relating everything.

39 Example
Consider $\emptyset \subseteq X \times X$ as a relation on X. It is transitive by virtue of relating nothing at all.

40 Example (Divisibility Revisted)
Recall again Example 34. This relation is transitive, a proof of which we leave to you in Exercise 50 In Fig. 2.1 we graphically depicted the relation of divisibility. This relation is quite wild, and is not especially well-suited to a nice planar representation. To smoothen things over we omit the reflexive arrows, which we already know to be there. Moreover, we also omit the arrows guaranteed by transitivity whenever possible.

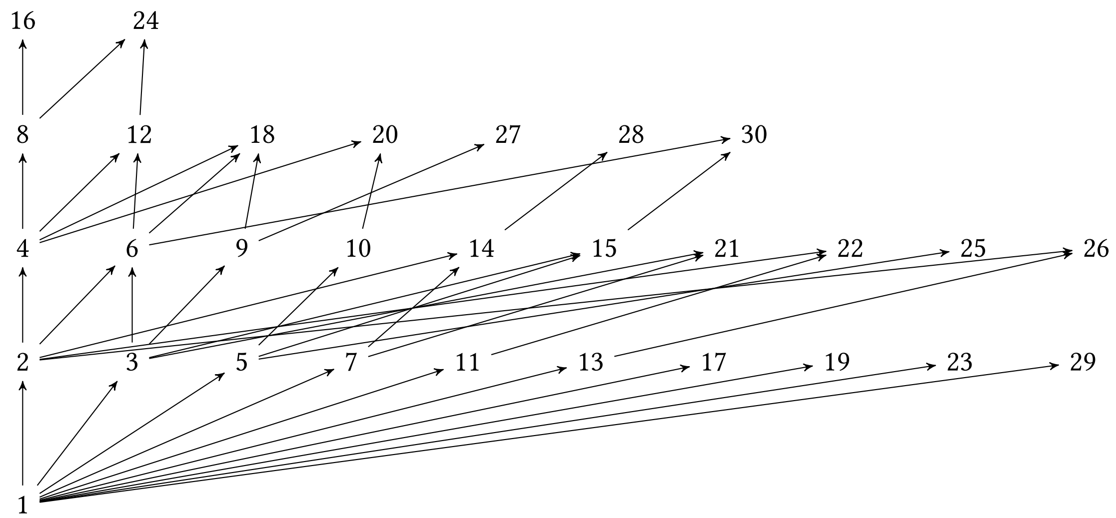

Figure 2.1: Depiction of the divisibility relation of Example 34. Reflexive and transitive arrows are not shown, but they are known to exist by the aforementioned example and Exercise 50.

41 Example (Lines)
Consider the picture in Fig. 2.2. For the purpose of this example, assume that K and L are perfectly parallel. Unfortunately this can not be inferred from the picture, but such lines can surely be constructed. We can quite readily see that $K \ R \ L$ and $L \ R \ M$, but $K \ R \ L$ does not hold. This proves that R is not transitive at all.

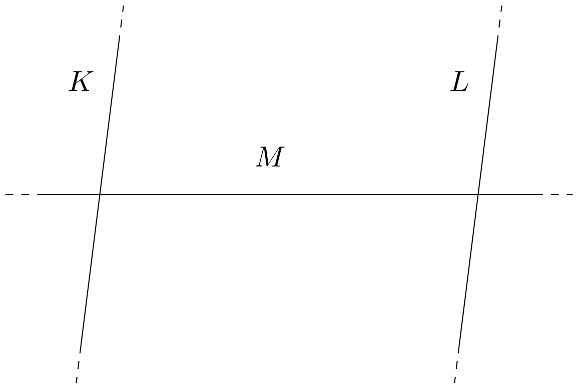

Figure 2.2: Three intersecting lines, but the outer lines do not intersect.

42 Example
The orders $\leq$ and $<$ of Example 30 and Example 31 respectively are both transitive.

43 Example (Subsequences)
Consider the set X of sequences of latin letters. We say that a sequence w is a subsequence of a sequence v when v is simply w, potentially padded with letters on the side. Let R be the relation of "being a subsequence of". Observe that "tom" is a subsequence of "tomato", and "thema" is a subsequence of "mathematics", but "spain" is not a subsequence of "europe", and neither is "apples" a subsequence of "apple". The relation R is an example of a transitive relation.

44 Example (Equality)
The relation $=$ on any set X is an example of a relation that is transitive. Furthermore, the relation is symmetric and reflexive as well. We will write id_X to mean this relation, to avoid confusion by using $=$ in unexpected placed. To be a little bit more precise, define

$$\mathrm{id}_X = \{ \langle a, b \rangle \in X \times X \mid a = b \} .$$

Transitivity respects intersections, in the sense that the intersection of two transitive relations is again transitive. We prove this formally, and leave Exercise 51 as an exercise to you.

9 Lemma
Let X be a set and let R and S be relations on X. If both R and S are transitive, then so is the relation $T = R \cap S$.

Proof. Suppose that $a, b, c \in X$ are such that $a\ T\ b$ and $b\ T\ c$. We now know that $a\ R\ b$ and $b\ R\ c$, but we also know that $a\ S\ b$ and $b\ S\ c$. Transitivity of R ensures that $a\ R\ c$, similarly, transitivity of S ensures that $a\ S\ c$. These two facts together prove that $a\ T\ c$ as desired. ∎

One could wonder whether transitivity is similarly respected by union. You are asked to inspect this in Exercise 52. Let R be any relation on a set X. We can "extend" the relation R in a minimal way to a relation S on X such that S is transitive. To be precisely, we can define the following. Note the similarity with the properties discussed in Exercise 59 and 60, hence their suggestive names.

10 Definition (Transitive Closure)

Let R be a relation on a set X. A relation S is said to be a transitive closure of the relation R if it satisfies the following three properties:

(i) the relation S extends R, in that $R \subseteq S$;

(ii) the relation S is transitive;

(iii) any transitive relation T on X such that $R \subseteq T$ satisfies $S \subseteq T$.

Does such a transitive closure always exist? Well, the definition already suggests a construction. Simply take the set $\mathcal{R}$ of all transitive relations T such that $R \subseteq T$. If the set $\mathcal{R}$ were non-empty, then we could take its intersection as defined per Lemma 9. This intersection will again be a transitive relation due to Exercise 51. We have sufficient intuition to attempt a formal proof, so let us get to work.

10 Lemma

Let X be any set and let R be a relation on X. There exists a transitive closure of R.

Proof. Consider the set $\mathcal{R}$ defined as

$$\mathcal{R} = \left\{\, T \subseteq X \times X \;\middle|\; T \text{ is a transitive relation on } X \text{ and } R \subseteq T \,\right\}.$$

Realize that $X \times X \in \mathcal{R}$ as explained in Example 38. This makes $\mathcal{R}$ a non-empty set. We can thus define $S = \bigcap \mathcal{R}$.

We now need but verify that this set S indeed is a transitive closure of R, so we need to check whether all the properties demanded in Definition 10 holds.

Note that the set S is a relation on X and S is transitive due to Exercise 51, so (ii) surely holds. To see that (i) holds, assume that $a \; R \; b$ for $a, b \in X$. This in turn ensures that $a \; T \; b$ for all $T \in \mathcal{R}$, because $R \subseteq T$ holds for those relations T. As a consequence, $\langle\, a, b \,\rangle \in \bigcap \mathcal{R}$, so $a \; S \; b$ follows by construction.

Finally, we need to check (iii). Take some transitive relation T such that $R \subseteq T$. This surely entails that $T \in \mathcal{R}$. But $S = \bigcap \mathcal{R}$, so Exercise 37 ensures us that $S \subseteq T$, as desired.

All of this proves that S indeed is a transitive closure of R. ■

Before inspecting other relational properties, let us first take a moment to conceive some transitive closures.

45 Example

Let X be the set $\{1, \ldots, 8\}$ and consider the relation R defined as

$$R = \{\, \langle 1, 2 \rangle, \langle 2, 4 \rangle, \langle 5, 6 \rangle, \langle 6, 7 \rangle, \langle 6, 8 \rangle, \langle 7, 3 \rangle \}.$$

This relation and its transitive closure S are illustrated in Fig. 2.3. In finite cases such as this, one can compute the transitive closure by simply checking which pairs need to be added.

Because $1 \; R \; 2 \; R \; 4$ we know $1 \; S \; 4$ must hold, likewise $5 \; R \; 6 \; R \; 7$ and $5 \; R \; 6 \; R \; 8$ we know that $5 \; S \; 7$ and $5 \; S \; 8$. Do note that $5 \; S \; 3$ also has to hold, because $5 \; S \; 7$ and $7 \; R \; 3$.

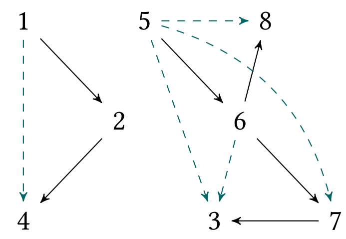

Figure 2.3: Example of a relation on $\{1, \ldots 8\}$ and its transitive closure.

46 Example (Successor)
Consider the relation R on $\mathbb{N}$ defined as

$$R = \{ \langle n, m \rangle \in \mathbb{N} \times \mathbb{N} \mid \mathrm{m = n + 1} \} .$$

This relation is not transitive at all, for $0 \ R \ 1$ and $1 \ R \ 2$, but $0 \ R \ 2$ is not the case. The relation $<$ on $\mathbb{N}$ is a relation which extends R. We also know it to transitive, as mentioned in Example 42.

One can reason that $<$ is in fact the transitive closure of R. To prove this, take some transitive relation T extending R. Assume that $n < m$ holds. It follows that $m = n + k$ for some positive number $k \in \mathbb{N}$. Note that $m \ R \ (m+1) \ R \ (m+2) \ R \ \ldots \ R \ (m+k) = n$. Because $R \subseteq T$ we now also know that $m \ T \ (m+1) \ T \ (m+2) \ T \ \ldots \ T \ n$. Transitivity ensures that $m \ T \ m+1$ and $(m+1) \ T \ (m+2)$ entail $m \ T \ m+2$. Proceeding in this fashion we see that $m \ T \ (m+k) = n$, which is exactly what we set out to prove.

47 Example
Let R be a transitive relation on some set X. Now R is a transitive closure of itself! It is easy to see that R is transitive, and $R \subseteq R$ surely holds. Moreover, if T is transitive and such that $R \subseteq T$, then $R \subseteq T$ surely holds. This proves that the transitive closure of any transitive relation is the original transitive relation.

Can you imagine several transitive closures? One would hope not, for there can only be one! This too we can prove. Note that this proof uses only Definition 10, the definition of a transitive closure. There is no deep mathematics involved, one simply uses the structure provided.

11 Lemma
Let R be a relation on X, and let S_1 and S_2 both be transitive closures of R. Then $S_1 = S_2$.

Proof. We will prove that $S_1 \subseteq S_2$, the other inclusion can be proven via a symmetric argument. These two inclusions together yield the desires equality.

Note that S_2 is a transitive relation extending R by definition. Indeed, these are (ii) and (i) respectively of Definition 10 reading S_2 for S. Now read (iii) of the same definition with S_1 for S and S_2 for T. This says that is S_2 were a transitive relation on X such that $R \subseteq S_2$, then $S_1 \subseteq S_2$. We just proved these two assumptions, so the conclusion follows readily. This finishes the argument. ∎

The following definition might seem a bit strange, but intuitively it says “if two things relate to the same thing, they must relate to one another”. This intuition taken to its logical conclusion is unfortunately not fully accurate, but in the presence of reflexivity it is, as explicated in Exercise 63. The same exercise also asks you to prove that a relation is euclidian whenever it is both symmetric and transitive.

11 Definition (Euclidian)
A relation R on X is said to be euclidian if for all $a, b, c \in X$ we have $b \; R \; c$ whenever $a \; R \; b$ and $a \; R \; c$.

48 Example
Consider the real plane $\mathbb{R}^2$, and say that $p \; R \; q$ holds for $p, q \in \mathbb{R}^2$ if and only if p and q lie on the same circle through the origin. This for instance means that $\langle \sqrt{2}, 0 \rangle \; R \; \langle 1, 1 \rangle$, but $\langle 1, 1 \rangle \; R \; \langle 1, 0 \rangle$ does not hold. Suppose we have points $a, b, c \in \mathbb{R}^2$ and we know that both $a \; R \; b$ and $a \; R \; c$ hold. Is it the case that $b \; R \; c$? Well, a and b lie on the same circle around the origin, and a and c do too. This means that b and c must lie on the same circle around the origin as well, so $b \; R \; c$. The relation R thus is an example of an Euclidian relation.

49 Example (Points on the Circle)
Consider the unit circle $S \subseteq \mathbb{R}^2$ defined by

$$S = \left\{ \langle x, y \rangle \in \mathbb{R}^2 \;\middle|\; x^2 + y^2 = 1 \right\}.$$

We define the relation R on S such that $p \; R \; q$ if and only if there is a straight line between p and q through the origin. From this mental picture one can infer that R is in fact euclidian. Do try to formally prove this!

50 Example
The above two examples are both reflexive, symmetric and transitive. Can one find examples of euclidian relations that are neither? Well, yes, see the relation in Fig. 2.4. It takes some work to verity

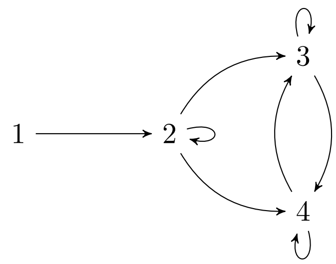

Figure 2.4: Example of an Euclidian relation which is neither symmetric, reflexive nor transitive.

that it is indeed euclidian. To see that it is not reflexive is considerably easier, for $1 \; R \; 1$ is missing. Symmetry also is lacking, because $1 \; R \; 2$ but $2 \; R \; 1$ does not hold. Transitivity is absent because $1 \; R \; 2$ and $2 \; R \; 3$ but $1 \; R \; 3$ does not hold.

12 Definition (Dense)
A relation R on X is said to be dense when for each $a, c \in X$ we have that when $a \; R \; c$, there exists a $b \in X$ such that $a \; R \; b$ and $b \; R \; c$.

51 Example
The relation $<$ on the rational numbers is dense. Suppose that $a < c$ is given, then a lies somewhere strictly below c on the number line. The midpoint between a and c will serve as the "b" from Definition 12. See that this midpoint is given by $\frac{1}{2} \cdot (a + c)$, and this number is rational is a and c are. It is also true that $a < a + \frac{1}{2}(c - a) = b$, and for similar reasons $b < c$. This proves the relation $<$ to be dense.

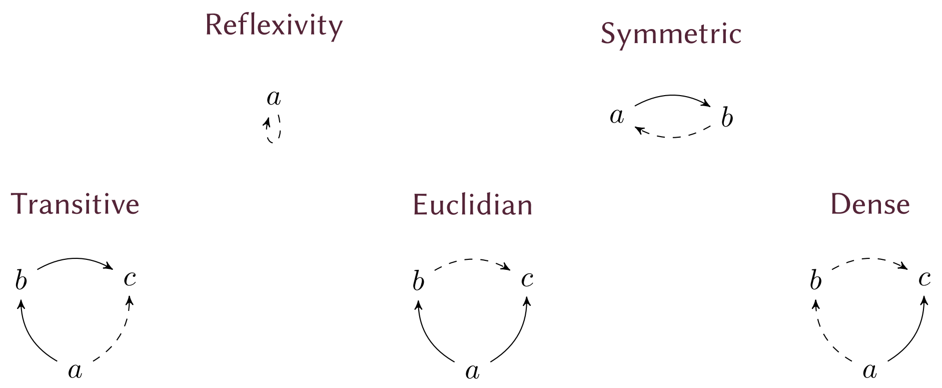

Figure 2.5: Graphical depictions of relational properties.

52 Example
The relation $<$ on natural numbers is not dense. A counterexample can be readily found, for instance $0 < 1$ but there is no natural number n such that $0 < n$ and $n < 1$.

53 Example (Reflexive relations are Dense)
Any reflexive relation is dense. For suppose that R is reflexive on X, and let $a, c \in X$ be such that $a \ R \ c$. By reflexivity we know $a \ R \ a$, and we assumed $a \ R \ c$, so a can serve as the "midpoint b" of Definition 12. This makes R a dense relation.

We now have seen several definitions of important properties of relations. Beforehand we noted that one has to be careful to state precisely which set the given relation is supposed to "be on". In the definition of reflexivity this immediately shines through, because enlarging the context destroys reflexivity. A more precise version of this statement is given in Exercise 64.

The definitions of a symmetric, transitive and euclidian relations depend much less on context. Indeed, if R is a relation on X and Y is any set, then R has any of the above properties on X if and only if it has these properties on $X \cup Y$.[1] The definition of density again depends a lot on context, but in a different way than reflexivity. This is illustrated by Example 52 and Example 51

In Example 37 we observed that the relation of begin less-than is not symmetric. Stronger even, it is so far from symmetry that a symmetric situation entails actual equality. This sounds somewhat vague, but the following definition should clear that up well enough. Do keep a relation like $\leq$ in mind when thinking of anti-symmetry.

13 Definition (Anti-Symmetric)
A relation R on X is said to be anti-symmetric when for each $a, b \in X$ we have that $a \ R \ b$ and $b \ R \ a$ entail $a = b$.

Recall Example 37, where we reasoned that $\leq$ is not symmetric from its anti-symmetry. This is a general fact, and let us state it as such. In Exercise 62 you are asked to prove some facts about relations that are both symmetric and anti-symmetric.

12 Lemma
Let R be a relation on a set X. Suppose that there exist $a, b \in X$ such that $a \ R \ b$ and $a \neq b$. If R is anti-symmetric, then X is not symmetric.

[1]That these enlargements make sense at all follows from Exercise 42.

Proof. We reason by contradiction, so assume that R is symmetric. Then from $a \; R \; b$ we may derive $b \; R \; a$. Anti-symmetry now ensures that $a = b$, but we know $a \neq b$, a contradiction. This proves the desired. ■

One may wonder whether the converse also holds, that is, in the above setting, does non-symmetry entail antisymmetry. This is not the case.

54 Example
Consider the relation R on the set $\{0, 1, 2\}$ as depicted in Fig. 2.6. It surely is not symmetric, because $3 \; R \; 1$ but $3 \; R \; 1$ does hold. But neither is it anti-symmetric, because $1 \; R \; 2$ and $2 \; R \; 1$ but $2 \neq 1$.

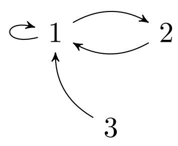

Figure 2.6: Example of a relation which is not symmetric, but not anti-symmetric either.

55 Example
There even is a relation which is both symmetric and anti-symmetric! The relation id_A of actual equality on a set A, as already discussed in Example 44, is surely symmetric. But if $x = y$ and $y = x$ then $x = y$ follows, so id_A is anti-symmetric too. We continue along this vein in Exercise 62.

56 Example
The relation $\subseteq$ on $\mathcal{P}(X)$ of Example 29 for any set X is anti-symmetric. This is an immediate consequence of Lemma 3.

57 Example (Divisibility Once More)
Recall the relation $\mid$ from Example 34 and 40. This relation is also anti-symmetric, and this we can prove. Suppose that $n \mid m$ and $m \mid n$. This means that there are k and l such that $n \cdot k = m$ and $m \cdot l = n$. Substituting these equalities into one another we obtain $(m \cdot l) \cdot k = m$. Dividing both sides by m yields $l \cdot k = 1$, from which we can derive that $l = 1 = k$. As a consequence, $n \cdot l = n \cdot 1 = n = m$. This proves $n = m$ as desired, so $\mid$ is anti-symmetric.

One can think of a relation R on some set X as a way of comparing elements in X. In this light it makes sense to specify those relations in which all elements of R can be compared to each other in some way. The following definition captures this.

14 Definition (Weakly Connected)
A relation R on a set X is said to be weakly connected when for each pair of elements $a, b \in X$ we have $a = b$, $a \; R \; b$ or $b \; R \; a$.

58 Example
The relations $<$ and $\leq$ on any of the common sets are weakly connected.

59 Example (Some More Lines in the Plane)
Recall the relation R on $\mathbb{L}$ from Example 24 and 36. In the latter example we say two parallel lines. It is clear that these two lines are neither equal, nor intersecting in any way. This means that these lines are not comparable, whence R is not a weakly connected relation.

60 Example (Containing)
Consider the real plane $\mathbb{R}^2$, and define a relation as follows:

$$R = \left\{ \langle p, q \rangle \in \mathbb{R}^2 \times \mathbb{R}^2 \;\middle|\; \text{the point } p \text{ is further away from the origin than } q \right\}.$$

This sounds slightly vague, but isn't really. A point p is further away from the origin than q precisely when the C circle whose origin is at the origin of the plane and which passes through p encompasses the point q.

The previous gives a nice geometric interpretation to "further away". Amore algebraic (or Cartesian) approach would be to say that a point p is actually a pair of coordinates, say $p = \langle x, y \rangle$ (this we know already, which is why we write $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$ for the plane). Now the distance between the origin and p is determined by Pythagoras' theorem, which equals it to $\sqrt{x^2 + y^2}$. With this machinery at hand, $p \; R \; q$ holds precisely if the distance of p to the origin is greater than the distance of q to the origin.

With all these different interpretations of R we are ready to check some of its properties. Reflexivity it certainly lacks, because nothing is further away than itself. It is not symmetric, but it is transitive. It also is well-connected. Indeed, consider two points p and q. Now simply draw the appropriate circles, and the one must be contained within the other, or the circles are equal. This shows that R is weakly connected.

The following property of relations makes sense even when the relation is a relation between two sets, instead of a relation on one given set. Intuitively, it says that to each element on the left-hand set there is something in the right-hand set which relates to it.

15 Definition (Serial)
A relation R between A and B is said to be serial when for each $a \in A$ there is a $b \in B$ such that $a \; R \; b$.

61 Example
Consider the relation defined below between $\mathbb{N}$ and $\mathbb{R}$.

$$R = \left\{ \langle x, y \rangle \in \mathbb{N} \times \mathbb{R} \;\middle|\; x = y^2 \right\}$$

For example, see that $4 \; R \; 2$ and $4 \; R \; {-2}$. This relation is serial, and we can prove it to be so. Let $x \in \mathbb{N}$ be any natural number, it is our task to find a value $y \in \mathbb{R}$ such that $x \; R \; y$. This is not tremendously hard, the number $y = \sqrt{x}$ does the job. In fact, $-\sqrt{x}$ works as well.

62 Example
The relation R as defined below between $\mathbb{N}$ and $\mathbb{N}$ is not serial.

$$n \; R \; m \text{ if and only if } n = m^2$$

Indeed, we have $2 \in \mathbb{N}$ but if $2 \; R \; m$ for some $m \in \mathbb{N}$ then $2 = m^2$ would follow. We know that $x^2 \leq y^2$ if $x \leq y$, so we know that $m \leq 2$ must hold. But it is easy to see that $0^2 = 0 \neq 2$, $1^2 = 1 \neq 2$ and $2^2 = 4 \neq 2$, a contradiction. This proves that R is not serial.

63 Example (Reflexive relations are Serial)
Suppose that R is some relation on X, and assume that R is reflexive. Then R is serial too. Indeed, for any $a \in X$ we know have some $b \in X$ such that $a \; R \; b$, namely $b = a$.

This property too makes sense for relations between two sets. Basically, it states that to each item on the left there can be at most one item on the right in relation to it. Compare this to seriality, which states that to each item on the left there is at least one item on the right in relation to it.

16 Definition (Determinacy)
A relation R between X and Y is said to be deterministic when if $x\ R\ a$ and $x\ R\ b$ holds for $x \in X$ and $a, b \in Y$, then $a = b$.

64 Example (Identity)
Recall that we write id_X for the identity relation on a set X, as described in Example 44. This relation is quite deterministic. For suppose that $x, a, b \in X$ are such that $x\ \mathrm{id}_X\ a$ and $x\ \mathrm{id}_X\ b$. Then, by the very definition of id_X, we know $x = a$ and $x = b$. As equality is euclidian this proves $a = b$, so id_X is deterministic.

65 Example
In Example 48 we had a relation R on the real plane, where points are related if and only if they lie on the same circle around the origin. This relation is not deterministic at all. Indeed, consider the points $\langle 1, 0 \rangle$, $\langle 0, 1 \rangle$ and $\langle -1, 0 \rangle$. One can verify that $\langle 0, 1 \rangle\ R\ \langle 1, 0 \rangle$ and $\langle 0, 1 \rangle\ R\ \langle -1, 0 \rangle$. We do know that $\langle 1, 0 \rangle\ R\ \langle -1, 0 \rangle$, but $\langle 1, 0 \rangle = \langle -1, 0 \rangle$ most certainly does not hold. This shows that R is not deterministic.

66 Example
The relation R from Example 46 on the set of natural numbers, which related each natural number n to its successor $n + 1$ is deterministic. For suppose that $x\ R\ a$ and $x\ R\ b$, then by definition we know that $a = x + 1 = b$, so again $a = b$ follows.

67 Example
We construct a relation S, similar to the relation R of Example 66 and 46. Define the relation S on $\mathbb{N}$ as follows:

$$S = \left\{ \langle n, m \rangle \in \mathbb{N} \times \mathbb{N} \;\middle|\; n = m + 1 \right\}.$$

Suppose that $x\ S\ a$ and $x\ S\ b$. By definition it follows that $x = a + 1$ and $x = b + 1$. Consequently we can derive that $a = b$, so this relation certainly is deterministic.

It is, however, not a serial relation. There is nothing "following" the number zero. For suppose that $a \in \mathbb{N}$ is such that $0\ S\ a$, then $0 = a + 1$, which could not possibly be.

Now that we know of several important properties of relations, we can group some of these together.

17 Definition (Orders)
A relation is said to be a partial order when it is both reflexive, transitive and anti-symmetric. It is called a total linear order when additionally, it is weakly connected.

68 Example (Intuitive Orders are Linear Orders)
The relation $\leq$ is a total linear order, when seen as a relation on any of the common sets. Indeed, reflexivity, transitivity, anti-symmetry and weakly-connectedness were discussed in Example 30, 42, 37 and Example 58 respectively. For reasons of symmetry, $\geq$ is a total linear order too.

69 Example
The relation $<$ is not a total linear order, because it is not reflexive. It does satisfy all the other properties.

70 Example (Divisibility as a Partial Order)
The relation $|$ is a partial order. The appropriate properties have been shown to hold in respectively Example 34, Exercise 50 and Example 57.

71 Example (Subsets as Partial Order)
For any set X, the relation $\subseteq$ on $\mathcal{P}(X)$ is a partial order. Reflexivity and anti-symmetry respectively were shown in Example 29 and 56. In Exercise 49 you will be asked to prove transitivity.

2.4 Equivalence relations

The relation of actual equality has several interesting properties, as pointed out in Example 44. There are several other relations which share this property, for instance, the relation R of Example 32. Let us first define the properties we are after.

18 Definition (Equivalence Relation)
A relation R on a set X is said to be an equivalence relation whenever it is reflexive, transitive and symmetric. On occasions, we will write $\equiv$ to refer to an equivalence relation.

72 Example (Largest Equivalence Relation)
Given any set X, the relation $R = X \times X$ is an equivalence relation. This is true by virtue of the relation R being "as lax as possible", anything is related to anything. Check for yourself that the relation R indeed is an equivalence relation.

73 Example (Birthday)
Let X be the set of all people currently alive on earth, and let R be the relation defined by

$$R = \{ \langle p, q \rangle \mid p \text{ and } q \text{ are people with the same birthday} \} .$$

This relation is in fact an equivalence relation.

74 Example (Smallest Equivalence Relation)
The relation of equality is the smallest equivalence relation on any set X. Indeed, in Example 44 we already discussed that id_X is an equivalence relation. Moreover, if R is any equivalence relation, then R must be reflexive. That means that $=$, when seen as a relation, must be a subset of R. This makes R in some sense "at least as large" as id_X.

75 Example
Consider the integers $\mathbb{Z}$ and define the following relation on it

$$\equiv = \left\{ \langle n, m \rangle \,\middle|\, 3 \mid n - m \right\} . \tag{2.1}$$

Note that $n \equiv n$ because $3 \mid 0 = n - n$, so $\equiv$ is reflexive. This in stark contrast with the relation R_3 of Example 35, where we worked with a slightly similar relation with $+$ in the place of $-$ of the defining equality above. It was exactly this $+$ which broke the above argument, and which made reflexivity unobtainable. Do try to figure out why the argument did work in Example 32.

Moreover, $\equiv$ is symmetric. To prove this, assume that $n \equiv m$. We derive that $3 \cdot k = n - m$ for some $k \in \mathbb{Z}$. This leads to $3 \cdot (-k) = -1 \cdot 3 \cdot k = m - n$, so $m \equiv n$ also holds.

The relation $\equiv$ is transitive as well. For suppose that $n \equiv m$ and $m \equiv k$, then we know of numbers a and b such that $a \cdot 3 = (n - m)$ and $b \cdot 3 = (m - k)$. Adding these equalities to one another we obtain

$$(a + b) \cdot 3 = a \cdot 3 + b \cdot 3 = (n - m) + (m - k) = n - k,$$

which proves that $3 \mid (n-k)$, so $n \equiv k$.

Now let us look a bit at the structure of $\equiv$. We know that $0 \equiv 3$, and in fact, $3 \cdot n \equiv 3 \cdot m$ because $3 \cdot (n-m) = 3n - 3m$. Now $1 \equiv 4 \equiv 7 \equiv \ldots$ and $2 \equiv 5 \equiv 8 \equiv \ldots$ both holds. Furthermore, $0 \not\equiv 1$. Indeed, if $1 \equiv 0$ then $3 \mid 1 = (1-0)$, but 3 certainly is no divisor of 1. From this it also follows that $4 \not\equiv 0$, because $4 \equiv 1$ and so this would lead to $1 \equiv 0$, which we know not to be the case.

We thus see that $\equiv$ partitions the set $\mathbb{Z}$ into three parts, namely

$$\begin{array}{rcl} \{\ldots,-6,-3,0,3,6,\ldots\} & = & \{\, 3n \mid n \in \mathbb{Z}\}\,, \\ \{\ldots,-5,-2,1,4,7,\ldots\} & = & \{\, 3n+1 \mid n \in \mathbb{Z}\}\,, \\ \{\ldots,-4,-1,2,5,8,\ldots\} & = & \{\, 3n+2 \mid n \in \mathbb{Z}\}\,. \end{array}$$

76 Example

There is nothing special about 3 in (75). In fact, we can replace it with any integer we like. Define $n \equiv_k m$ for $n, m \in \mathbb{Z}$ to hold exactly if $k \mid (n-m)$. One can repeat all the argument in Example 75 more-or-less verbatim to prove that $\equiv_k$ is an equivalence relation.

77 Example (Logically Equivalent Formulae)

Consider the set $\mathcal{L}_{\mathsf{PROP}}$ and the relation from Example 23, let us call it $\equiv$. This relation is in fact an equivalence relation. To prove that this is true knowledge of propositional logic would come in handy. We omit the proof here, but do try this at home! This illustrates that the relation of "logical equivalence" on propositional formulae is an equivalence relation, giving additional credence to the nomenclature in use.

78 Example

Consider the set $X = \{\, \langle\, n, m \,\rangle \in \mathbb{Z} \times \mathbb{Z} \mid m \neq 0\}$ and the relation $\equiv$ on such pairs, defined as follows:

$$\langle\, a, b \,\rangle \equiv \langle\, c, d \,\rangle \quad \text{if and only if} \quad a \cdot d = c \cdot b.$$

For example, $\langle\, 1, 1 \,\rangle \equiv \langle\, -1, -1 \,\rangle$ and $\langle\, 3, 6 \,\rangle \equiv \langle\, 1, 2 \,\rangle$. Is it justified to use the symbol $\equiv$ for this relation, that is, is this a bona fide equivalence relation? It most certainly is, and we can quite readily prove this.

The relation is reflexive, because $\langle\, a, b \,\rangle \equiv \langle\, a, b \,\rangle$ has to hold as $a \cdot b = a \cdot b$. The relation is symmetric as well, as one can plainly read from the equalities involved.

Transitivity is a bit more work, but not significantly more difficult to grasp. Suppose that $\langle\, a, b \,\rangle \equiv \langle\, c, d \,\rangle$ and $\langle\, c, d \,\rangle \equiv \langle\, e, f \,\rangle$, for pairs from the set X. This means that $a \cdot d = c \cdot b$ and $c \cdot f = e \cdot d$. Multiply the left-hand side equation by f and the right-hand side equation by b, and see that we get the following equality.

$$a \cdot d \cdot f = c \cdot b \cdot f = c \cdot f \cdot b = e \cdot d \cdot b$$

Now as $\langle\, c, d \,\rangle \in X$ we know $d \neq 0$, so we can divide everything above by d. This results in $a \cdot f = e \cdot b$, proving $\langle\, a, b \,\rangle \equiv \langle\, e, f \,\rangle$.

79 Example (Parallel Lines)

Consider again the set X for Example 78. Each pair $\langle\, a, b \,\rangle \in X$ determines a line. For instance, the pair $\langle\, 3, 2 \,\rangle$ determines the line which intersects the y-axis at 2 and the x-axis at 3, as illustrated in Fig. 2.7.

This line in turn determines a triangle. There is an angle between the line an the x-axis, denote this $\angle\langle\, a, b \,\rangle$. Recall from trigonometry that this angle is the tangent of the opposite side (a) divides by the adjacent side (b). In summary, $\angle\langle\, a, b \,\rangle = \tan \frac{a}{b}$.

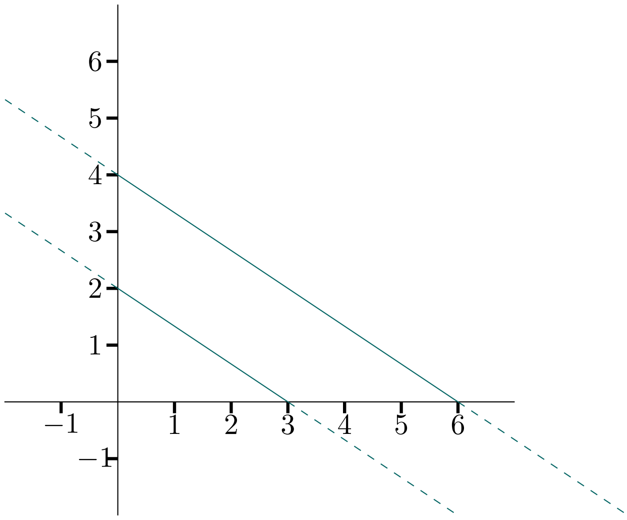

Figure 2.7: Lines in the real plane with integer intersection points.

One can see that two parallel lines, as shown in Fig. 2.7, yield the same angle. In fact, parallel lines yield the same fraction. So there are several ways to look at the equivalence of Example 78:

(i) pairs that yield the same ratio are equivalent;

(ii) pairs that yield the same angle are equivalent;

(iii) pairs that yield parallel lines are equivalent.

Alternatively we could have defined an equivalence relation as a reflexive euclidian relation, as you are asked to prove in Exercise 63. Equivalence relations are used in settings where we have a notion of "sameness" and want to treat all elements of a set that are the "same" as identical. The rationals numbers are an example: although given by different expressions, the numbers $\frac{2}{7}$ and $\frac{4}{14}$ are considered to be "the same", as are -1 and $\frac{-9}{9}$, and so on. We first discuss equivalence relations in general, and then return to $\mathbb{Q}$.

Equivalence relations give rise to a partition of a set, much like in Example 75. Let us grasp this in a formal way. To this end we first need to define what we understand a partition to be.

19 Definition (Partition)
A partition on a set X is a subset $P \subseteq \mathcal{P}(X)$ such that the following three properties hold:

(i) the empty set is not an element of P;

(ii) the set X is covered by P, that is, $\bigcup P = X$;

(iii) the elements of P are pairwise disjoint, that is, if $A, B \in P$ and $A \neq B$ then $A \cap B = \emptyset$.

Before we consider examples, let us first prove a nice property of partitions. This property basically says that the partition actually partitions the set it is a partition of. That is to say, each element of the partitioned set belongs to one and only one element of the partition. We will use this property later on to relate partitions and equivalence relations in Lemma 16.

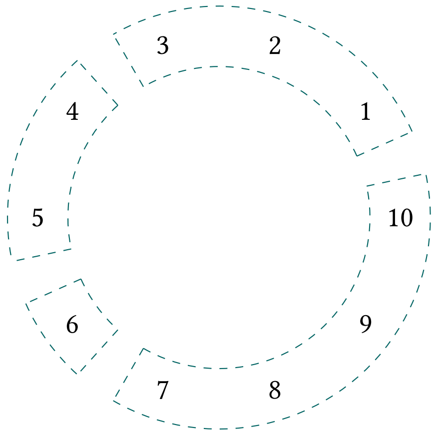

Figure 2.8: Example of a partition of the set $\{1, 2, \ldots, 10\}$.

13 Lemma

Let P be a partition on X. To each $a \in X$ there is a unique $p \in P$ such that $a \in p$.

Proof. Consider an element $a \in X$. By (ii) of Definition 19 we know that $\bigcup P = X$, so the definition of $\bigcup$ ensures us the existence of a $p \in P$ such that $a \in p$.

Now suppose p and q are both elements of P such that $a \in p$ and $a \in q$. We need to prove that $p = q$. Assume the contrary, so $p \neq q$. By (iii) of Definition 19 we now know that $p \cap q = \emptyset$. But surely $a \in p \cap q$, a blatant contradiction whence the desired follows. ■

80 Example

An example of a partition of the numbers 1 through 10 is given in Fig. 2.8. Formally, the partition depicted there equals the set

$$\left\{ \{1, 2, 3\}, \{4, 5\}, \{6\}, \{7, 8, 9, 10\} \right\}.$$

One can verify that all conditions of Definition 19 indeed are met.

81 Example

Is there a partition of the empty set $\emptyset$? Ponder this for a moment.

82 Example

In Fig. 2.9 we graphically depict a partition of $\mathbb{Z}$ into two sets

$$\big\{\{-1, 1, 3, -3, 5, -5, \ldots\}, \{0, 2, -2, 4, -4, 6, -6, \ldots\}\big\}.$$

Indeed, this partitions the integers into the odd and even numbers.

83 Example (Wrapping the Non-Negative Real Line)

Imagine a cylinder with a circumference of length 1. For the numerically included, this means that the radius of this cylinder is $\frac{1}{2\pi}$. Now picture the non-negative real line $\mathbb{R}_{\geq 0}$, and attach it to the cylinder at some point. Imagine rolling the cylinder, winding the non-negative real line around it.

$$\boxed{\cdots \quad -5 \quad 5 \quad -3 \quad 3 \quad -1 \quad 1} \quad \boxed{0 \quad 2 \quad -2 \quad 4 \quad -4 \quad 6 \quad -6 \quad \cdots}$$

Figure 2.9: Example of a partition of the set $\mathbb{Z}$.

As the real line has no width or height (only length), you see that the point 1 falls directly atop 0. Keep wrapping, and see that 2 falls on 1, et cetera. This process is illustrated in Fig. 2.10.

When you look from the center of the cylinder towards the real line you wrapped around it, you see somethings like this. First you see a real number, r say. Then you see $r+1$, and then $r+2$, going on indefinately. Each angle you can take gives another such sequence. This yields the following partition of the real numbers:

$$\left\{ \, \{ r+n \mid n \in \mathbb{N} \} \, \middle| \, r \in \mathbb{R}_{\geq 0} \right\}.$$

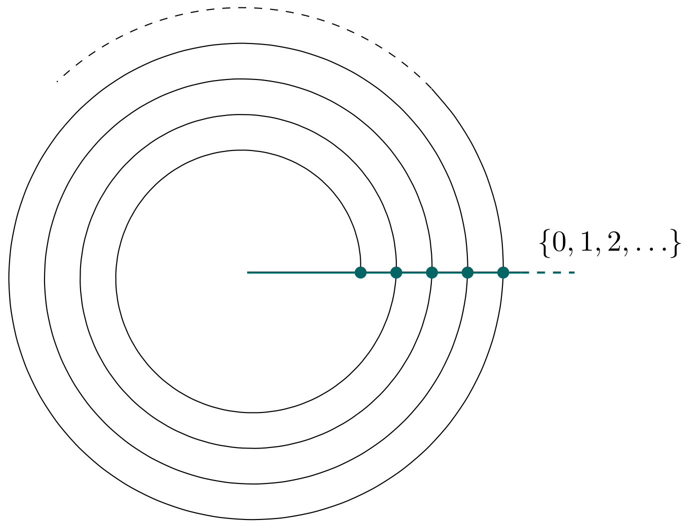

Figure 2.10: The non-negative real line wrapped around a cylinder with unit circumference.

84 Example (Folding the Real Line)
This time, imagine the entire real line. Pick some particular point of it, the point r say. Now fold the real line onto itself from the left to the right pivoting around the point r. This leaves you with a line stretching for ever onward towards the right.

On the far left you have but one point, the point r. Moving x further to the right you see two points atop one another, the points $r+x$ and $r-x$. See Fig. 2.11 for a sketch of this.

Given an equivalence relation $\equiv$ on a set X we can consider the equivalence class of any element $a \in X$ under $\equiv$. This equivalence class is the set

$$\{ x \in X \mid a \equiv x \},$$

and a is said to be a representative of this equivalence class. We will often write $[a]$ for this set, or when we want to emphasize that this set arises from the relation $\equiv$ we write $a/\equiv$. This equivalence class has

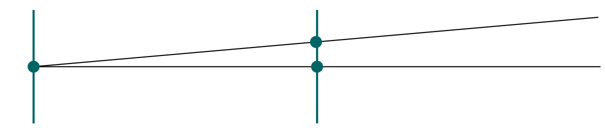

Figure 2.11: The real line folded onto itself.

several nice properties. First of all, $[a]$ is never empty. This we can easily prove, because for any $a \in X$ we have $a \equiv a$, so $a \in [a]$. Secondly, when two equivalence classes coincide, (that is to say, have a non-empty intersection), exactly when the representatives are equivalent.

14 Lemma
Let $\equiv$ be an equivalence relation on a set X and let a and b be any two elements from X. The following three items are logically equivalent:

(i) $a \equiv b$;

(ii) $[a] = [b]$;

(iii) $[a] \cap [b]$ is non-empty;

Proof. We will show that each item entails the following item, and the last item entails the first. This forms a chain of implications, making all items logically equivalent.

First suppose that (i) holds. It suffices to show that $[a] \subseteq [b]$, because if this holds, then by symmetry we also have the converse inclusion. These inclusions together entail (ii), as was shown in Lemma 3. Now let $x \in a/$ be arbitrary, we wish to prove that $x \in b/$. We know that $a \equiv x$, and $a \equiv b$. Symmetry, transitivity and symmetry again now yield $b \equiv x$, proving the desired.

Suppose that (ii) holds. Because $a \in [a]$ we know it to be non-empty, so (iii) follows immediately.

Finally, suppose that (iii) holds. This gives us some c in this intersection. By definition we now know that $c \equiv a$ and $c \equiv b$. Because $\equiv$ is an equivalence relation we know it to be euclidian as well, so $a \equiv b$ follows. This proves (i), which completes the chain. ■

Armed with the above lemma, we can prove that each equivalence relation gives rise to a partition. This construction is very important, and you will see it quite often.

20 Definition
Let X be a set and $\equiv$ an equivalence relation on X. Define the set $X/\!\equiv$ as follows:

$$X/\!\equiv \; = \{\, a/\equiv \mid a \in X \,\}\,.$$

15 Lemma
Let $\equiv$ be an equivalence relation on X. Now $X/\!\equiv$ is a partition.

Proof. It is up to us to prove that the three properties of Definition 19. We proceed in order, and show them all to be true.

First we prove (i). Assume that $\emptyset \in X/\!\equiv$. This means that $\emptyset = [a]$ for some $a \in X$. But we know that $a \in [a]$ by reflexivity, so $a \in \emptyset$, which is utter nonsense. This proves (i).

Now on to the next item. By the above paragraph we know that $a \in a/$, so $\bigcup X/\equiv$ will contain X. Naturally, $[a] \subseteq X$, so the converse inclusion holds as well. This proves that $\bigcup X/\equiv \;=\; X$, so (ii) holds.

The final item requires a bit more work, but the bulk is already done. To show that (iii) holds, we have to prove that when $[a] \neq [b]$ then $[a]$ and $[b]$ have an empty intersection. But this follows from Lemma 14, so we are done. ■

In Example 75 we already saw an equivalence of a relation and the induced partition. Let us look at some more examples.

85 Example (Singleton Partitions)
Recall the trivial equivalence relation $R = X \times X$ on X from Example 72. What does the set X/R look like? It is a singleton! Indeed, for any $a \in X$ we have $a/R = X$. This means that the set X/R equals $\{X\}$, so it is a singleton.

We do have to be a bit careful here. What happens in the case that X is the empty set? Then a/R does not contain any elements, so it is the empty set as well. So in the above paragraph we actually proved that were X non-empty, then X/R would be a singleton.

We can wonder when the converse holds, that is to say, for which equivalence relations R on a non-empty set X is it the case that X/R is a singleton. This is left to you as Exercise 80.

86 Example
Recall Example 32, 76 and 82. Consider the relation $\equiv$ on $\mathbb{Z}$ where $n \equiv m$ if and only if $n - m$ is even. Do check that this number is even precisely if $n + m$ is even!

Note that the equivalence relation $\equiv$ gives rise to a partition $\mathbb{Z}/\equiv$ of $\mathbb{Z}$. This partition is exactly the partition as depicted in Fig. 2.9 and described in Example 82.

87 Example (Clocks)
Recall the relation from Example 76 with k set to twelve. For convenience, simply write $\equiv$ for $\equiv_{12}$. An equivalence class of a number contains that number, and any other number which differs a multiple of twelve from the original number. In this way, one can think of $\mathbb{Z}/\equiv$ as "integers up to multiples of 12".

There is a very natural interpretation of this which many of us come into contact with every day, that is, the numbers on a clock. See Fig. 2.12 for a sketch.

88 Example (Logically Equivalent Formulae)
Consider the set $\mathcal{L}_{\mathsf{PROP}}$ and the relation from Example 77 and 23. The set $\mathcal{L}_{\mathsf{PROP}}/\equiv$ is the partition of propositional formulae into sets of logically equivalent formulae.

89 Example (The Rational Numbers)
The rational numbers $\mathbb{Q}$ can be represented in an elegant way using the equivalence relation $\equiv$ from Example 78. A rational $\frac{n}{m}$ can be represented as the pair $\langle n, m \rangle$ from X. One can verify that when $\frac{a}{b} = \frac{c}{d}$, then $\langle a, b \rangle \equiv \langle c, d \rangle$. The converse also holds, so rationals can be coded as the partition of X into equivalence classes $X/\equiv$.

We could do even better by replacing X by the set $\mathbb{Z} \times \mathbb{N}_{>0}$. This is left as Exercise 86.

We know that each equivalence relation yields a partition, but is the converse true as well? It most certainly is.

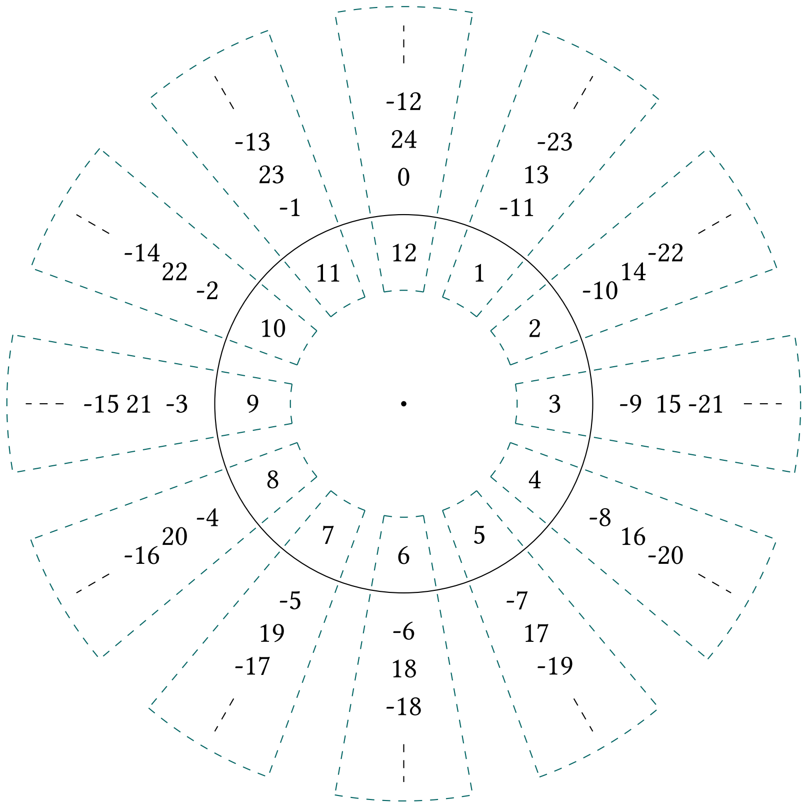

Figure 2.12: Partition of the integers up to multiples of 12, or rather, a clock.

16 Lemma

Let X be any set and let P be a partition on X. Define the relation R on X by $a\ R\ b$ if and only if there is an $p \in P$ such that $a \in p$ and $b \in p$. Now R is an equivalence relation. Furthermore, when $P = X/S$ for some equivalence relation S, then $R = S$.

Proof. We need to check that R indeed is an equivalence relation. Reflexivity follows immediately from Lemma 13. Symmetry is immediate from the definition.

To check transitivity, suppose that $a\ R\ b$ and $a\ R\ c$. This yields $p, q \in P$ such that $a, b \in p$ and $a, c \in q$. But now $b \in p \cap q$, so $p = q$ must follow from the pairwise disjointness of the elements of P. As a consequence we know that both a and c are elements of p, which proves $a\ R\ c$.

To prove the final statement, fix some equivalence relation S such that $P = X/S$. We need to prove that $R \subseteq S$ and $S \subseteq R$.

Let us first prove the inclusion of R into S. To this end, assume $a\ R\ b$. We know that $a \in [a]$, so Lemma 13 ensures that $b \in [a]$. By Lemma 14 we now know that $a\ S\ b$.

The other inclusion goes like this. If $a\ S\ b$ then Lemma 14 ensures us that $a, b \in [a]$, whence $a\ R\ b$ must follow. This finishes our argument. ∎

90 Example

Recall the partition from Example 83, which was given as

$$P = \left\{ \left\{ r + n \;\middle|\; n \in \mathbb{N} \right\} \;\middle|\; r \in \mathbb{R}_{\geq 0} \right\}.$$

This partition induces an equivalence relation $\equiv$ as per Lemma 16. Can we describe this equivalence relation in a nice way? Sure we can! For all $x, y \in \mathbb{R}_{\geq 0}$ we have $x \equiv y$ if and only if $x - y$ is an integer. Let us prove this claim.

First, if x and y from $\mathbb{R}_{\geq 0}$ are such that $x - y = k$ for some $k \in \mathbb{Z}$ we can distinguish two cases. On the one hand k may be positive. In this case y is smaller than x, and $x = (x - y) + y = y + k$ But this means that $x \in \{ y + n \mid n \in \mathbb{N}\}$, so $x \equiv y$ follows. On the other hand, k may be negative. In this case x is smaller than y and $y = x - (x - y) = y - k = y + (-k)$. This again shows that $y \equiv x$, as desired.

To prove the converse, assume that $x \equiv y$. This means that $x, y \in \{ r + n \mid n \in \mathbb{N}\}$ for some $r \in \mathbb{R}_{\geq 0}$. As a consequence we know of natural numbers k and l such that $x = r + k$ and $y = r + l$ respectively. We can now easily see that $x - y = (r + k) - (r + l) = k - l \in \mathbb{Z}$, proving the desired.

2.5 Congruence relations

Think again of the integers $\mathbb{Z}$ and the equivalence relation $\equiv$ defined by $n \equiv m$ if and only if $n - m$ is even, as discussed many times before, see for instance Example 86. This equivalence relation considers all natural numbers with the same parity equivalent. When $a \equiv b$ and $c \equiv d$ then $a + c \equiv b + d$, as one can quite readily compute. Indeed, these two assumptions respectively ensure the existence of n and m such that $2n = a - b$ and $2m = c - d$. We see that

$$(a + c) - (b + d) = (a - b) + (c - d) = 2n + 2m = 2 \cdot (n + m),$$

so $a + c \equiv b + d$ indeed holds.

In general, when we have a set X with some operations on it, one can wonder whether an equivalence relation R respects these operations as above. In that case, we say that R is a congruence relation with respect to these operations. Let us examine some examples.

91 Example (Addition on Rational Numbers)
Recall the set X and the equivalence relation $\equiv$ on it from Example 78 and 89. We can define an operation $\oplus$ on X by

$$\langle a, b \rangle \oplus \langle c, d \rangle = \langle a \cdot d + c \cdot b, b \cdot d \rangle .$$

It is easy to see that the right-hand pair again is an element of X, for $bd \neq 0$ when both b and d are non-zero.

Is $\equiv$ a congruence relation with respect to $\oplus$? Well, to see this we need to prove that whenever $\langle a, b \rangle \equiv \langle k, l \rangle$ and $\langle c, d \rangle \equiv \langle m, n \rangle$ we have that

$$\langle a \cdot d + c \cdot b, b \cdot d \rangle = \langle a, b \rangle \oplus \langle c, d \rangle \equiv \langle k, l \rangle \oplus \langle m, n \rangle = \langle k \cdot n + m \cdot l, l \cdot n \rangle .$$

Checking this comes down to wether

$$(a \cdot d + c \cdot b) \cdot l \cdot n = a \cdot d \cdot l \cdot n + c \cdot b \cdot l \cdot n = k \cdot n \cdot b \cdot d + m \cdot l \cdot b \cdot d = (k \cdot n + m \cdot l) \cdot b \cdot d$$

holds. Now we know that $al = bk$ and $cn = dm$, substituting this in the above equation gives demonstrates the desired.

92 Example (Multiplication on Rational Numbers)

In Example 91 above we considered addition, let us now consider multiplication on X. First define the operation $\otimes$ on X as

$$\langle a, b \rangle \otimes \langle c, d \rangle = \langle a \cdot c, b \cdot d \rangle ,$$

and note that the right-hand pair is an element of X whenever both left-hand pairs are. We now need to verify that whenever $\langle a, b \rangle \equiv \langle k, l \rangle$ and $\langle c, d \rangle \equiv \langle m, n \rangle$ we have that

$$\langle a \cdot c, b \cdot d \rangle = \langle a, b \rangle \oplus \langle c, d \rangle \equiv \langle k, l \rangle \oplus \langle m, n \rangle = \langle k \cdot m, l \cdot n \rangle .$$

This again comes down to a straightforward computation, as below.

$$(a \cdot c) \cdot (l \cdot n) = (a \cdot l) \cdot (c \cdot n) = (b \cdot k) \cdot (d \cdot m) = (b \cdot d) \cdot (k \cdot m)$$

93 Example (Logical Equivalence is a Congruence Relation with respect to the Connectives)

Recall the set $\mathcal{L}_{\text{PROP}}$ and the relation $\equiv$ as discussed in Example 77, 23 and 88. The relation $\equiv$ is a congruence relation with respect to all connectives. We leave it up to you to prove this, but note that intuitively it feels quite right that whenever $\phi \equiv \xi$ and $\psi \equiv \zeta$ both holds, one has $\phi \wedge \psi \equiv \xi \wedge \zeta$.

94 Example

Recall the partition from Example 83, which was given as

$$P = \left\{ \{ r + n \mid n \in \mathbb{N} \} \;\middle|\; r \in \mathbb{R}_{\geq 0} \right\} .$$

This partition induces an equivalence relation $\equiv$, and it is described by the logic equivalence below as was discussed in Example 90.

$$x \equiv y \text{ if and only if } x - y \text{ is an integer}$$

This equivalence relation is a congruence relation with respect to addition. Indeed, suppose that $a \equiv b$ and $c \equiv d$. This means that $a - b = k \in \mathbb{Z}$ and $c - d = l \in \mathbb{Z}$. We can now compute that

$$(a + c) - (b + d) = (a - b) + (c - d) = k + l \in \mathbb{Z},$$

whence it is immediate that $a + c \equiv b + d$. In Exercise 87 you are asked to check whether this is a congruence relation with respect to multiplication as well.

95 Example

Recall Example 84. Assume for the purpose of this example that $r = 0$. The partition described there with its induced equivalence relation on $\mathbb{R}$ is given below

$$P = \{ \{-x, +x\} \mid x \in \mathbb{R} \} , \quad x \equiv y \text{ if and only if } x = ky \text{ for } k \in \{-1, 1\}.$$

It is left to you to prove that this description in fact is correct.

It is not hard to verify that $1 \equiv -1$, $-1 \equiv -1$, $-2 \not\equiv 42$ and $2 \not\equiv 0$. Is $\equiv$ a congruence relation with respect to addition? Most certainly not! We know that $-1 \equiv 1$, but $2 = 1 + 1 \equiv 1 - 1 = 0$ does not hold.

We can prove however that this is an equivalence relation with respect to multiplication. Assume that $a \equiv b$ and $c \equiv d$. This means that $a = kb$ and $c = ld$ with both l and k elements of $\{-1, 1\}$. We get that

$$a \cdot c = (b \cdot k) \cdot (d \cdot l) = (b \cdot d) \cdot (k \cdot l),$$

and as $k \cdot l \in \{-1, 1\}$ the desired equivalence $a \cdot c \equiv b \cdot d$ is immediate.

2.6 Composition of relations

Thinking of some relation R, one can see $a\ R\ b$ as a step from a to b. Suppose there is another step from b to c, i.e. $b\ R\ c$ holds. We can now proceed from a in two steps to c. In fact, we can form a relation of such two-steps along R, and inspect this relation. Were R reflexive, the new two-step relation must be reflexive as well. If R is transitive, then the two-step relation is contained within R. In this section we will focus on such observations, but in a slightly more general context. We first give a formal definition of the two-step relation in general terms.

21 Definition (Composition)
Given a relation R between A and B and a relation S between B and C we define the composition of R and S, denoted $R \circ S$ as

$$R \circ S = \left\{ \langle a, c \rangle \;\middle|\; \text{there exists a } b \in B \text{ such that } a\ R\ b \text{ and } b\ S\ c \right\}.$$

96 Example
Let X be any set, and consider the relation of equality, the relation id_X, on this set. We now see that $\mathrm{id}_X \circ \mathrm{id}_X$ equals id_X.

97 Example
Consider the relation R on $\mathbb{Z}$ as defined in Example 46, which relates x to $x+1$. What does $R \circ R$ look like? We claim that $x\ (R \circ R)\ y$ if and only if $y = x + 2$.

The implication from right to left is easiest, so let us do that one first. We see that $x\ R\ (x+1)$ and $(x+1)\ R\ (x+2)$, so $x\ (R \circ R)\ (x+2)$ follows immediately from the definition of composition.

Now to prove the other direction, suppose that $x\ (R \circ R)\ y$. This gives us some b such that $x\ R\ b$ and $b\ R\ y$. Due to the first fact we know that $b = x + 1$, and the second fact shows that $y = b + 1$. Substituting the former equation into the latter yield the desired result.

98 Example
Two relations and their composition are graphically depicted in Fig. 2.13.

99 Example (Composition with Identity)
Actually, Example 96 is a lot more concrete than it needs to be. Consider any relation R between sets A and B. Also consider the relation id_B of equality on B. The relation R equals $R \circ \mathrm{id}_B$.

Let us prove this. First assume that $x\ R\ y$. It is clear that $x\ R\ y$, as this is precisely what we assumed. Moreover, $y = y$ also holds. This entails that $x\ (R \circ \mathrm{id}_B)\ y$.

Conversely, suppose that $x\ (R \circ \mathrm{id}_B)\ y$. Then there is a $b \in B$ such that $x\ R\ b$ and $b = y$. Substituting the latter in the former yields $x\ R\ y$, as desired. Convince yourself that id_A as a relation on A is such that R equals $R \circ \mathrm{id}_A$.

We can succinctly summarize the above two facts as follows:

$$\mathrm{id}_A \circ R = R = R \circ \mathrm{id}_B \quad \text{for all relations } R \text{ between } A \text{ and } B.$$

Recall from Example 46 that the relation R from that example and Example 97 has $<$ as its transitive closure. It is clear that $R \circ R$ is a subset of $<$. This is no accident or coincidence, it holds in quite some generality.

17 Lemma
Let R be some relation on A, and let S be a transitive relation containing R. Now $R \circ R \subseteq S$.

Proof. Assume that $x\ R \circ R\ z$. This gives us some y such that $x\ R\ y$ and $y\ R\ z$. Because S is contains R we know that $x\ S\ y$ and $y\ S\ z$ follow. The transitivity of S now ensures $x\ S\ z$. ■

As a corollary, note that the transitive closure of R contains $R \circ R$. We could prove even more interesting facts about composition and transitivity, but we refrain from doing so and leave this joyous task to you in Exercise 90.

When one considers the sum x, y and z there is an issue of bracketing. Do we mean $x + (y + z)$ or $(x + y) + z$? This does not matter! Similarly, when given three sets X, Y and Z one can consider the union of the three. Do we mean $X \cup (Y \cup Z)$ or $(X \cup Y) \cup Z$? Again, this does not matter! As an aside, one can easily prove this by realizing that

$$X \cup (Y \cup Z) = \bigcup \{X, Y, Z\} = (X \cup Y) \cup Z,$$

so all questions of bracketing become quite moot.

This property of “irrelevance of bracketing” is called associativity. The operation of relation composition is yet another operation that enjoys this nice property.

18 Lemma (Associativity of Composition)
Let R, S and T be relations between A and B, B and C and finally, C and D. Then $R \circ (S \circ T) = (R \circ S) \circ T$.

Proof. We prove the inclusion from left to right, the other inclusion is left to you as an exercise. Assume that $a\ (R \circ (S \circ T))\ d$ holds for some $a \in A$ and $d \in D$. By definition this yields a $b \in B$ such that $a\ R\ b$ and $b\ (S \circ T)\ d$. The latter, again by definition, yields a $c \in C$ such that $b\ S\ c$ and $c\ T\ d$.

We can now collate all this information. From $a\ R\ b$ and $b\ S\ c$ we derive that $a\ (R \circ S)\ c$. This, together with $c\ T\ d$, yields $a\ ((R \circ S) \circ T)\ d$ as desired. ■

In Example 45 you might have gotten the idea that the transitive closure can be approximated iteratively. Now that we know of composition, this is something we can explore further. Instead of providing a full proof at this stage, we but hint at the appropriate direction. The concept of mathematical induction can be used to make the following proof completely watertight. Unfortunately we have not covered this principle yet, so the proof will remain a bit leaky.

19 Lemma
Let R be a relation on some set X. Define $R_1 = R$ and $R_{n+1} = R \circ R_n$ for each $n \in \mathbb{N}$. Finally, define $S = \bigcup_{n=1}^{\infty} R_n$. The relation S is the transitive closure of R.

Proof. First note that $R = R_1 \subseteq S$, so S certainly extends R. To prove that S is transitive, assume that $x\ S\ y$ and $y\ S\ z$. By construction we now know of natural numbers n and m greater than zero such that $x\ R_n\ y$ and $y\ R_m\ z$. Consequently, $x\ R_n \circ R_m\ z$ follows.

We claim that $R_n \circ R_m$ in fact equals R_{m+n}. This is all too easy to see when $n = 1$. If $n = 2$ then

$$R_2 \circ R_m = R_{1+1} \circ R_m = (R \circ R_1) \circ R_m = R \circ (R_1 \circ R_m) = R \circ (R_{m+1}) = R_{m+2},$$

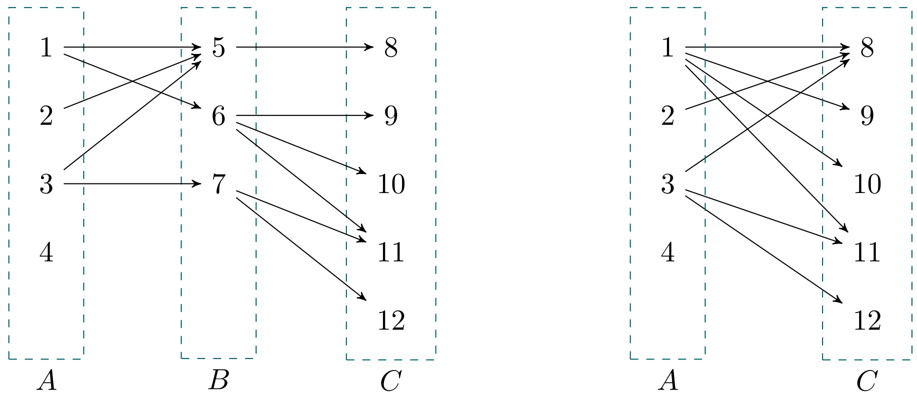

Figure 2.13: A relation R between A and B, a relation S between B and C and its composition $R \circ S$ between A and C.

where we used the associativity of composition in the middle. When $n = 3$ we can use the same trick, and so onward for each other natural number. Intuitively, this shows that the equality $R_n \circ R_m = R_{m+n}$ holds for each natural n and m greater than zero. The above entails that $x \ R_{m+n} \ z$, and as $R_{m+n} \subseteq S$ this ensures $x \ S \ z$ as desired.

Finally, assume that T is some transitive relation such that $R \subseteq T$. We want to prove that $S \subseteq T$. To this end, suppose that $x \ S \ z$. This gives some natural $n \geq 1$ such that $x \ R_n \ z$. If $n = 1$ then it is easy to see that $x \ T \ z$, because T extends $R = R_1$. When $n = 2$ we see that from $x \ R_2 \ z$ we get a $y \in X$ such that $x \ R \ y$ and $y \ R \ z$. This in turn implies that $x \ T \ y$ and $y \ T \ z$, so transitivity does the job. Intuitively, the pattern is this. Because $R \subseteq T$ and $x \ R_n \ z$ we know that $x \ T \ y_1 \ T \ y_2 \ T \ y_{n-2} \ T \ z$ for some $y_1, \ldots, y_{n-2} \in X$. Transitivity now ensures that $x \ T \ z$. But this is what we wanted to prove.

These arguments are all intuitively moderately convincing, but leave one slightly dissatisfied. The proof is less rigorous than we had gotten used to. Later on, when we have mathematical induction at our fingertips, we revisit this proof and re-do it properly. ■

2.7 Exercises

38 Exercise (Writing out the Cartesian Product)

Write down the elements of $\{a, b\} \times \{a, c, d\}$.

39 Exercise (Coding Pairs)

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

40 Exercise (Other Codings)

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

$$\begin{tikzcd} 0 \arrow[r] \arrow[d] & 1 \arrow[dl] \arrow[d] \\ 2 & 3 \end{tikzcd}$$

Figure 2.14: Some relation on the set $\{0, 1, 2, 3\}$.

41 Exercise

Which of the following hold:

(i) $\{a\} \in \{\langle\, a, b\,\rangle\}$;

(ii) $\{b\} \in \{\langle\, a, b\,\rangle\}$;

(iii) $\langle\, 1, 2\,\rangle \subseteq \mathbb{N}$;

(iv) $\{\langle\, 1, 2\,\rangle \subseteq \mathcal{P}(\mathbb{N})$.

42 Exercise (Product of Unions)

Let X, Y, A and B be sets. Prove that

$$(X \cup A) \times (Y \cup B) = X \times Y \cup X \times B \cup A \times Y \cup A \times B$$

43 Exercise

Write the the relation of pairs of reals for which the second element is the square of the first in set-notation.

44 Exercise (Identity in the Plane)

Describe the subset $\{\,\langle\, x, y\,\rangle \mid x = y\}$ of the real plane $\mathbb{R}^2$.

45 Exercise (Triples)

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 does this relation have? Give two elements of the relation.

46 Exercise

Is the relation given by Fig. 2.14 euclidean? Which arrows have to be added to make it a transitive relation?

47 Exercise

Are the relations in Fig. 2.15 dense? Serial? Is the following relation dense? Serial?

48 Exercise

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

49 Exercise (Subset Relation is Transitive)

Let X be any set. Prove that $\subseteq$ on $\mathcal{P}(X)$ is transitive.

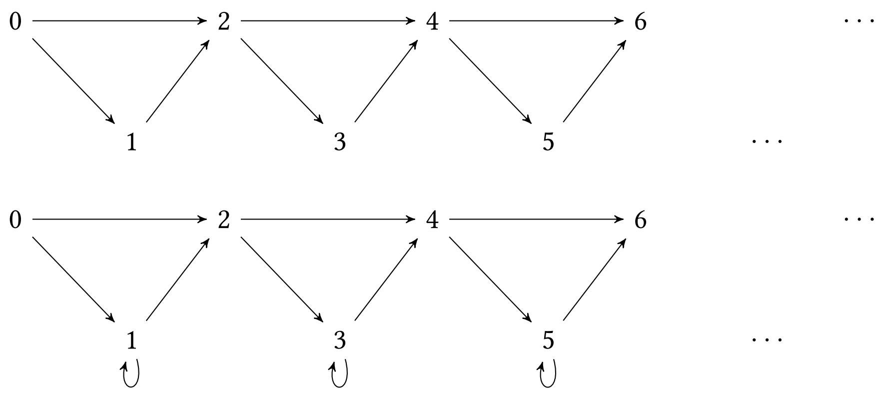

Figure 2.15: Some relations on $\mathbb{N}$.

50 Exercise (Divisibility is Transitive)
Prove that the relation $|$ as introduced in Example 34 is transitive.

51 Exercise (Intersection and Transitivity)
In this exercise we generalize the result of Lemma 9, where we showed transitive relations to be "closed" under binary intersection, to the "closure under arbitrary intersection". First, recall the set-operation $\bigcap$ from Exercise 37. Let X be any set, and suppose that A is a set of transitive relations on X. That is to say, all elements of A are in fact transitive relations on X. Prove that $\bigcap A$ is a transitive relation on X.

52 Exercise (Union and Transitivity)
Prove or disprove: for any pair of transitive relations R and S on any set X, the union $R \cup S$ is transitive as well.

53 Exercise (Euclidian Both Ways)
Show that for any euclidean relations R on X the following holds:

$$\text{for all } a, b, c \in X, \text{ if } a \; R \; b \text{ and } a \; R \; c \text{ then } b \; R \; c \text{ and } c \; R \; b.$$

54 Exercise (Trivial Seriality)
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 or A is empty.

55 Exercise (Symmetry)
The definition of symmetry even makes sense when R is a relation between sets A and B.

(i) Give a sensible definition of symmetry in this setting.

(ii) Prove that the relation that is the cartesian product $A \times B$ of two sets is symmetric if $A = B$.

56 Exercise (Not a Total Order)
Prove that the relation $\{ \langle x, y \rangle \in \mathbb{R} \times \mathbb{R} \mid x^2 = y \}$ is not a total order on $\mathbb{R}$.

57 Exercise (Logically Equivalent Formulae)
Show that the relation $\equiv$ of Example 23 on the set of propositional formulas indeed is an equivalence relation, as it was claimed to be in Example 77.

58 Exercise (Subsets of a Set)
Consider the relation $\subseteq$ restricted to $\mathcal{P}(X)$ for an arbitrary set X.

(i) Prove that this relation is a partial order;

(ii) What about the relation $\subset$?

(iii) Prove that $\subseteq$ is not a total order when X has 1023 elements.

(iv) There is not much special about the number 1023 in the above item. Give the least number which would work there.

59 Exercise (Reflexive Closure)
Let R be any relation on X. Prove that:

(i) Any reflexive relation on X contains id_X;

(ii) The relation $S = R \cup \mathrm{id}_X$ is reflexive;

(iii) For any reflexive relation T extending R we have that $S \subseteq T$.

These items suggest that $R \cup \mathrm{id}_X$ is the "least reflexive relation extending R". We will revisit this notion in Exercise 66.

60 Exercise (Symmetric Closure)
Let R be a relation on X. Consider the relation S defined by:

$$x \; S \; y \quad \text{if and only if} \quad x \; R \; y \text{ or } y \; R \; x$$

Prove that:

(i) The relation R is reflexive if and only if S is reflexive;

(ii) The relation S is symmetric.

(iii) For any symmetric relation T such that $R \subseteq T$ we have $S \subseteq T$.

These items above suggest that S is the "least symmetric relation extending R". We will revisit this notion in Exercise 66.

61 Exercise (Size of Union)
Prove that for finite sets X and Y the following holds:

$$|\, X \cup Y \,| \leq |\, X + Y \,| \, .$$

62 Exercise
In this exercise we will show that $=$ is the largest relation satisfying both symmetry and anti-symmetry. Let us make this a bit more precise. Consider some set X and a relation R on X. Suppose furthermore that R is both symmetric and anti-symmetric. Prove that:

(i) for all $a, b \in X$ we have that if $a\ R\ b$, then $a = b$.

(ii) if R is reflexive, then $R = \mathrm{id}_X$.[2]

(iii) Lemma 12 holds, using (i).

63 Exercise

Let R be an relation on X. Prove the following:

(i) if R is reflexive and euclidian, then R is symmetric and transitive as well;

(ii) if R is transitive and symmetric, it is euclidian as well;

(iii) the relation R is an equivalence relation if and only if R is reflexive and euclidian.

64 Exercise

Let R be a relation on the set X, and assume that R is reflexive. Prove that for any set Y we know R to be reflexive as a relation on $X \cup Y$ if and only if $Y \subseteq X$.

65 Exercise

Given a relation R on a set X and some subset $Y \subseteq X$ we can define the restriction of R to this subset Y, which we denote as $R \restriction Y$. It is defined as $R \cap Y \times Y$.

A property is called subset-hereditary if whenever R has a property, then so does $R \restriction Y$ for all subsets Y of X. Which of the properties given in Section 2.3 are subset-hereditary, and which are not? In the latter case, provide counter examples.

66 Exercise (Reflexivity, Symmetry & Intersection)

In Exercise 51 we proved that the intersection of a set of transitive relations on a particular set is in turn transitive. This comes in handy when proving that the transitive closure exists. In Exercises 59 and 60 we considered the reflexive and symmetric closure. We also gave a fairly explicit construction of these closures. One may wonder whether the approach of Lemma 10 not only works in the transitive case, but also for reflexive and symmetric closures. Let us investigate this. Let X be a set, let R be a relation on X and let A be a non-empty set of relations on X.

(i) Prove that when all relations in A are reflexive, $\bigcap A$ is reflexive as well;

(ii) Prove that when all relations in A are symmetric, $\bigcap A$ is symmetric as well;

(iii) Prove that the intersection of all reflexive relations on X extending R is the reflexive closure of R.

(iv) Prove that the intersection of all symmetric relations on X extending R is the symmetric closure of R.

67 Exercise

Recall the relation $\equiv$ on the reals $\mathbb{R}$ as discussed in Example 84 and 95. Prove that $x \equiv y$ if and only if $x^2 = y^2$.

[2] This is precisely one of those places where using $=$ instead of id_X would be confusing, as foretold in Example 44.

68 Exercise

Let X be the set of students in this course. Which of the following relations on X are equivalence relations:

(i) the relation R such that $a\ R\ b$ if and only if a and b have the same first name;

(ii) the relation S such that $a\ S\ b$ if and only if a and b live within one kilometers of one another;

(iii) the relation T such that $a\ T\ b$ if and only if a and b do not differ in the grades they got for their homework exercises.

69 Exercise

Define a relation R on $\mathbb{N}^+$ as

$$R = \left\{ \langle n, m \rangle \in \mathbb{N}^+ \times \mathbb{N}^+ \;\middle|\; \text{for all } k \in \mathbb{N}^+ \text{ one has } k \mid n \text{ if and only if } k \mid m \right\}$$

Prove or disprove: the relation R is an equivalence relation. Can you describe R in a simpler way?

70 Exercise

Consider the set $X = \mathbb{R} \times \mathbb{R} \setminus \{\langle 0, 0 \rangle\}$. We define a relation D on X as

$$D = \left\{ \langle \langle a, b \rangle, \langle c, d \rangle \rangle \;\middle|\; \text{there exists an } r \in \mathbb{R} \text{ with } r \neq 0,\ a \cdot r = c \text{ and } b \cdot r = d \right\}.$$

See for instance that $\langle 1, -1 \rangle\ D\ \langle -1, 1 \rangle$ and $\langle 1, 0 \rangle\ D\ \langle -5, 0 \rangle$ but not $\langle 1, 2 \rangle\ D\ \langle 2, 1 \rangle$.

(i) Prove that $\langle x, 1 \rangle\ D\ \langle x \cdot y, y \rangle$ for all x and y in $\mathbb{R}$;

(ii) Prove that $x \in \mathbb{R}$, we have $\langle x, 0 \rangle\ D\ \langle 1, 0 \rangle$ for all $x \in \mathbb{R}$;

(iii) Give a geometric description of the equivalence classes of $\langle 0, 1 \rangle$, $\langle 1, 0 \rangle$ and $\langle 3, 2 \rangle$;

(iv) (Geometrically) describe the partition X/D.

71 Exercise

Let R be the relation on $\mathbb{R}$ defined as below. Prove or disprove: the relation R is an equivalence relation.

$$x\ R\ y \text{ if and only if } (x - y)^2 \leq (x + y)^2$$

72 Exercise

Recall the relation R_n on $\mathbb{Z}$ from Example 35, defined such that

$$x\ R_n\ y \text{ if and only if } n \mid x - y.$$

In this exercise we will inspect this relation and prove the presence and absence of some properties. Prove that:

(i) $R_1 = \mathbb{Z} \times \mathbb{Z}$;

(ii) for any $n \geq 2$ it is the case that the relation R_n is reflexive if and only if $n = 2$.

(iii) the relation R_n is symmetric for all $n \geq 2$.

(iv) the relation R_n is not transitive for all $n \geq 3$.

73 Exercise (Equivalence Closure)
Let X be any set and let R be a relation on X. We revisit Exercises 59, 60 and 66 and consider the equivalence closure, that is, the smallest equivalence relation extending a particular relation.

(i) Prove that if R is reflexive, then so is the relation S defined as:

$$S = \{ \langle x, y \rangle \in X \times X \mid x \; R \; y \text{ or } y \; R \; x \} .$$

(ii) Prove that if R is symmetric, then so is the relation S defined as $S = R \cup \mathrm{id}_X$;

(iii) Prove that if R is reflexive and symmetric, then its transitive closure is an equivalence relation;

74 Exercise (Sensitivity to Order)
Let R be a relation on a set X. In Exercise 73 we proves that if R is reflexive and symmetric, then so is the transitive closure of R. Prove or disprove:

(i) if R is transitive and reflexive, then the relation S as defined below is an equivalence relation;

$$S = \{ \langle x, y \rangle \in X \times X \mid x \; R \; y \text{ or } y \; R \; x\}$$

(ii) if R is transitive and symmetric, then the relation $S = R \cup \mathrm{id}_X$ is an equivalence relation.

75 Exercise (Equidistant Points)
We define a relation R on the real plane $\mathbb{R}^2$ as follows:

$$\langle a, b \rangle \; R \; \langle c, d \rangle \text{ if and only if } (a - b)^2 = (c - d)^2 .$$

(i) Prove that the relation R is an equivalence relation;

(ii) Prove that $\langle x, x + \lambda \rangle \; R \; \langle y, y + \lambda \rangle$ holds for all $x, y, \lambda \in \mathbb{R}$;

(iii) Describe the partition $\mathbb{R} \times \mathbb{R}/R$.

76 Exercise (Rational Difference)
Consider the real numbers $\mathbb{R}$ and the relation R defined on $\mathbb{R}$ as

$$R = \{ \langle x, y \rangle \in \mathbb{R} \times \mathbb{R} \mid x - y \in \mathbb{Q}\}$$

(i) Show that $0 \; R \; 5$, $\frac{1}{2} \; R \; \frac{5}{7}$ and $\sqrt{2} \; R \; (\sqrt{2} + \frac{11}{15})$;

(ii) Let n and m be integers with greatest common divisor 1. That is to say, for any $k \in \mathbb{N}^+$ we have that if $k \mid n$ and $k \mid m$ then $k = 1$. Furthermore, assume that $n^2 = m^2 \cdot 2$. Derive a contradiction from this fact.

(iii) Use (ii) to prove that $\sqrt{2} = \frac{a}{b}$ for some $a, b \in \mathbb{Z}$ leads to a contradiction.

(iv) Prove or disprove: there exist $x, y \in \mathbb{R}$ such that $x \; R \; y$ does not hold.

(v) Describe the partition $\mathbb{R}/R$ in set-notation.

77 Exercise (Grothendieck Group Construction)

In this exercise we will describe the set of integers $\mathbb{Z}$ as a partition of $\mathbb{N} \times \mathbb{N}$. To this end we first define the relation $\equiv\ \subseteq (\mathbb{N} \times \mathbb{N}) \times (\mathbb{N} \times \mathbb{N})$ as

$$\langle a, b \rangle \equiv \langle c, d \rangle \text{ if and only } a + d = b + c.$$

We will show that $\mathbb{N} \times \mathbb{N}/\equiv$ "behaves" just like $\mathbb{Z}$.

(i) Prove that the relation $\equiv$ actually is an equivalence relation;

(ii) Describe the partition $\mathbb{N} \times \mathbb{N}/\equiv$;

(iii) Define the operation $\oplus$ on $\mathbb{N} \times \mathbb{N}$ as follows:

$$\langle a, b \rangle \oplus \langle c, d \rangle = \langle a + c, b + d \rangle$$

Prove that if $x_1 \equiv x_2$ and $y_1 \equiv y_2$ then $x_1 \oplus y_1 \equiv x_2 \oplus y_2$;

(iv) Prove that for each natural number $n \in \mathbb{N}$ one has:

$$\langle n, 0 \rangle \oplus \langle 0, n \rangle \equiv \langle 0, 0 \rangle ;$$

(v) To strengthen the result of (iv), show that for each $\langle a, b \rangle \in \mathbb{N} \times \mathbb{N}$ one has

$$\langle a, b \rangle \oplus \langle b, a \rangle \equiv \langle 0, 0 \rangle .$$

78 Exercise (Equal Sums)

Let M be the following relation on $\mathbb{Z}^3$:

$$\langle a, b, c \rangle \ M \ \langle d, e, f \rangle \text{ if and only if } a + b + c = d + e + f$$

Prove or disprove: M is an equivalence relation.

79 Exercise (Not Symmetric and Not Anti-Symmetric)

Recall Example 54, where we constructed a relation R on a set X such that R is both not symmetric and not anti-symmetric. In that example we have $|X| = 3$. Can we make a set X and a relation R on X such that R is neither symmetric nor anti-symmetric with $|X| = 2$? And can we make it even smaller? Prove your answer!

80 Exercise (Singleton Partitions)

We continue from Example 85. Prove that for any non-empty set X and any equivalence relation R on X the following are logically equivalent:

(i) the set X/R is a singleton;

(ii) the relation R is weakly connected;

(iii) the relation R equals $X \times X$

81 Exercise (Equivalence from a Relation)
Let R be a relation between sets X and Y. Using this relation R we define a relation S on X as follows:
$$S = \{ \langle a, b \rangle \in X \times X \mid \text{there exists a } y \in Y \text{ such that } a\ R\ y \text{ and } b\ R\ y. \}$$

(i) Prove that S is reflexive if and only if R is serial;

(ii) Prove that S is symmetric, and that if R is deterministic then S is transitive;

(iii) Assume from now on that R is serial and determinstic. By the above two items we know that S is an equivalence relation. Consider the relation T between X/S and Y defined as
$$A\ T\ y \text{ if and only if } a\ R\ y \text{ for all } a \in A$$
Prove that T is both serial and deterministic.

(iv) Prove that for all $A, B \in X/S$ and $y \in Y$ we have that $A\ T\ y$ and $B\ T\ y$ entail $A = B$.

Hint: Use Lemma 14.

82 Exercise
Recall Exercise 75 and Exercise 81. The former exercise falls into the pattern described by the latter. Find a relation R between $\mathbb{R}^2$ and $\mathbb{R}$ such that D of Exercise 75 coincides with S as constructed in Exercise 81.

83 Exercise
Find a set Y and a relation R between $\mathbb{Z}^3$ and Y such that the relation M of Exercise 78 arises as the relation S from Exercise 81, using this R.

84 Exercise
Consider the following relation E on $\mathbb{R}$:
$$x\ E\ y \text{ the decimal expansions of } x \text{ and } y \text{ agree up to the tenth digit}$$
This means that $\pi\ E\ 3.14149265358$ and $\frac{1}{1099511627776}\ E\ 0$ hold, but $\frac{1}{128}\ E\ 0.007$ does not.

(i) Prove that E is an equivalence relation;

(ii) Find a set Y and a relation R between $\mathbb{R}$ and Y such that the relation S from Exercise 81 equals the relation E as defined above.

85 Exercise (Sudoku)
We can represent sudokus fully using partitions. First we define the sudoku frame (or: the empty sudoku) by three partitions on the set of fields S, where a field is a small square into which a number fits. The partitions are $\mathcal{S}$ (the big squares), $\mathcal{R}$ (the rows) and $\mathcal{C}$ (the columns).

These partitions have some special properties. For example if $R \in R$ and $C \in \mathcal{C}$, then $R \cap C$ has precisely one element. Another example is: each S in $\mathcal{S}$ has precisely 9 elements.

(i) Can you give three other examples of a special properties?

(ii) We can describe a fully solved sudoku by a fourth partition $\mathcal{N}$. What is the idea of this partition?

(iii) This partition should satisfy a constraint (have a special property) to represent a correct solution. What is this constraint?

(iv) Our representation cannot distinguish between two sudoku's where we have, for example interchanged the 8 and the 9 everywhere. Is that a good or a bad thing?

(v) Can you define a partially filled-in sudoku? What is the (minimal) condition that a partially filled-in sudoku has to satisfy in order to qualify as a sudoku puzzle?

86 Exercise (Encoding the Rationals Again)
Construct an equivalence relation R on the set $\mathbb{Z} \times \mathbb{N}_{>0}$ such that the rational numbers $\mathbb{Q}$ correspond to equivalence classes of this relation. Prove that the equivalence relation R is a congruence relation with respect to addition and multiplication.

87 Exercise
Recall the equivalence relation $\equiv$ on the non-negative reals $\mathbb{R}_{\geq 0}$ from Example 83, 90 and 94. In the latter example we showed that $\equiv$ is a congruence relation with respect to addition on the non-negative reals. Prove or disprove: $\equiv$ is a congruence relation with respect to multiplication on the non-negative reals.

88 Exercise (Equivalence from Partial Order)
Let $\leq$ be a relation on a set D, and assume that $\leq$ is both reflexive and transitive. Define a relation $\equiv$ on D by

$$x \equiv y \text{ if and only if } x \leq y \text{ and } y \leq x.$$

(i) Prove that $\equiv$ is an equivalence relation.

(ii) Prove that $\equiv$ is a congruence relation with respect to $\leq$. That is to say, prove that if $x_1 \equiv x_2$ and $y_1 \equiv y_2$ then $x_1 \leq y_1$ if and only if $x_2 \leq y_2$.

(iii) We define a relation $\preceq$ on $D/\equiv$ by

$$X \preceq Y \text{ if and only if } x \leq y \text{ holds for all } x \in X \text{ and } y \in Y.$$

Prove that this relation is a partial order on $D/\equiv$.

89 Exercise (Congruence on the Reals divided by the Rationals)
Let R be the equivalence relation of Exercise 76 and let $r \in \mathbb{R}$ be any real number. Show that R is a congruence for the function $F_r(x) = x + r$.

90 Exercise
Let R be any relation on A. Prove that

(i) $R \circ R \subseteq R$ if and only if R is transitive;

(ii) $R \subseteq R \circ R$ if and only if R is dense.

91 Exercise
Let R be and S be relations on X. Prove that:

(i) if R and S are symmetric, so is $R \circ S$;

(ii) if R and S are transitive, so is $R \circ S$;

(iii) if R and S are serial, so is $R \circ S$.

92 Exercise (Distributive Laws Again)
Let R, S and T be relations on a set X. Prove that

$$\begin{aligned} R \circ (S \cup T) &= (R \circ S) \cup (R \circ T) \\ R \circ (S \cap T) &= (R \circ S) \cap (R \circ T). \end{aligned}$$

93 Exercise (Anti-Symmetry)
Let R and S be relations on a set X. Suppose that S is anti-symmetric. Prove that R is symmetric if and only if $R = \mathrm{id}_X$.

Hint: Derive a contradiction assuming that R is symmetric yet does not equal id_X. This proves the implication "R is symmetric entails $R = \mathrm{id}_X$" by contradiction.

3 Functions

On an intuitive level, a function is some sort of relation between input and output. Think for instance of the function which associates to each natural numbers its immediate successor. The relation between input and output is quite clear, and one can easily see how it could be computed. This function has a clear algorithmic content, and is easily described in such a manner. We will adopt special notation for this, and write $x \in \mathbb{N} \mapsto x + 1 \in \mathbb{N}$, which is to be read as "the function which maps a natural number x to the natural number $x + 1$.

Not all functions lend themselves to such a straightforward description. Think of the unit circle in the plane. Now think of any real angle between 0 and 360, say r. This angle determines a point on the circle, which, as any point, has both an x-coordinate and a y-coordinate. We can define a function which maps a real $0 \leq r \leq 360$ to the x-coordinate of the point described above, and this is a perfectly valid function. See Fig. 3.1 for a graphical depiction of this process. You might know already that this is a well-known mathematical function, the cosine. Intuitively, this is just as much a function as the successor function is, but a clear algorithmic description is lacking.

The above suggests that a workable definition of a mathematical function ought not to contain the algorithmic process by which the input is related to the output, it need only to describe what this relation looks like. In the previous chapter it has been explained how relations can be coded as sets, namely as sets of ordered pairs. Functions too can be viewed as sets, or relations, but with certain additional properties. The first relational property one would expect a function to have is seriality, that is, each input yields output. The other property is that of determinacy, which states that one the input is known, the output is fixed. With these two notions we are now ready to define what we will mean by a "function". Note that as with relations, it is important to know "between" what a function works.

22 **Definition (Function)**
A function f from X to Y is a relation between X and Y which is both serial and deterministic. We denote this as $f : X \to Y$ and call A the domain of f, written $\mathrm{dom}(f) = X$, and Y is the codomain of f, written $\mathrm{cod}(f) = Y$.

If $f : X \to Y$ is a function then to each $x \in X$ there is a unique $y \in Y$ such that $x \ f \ y$. We write this as $f(x) = y$. Functions are also called maps or mappings. When the domain and codomain of a function f are both equal to X, we say that f is a function on X.

This is not a computational view on functions, as f is not viewed as an operation or algorithm that on input x provides an outcome $f(x)$, like e.g. the function $\mathrm{gcd}(x, y)$ that outputs the greatest common divisor of numbers x and y. The intuitive notion of a function $f : A \to B$ is intensional: f is given by a rule or computation that associates an element in B with every element in A. From an intensional perspective, two functions f and g may be such that $f(x) = g(x)$ for all values x, but when they arise from distinct algorithms, they are seen as different entities. This makes good intuitive sense, and it can be quite sensible to discern between these things, for instance when the one function is significantly simpler to compute than the other.

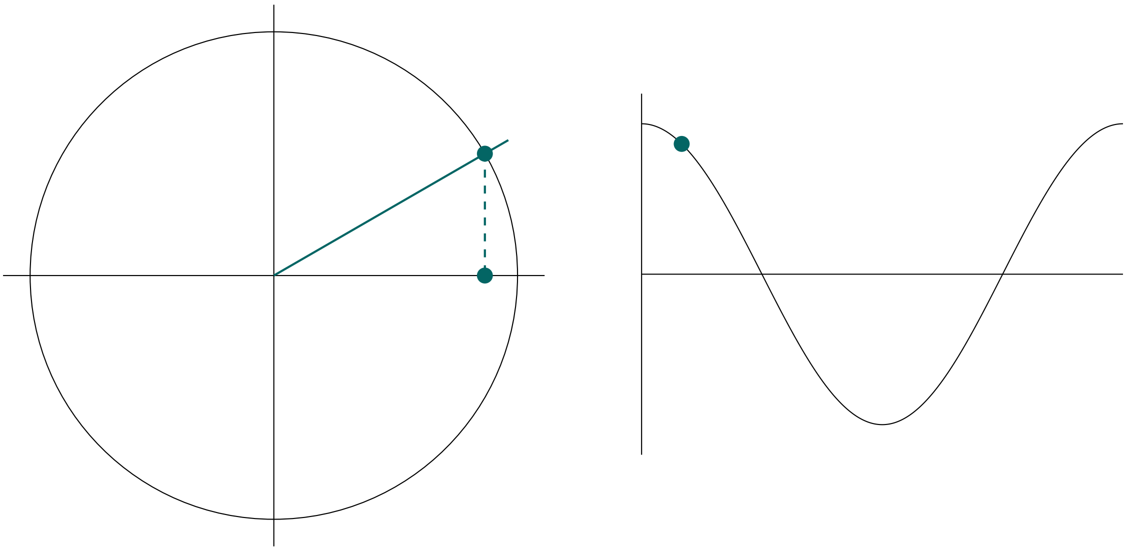

Figure 3.1: Graphical depiction of the cosine function.

These intuitions we lose in set theory, as in this setting functions are extensional: if $f : X \to Y$ and $g : X \to Y$ then from $f(x) = g(x)$ for all $x \in X$ we can derive $f = g$, because the sets $\{\langle x, y \rangle \in X \times Y \mid f(x) = y\}$ and $\{\langle x, y \rangle \in X \times Y \mid g(x) = y\}$ are the same, and these sets are respectively equal to f and g. Thus there is no reference to the processes underlying f and g which might distinguish them. What we gain by this at first sight somewhat unnatural set-theoretic view is the insight that functions can be defined in terms of sets, thus again showing that basic notions of mathematics can be defined in terms of sets.

100 Example
The function $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = 2x$ is the set $\left\{ \langle x, y \rangle \in \mathbb{R}^2 \;\middle|\; 2x = y \right\}$.

101 Example
Recall the identity relation id_X on a set X as introduced in Example 44. In Example 64 we already proved it to be deterministic. Example 63 proves every reflexive relation to be serial, and id_X is the archetypical reflexive relation. Consequently, id_X is a bonafide function. In function notation we could denote it as $x \in X \mapsto x$.

102 Example
The unit circle $S = \left\{ \langle x, y \rangle \in \mathbb{R}^2 \;\middle|\; x^2 + y^2 = 1 \right\}$ is a subset of $\mathbb{R}^2$, the plane. There exists functions $f, g : S \to \mathbb{R}$ defined by $f(x, y) = x^2$ and $g(x, y) = 1 - y^2$. Take care to note that although f and g are defined by ostensibly different expressions, they are (extensionally) equal because for all $\langle x, y \rangle \in S$ we have:

$$f(x, y) = x^2 = x^2 + (1 - x^2 - y^2) = 1 - y^2 = g(x, y).$$

103 Example (Cantor Pairing)
Picture $\mathbb{N} \times \mathbb{N}$ as the upper-right quadrant of the plane with natural coordinates. Fix your minds eye on the origin, the point $\langle 0, 0 \rangle$. Skip to $\langle 1, 0 \rangle$ and glance diagonally upwards to $\langle 0, 1 \rangle$. Now skip again, this time to $\langle 2, 0 \rangle$, and diagonally move upwards to $\langle 0, 2 \rangle$. Again, skip to $\langle 3, 0 \rangle$ and diagonally move to $\langle 0, 3 \rangle$.

One can repeat this process without end, and each point of $\mathbb{N} \times \mathbb{N}$ will eventually be looked at. The process is illustrated in Fig. 3.2. It defined a function from $\mathbb{N} \times \mathbb{N}$ to $\mathbb{N}$, where $\langle x, y \rangle$ is mapped to the amount of elements of $\mathbb{N} \times \mathbb{N}$ you have to look at before the above described process gets you to $\langle x, y \rangle$.

This function can be mathematically described. It is precisely the number of natural numbers in the triangle determined by the origin, the point $\langle x + y - 1, 0 \rangle$ and the point $\langle 0, x + y - 1 \rangle$, plus y. This comes down to the function

$$\langle x, y \rangle \mapsto \frac{1}{2}\Big(x + y\Big)\Big(x + y + 1\Big) + y.$$

One can note that $\langle x, y \rangle = \langle a, b \rangle$ if and only if $a = x$ and $b = y$, as you will be asked to prove later in Exercise 124.

104 Example
Consider the function $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = \sqrt{x^2}$. For all $x \geq 0$ we have $f(x) = x$, but $f \neq \mathrm{id}_{\mathbb{R}}$. Indeed, for any $x < 0$ we know $f(x) = -x$, yet $\mathrm{id}_{\mathbb{R}}(x) = x$ as stipulated in Example 101. The function $g : \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}$ defined by $g(x) = \sqrt{x^2}$ does equal $\mathrm{id}_{\mathbb{R}_{\geq 0}}$.

105 Example (Cosines Again)
Upon closer inspection of Fig. 3.1 one clearly sees that the cosine of an angle equals the cosine of that very angle plus 360. Let cos denote the cosine functions, which maps a real number representing a radian to the x-coordinate of the point on the unit circle intersecting the triangle determined by this radian. That is to say, let cos stand for the cosine function as you are familiar with it from high school. We now define functions $f : \mathbb{R} \to \mathbb{R}$ and $g : \mathbb{R} \to \mathbb{R}$ as

$$f(x) = \cos(x + 3\pi), \qquad\qquad g(x) = \cos(x + 5\pi).$$

Due to our above argument, we can see that the following equality holds for all $x \in \mathbb{R}$.

$$f(x) = \cos(x + 3\pi) = \cos(x + 3\pi + 2\pi) = \cos(x + 5\pi) = g(x)$$

In our extensional view of functions, it now follows that f and g are equal.

106 Example
Consider the real numbers $\mathbb{R}$. We define an equivalence relation $\equiv$ on $\mathbb{R}$ as

$$x \equiv y \text{ if and only if } x - y = 2 \cdot k \cdot \pi \text{ for some } k \in \mathbb{Z}.$$

One can readily verify that this is indeed an equivalence relation. It is, after all, not much different from the equivalence relation described in Lemma 16.

We can see that $\mathbb{R}/{\equiv}$ is actually equal to the set

$$\Big\{\, \{ x + 2 \cdot k \cdot \pi \mid k \in \mathbb{Z}\} \;\Big|\; x \in \mathbb{R} \Big\}.$$

There is a function $p : \mathbb{R} \to R/{\equiv}$ defined by $p(x) = [x]$.

107 Example (Canonical Projection)
In defining the function p of Example 106 we used nothing special about the equivalence relation $\equiv$ of that example. In fact, for any set X and any equivalence relation $\equiv$ on X we have a function

$$p : X \to X/{\equiv}, \quad x \mapsto [x].$$

This map p is often called the canonical projection of the equivalence relation $\equiv$.

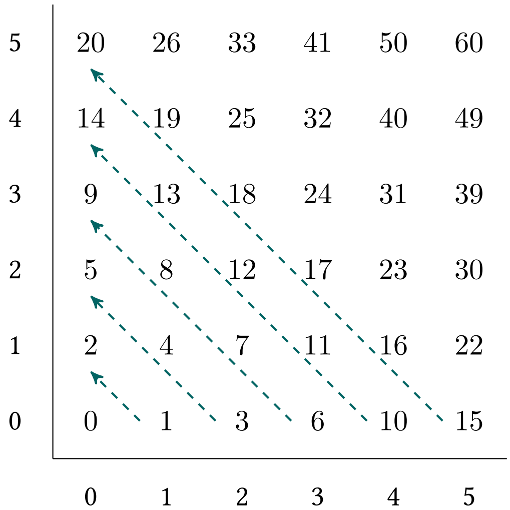

Figure 3.2: Cantor pairing graphically depicted.

Given any set $A \subseteq X$ and a function $f : X \to Y$ one can consider the points in Y that are reachable via f from A. We can define this formally as follows.

23 Definition (Range)
Let $f : X \to Y$ be a function. For any set $A \subseteq X$ we define the image (beeld in Dutch) of A under f to be

$$f(A) = \{ f(a) \mid a \in A \} .$$

The range (bereik in Dutch) of f, denoted $\mathrm{rng}(f)$, is defined by $f(\mathrm{dom}(f))$.

The above neatly shows that the range is simply the full image of the function, that is, all points that are reached by something in the domain. This suggests an alternate description, which we can prove to be equivalent. Let us do this.

20 Lemma
Let $f : X \to Y$ be any function. The following equality holds for all $A \subseteq X$:

$$f(A) = \{ y \in Y \mid \text{there exists a } a \in A \text{ such that } f(a) = y \} .$$

Proof. This is not tremendously hard to prove. First suppose that $y \in f(A)$. By definition this gives us an $a \in A$ such that $f(a) = y$, so y is clearly an element of the right hand side.

Conversely, suppose that y is an element of the right hand side. This gives us an $a \in A$ such that $f(a) = y$. We know that $f(a) \in f(A)$, so $y = f(a)$ proves $y \in f(A)$ as desired. ■

Dual to the notion of the image of a set is the pre-image or inverse image of a set. This, too, can be defined formally.

24 Definition (Inverse Image)
Let $f : X \to Y$ be a function and let $B \subseteq Y$ be a subset. We define the inverse image (volledig origineel in Dutch) of B, denoted $f^{-1}(B)$, as follows:

$$f^{-1}(B) = \{ x \in X \mid f(x) \in B \} .$$

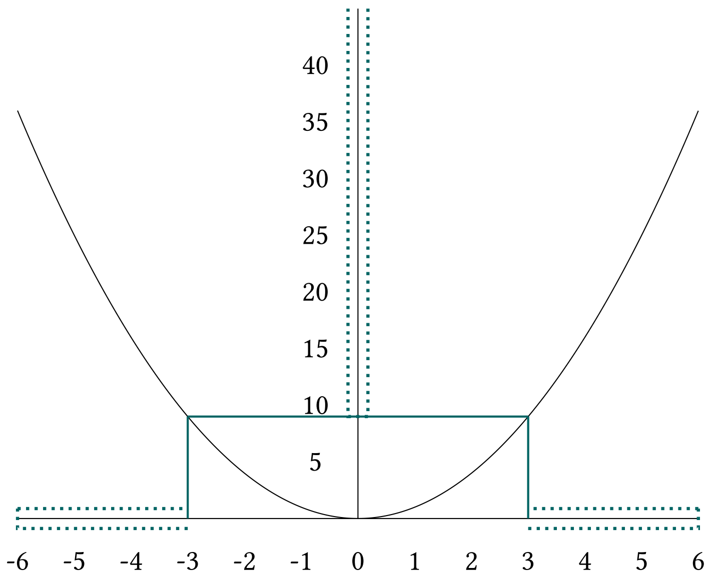

Figure 3.3: The function $f : \mathbb{R} \to \mathbb{R},\ x \mapsto x^2$ and an indication of $f^{-1}(\mathbb{R}_{\geq 9})$.

108 Example

Consider the function which embeds the natural numbers into the non-postive integers, that is to say, the function $f : \mathbb{N} \to \mathbb{Z}$ given by $f(n) = -n$ is $\mathbb{N}$. Its domain equals $\mathbb{N}$, its codomain is $\mathbb{Z}$ and its range is $\mathbb{Z}_{\leq 0}$. One can readily prove that

$$f\big(\{\, n \in \mathbb{N} \mid n \leq 7 \}\big) = \{\, n \in \mathbb{Z}_{\leq 0} \mid n \geq -7 \}\,.$$

Indeed, if $n \leq 7$ then $f(n) = -n \geq -7$. Conversely, if $n \in \mathbb{Z}_{\leq 0}$ and $n \geq 7$ then $-7 \leq n \leq 0$. This ensures that $0 \leq -n \leq 7$, and clearly $f(-n) = -(-n) = n$ as desired.

109 Example

The domain of the function $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = x^2$ is $\mathbb{R}$ and its range is $\mathbb{R}_{\geq 0}$. We can prove that

$$f^{-1}(\mathbb{R}_{\geq 9}) = \mathbb{R}_{\leq -3} \cup \mathbb{R}_{\geq 3}.$$

See Fig. 3.3 for a sketch of all this.

110 Example

The relation f on the set $X = \{-1, 0, 1\}$ given by Fig. 3.4 is actually a function on X. Its domain, codomain and range are all equal to X. For each $x \in X$ we have $f^{-1}\big(\{\{x\}\big) = \{-x\}$.

111 Example

Recall the set $\mathcal{L}_{\mathsf{PROP}}$ of all propositional formulae and mentioned once before in Example 23. The function $f(\varphi) = \neg\varphi$ is the function on $\mathcal{L}_{\mathsf{PROP}}$ that maps formulas to their negation. One can readily prove the following equation to hold.

$$f\Big(\{\varphi, \varphi \vee \psi\}\Big) = \{\neg\varphi, \neg(\varphi \vee \psi)\}$$

It will often be useful to look at the set of all functions between two sets. There is quite a bit of structure in these so-called function spaces, some of which we will investigate further.

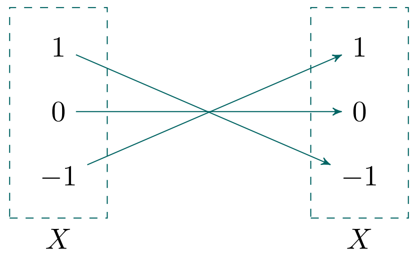

Figure 3.4: A function on $X = \{-1, 0, 1\}$.

25 Definition (Function Space)
Let X and Y be sets. We define the set Y^X, the function space between X and Y, as follows

$$Y^X = \{\, f \mid f \text{ is a function } f : X \to Y \,\} .$$

112 Example
The set of all the real functions on the reals is $\mathbb{R}^{\mathbb{R}}$. $\{0,1\}^{\mathbb{N}}$ 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.

113 Example (Functions from Nothing)
Let X be any set. One may wonder how many functions $f : \emptyset \to X$ exist. Fortunately one need not wonder for long, as Lemma 6 gives us a strong tool to deal with this.

Any function $f : \emptyset \to X$ is a relation $X \times \emptyset$, which by the aforementioned lemma is the empty set. Consequently, we know that f is empty, as you were asked to prove in Exercise 17. This means that each function $f : \emptyset \to X$ must equal, as a relation, the set $\emptyset$. Now note that $\emptyset$ is serial and deterministic as a relation between $\emptyset$ and X, so there exists precisely one function from $\emptyset$ to X.

The above can succinctly be summarized as saying that $X^{\emptyset}$ is a singleton. Recall that $\times$ behaves a bit like a product, with $\emptyset$ the analogue of zero and any singleton the analogue to one. Function spaces look a bit like exponentiation, as will be proven for finite sets in Theorem 3. This example gave the analogue to the law that $x^0 = 1$.

114 Example (Functions into Nothing)
There does not exist any function $f : X \to \emptyset$ when X is non-empty. Indeed, suppose that $f : X \to \emptyset$ were a function for some non-empty set X. Then f would be a serial relation between X and $\emptyset$. As X is non-empty, we have some $x \in X$. Seriality demands that there is some $y \in \emptyset$ such that $x \; f \; y$, a contradiction.

More intuitively, f must take a value at x. But there is space to take values in, as $\emptyset$ is quite empty. This neatly proves that $\emptyset^X = \emptyset$ for all $X \neq \emptyset$, analogous to the law that $0^x = 0$ for all $x \neq 0$.

115 Example
Let $\mathcal{W}$ be the set of finite sequences of 0's and 1's, and $f, g \in \mathcal{W}^{\mathcal{W}}$ given by $f(w) = 0w0$ and $g(w) = ww$. The range of f is all words that start and end with a 0, and the range of g are all words of even length.

The following theorem is left to you as Exercise 103, and shows that exponentiation and function spaces really do behave the same way when regarding finite sets.

3 Theorem
For finite sets X and Y the following equation holds

$$\left| Y^X \right| = |\, Y \,|^{|\, X \,|}$$

Recall that relations can be composed. The same is true for functions, and in fact, the composition of two functions is again a function. Intuitively, the composition of functions stands for the consecutive application of them. Let us first prove this assertion.

21 Lemma
Let $f : X \to Y$ and $g : Y \to Z$ be functions. The composition $g \circ f$ is a function $X \to Z$.

Proof. We need to prove that $g \circ f$ is serial and deterministic. First note that $g \circ f$ can quite easily be described. We already adopted the custom of writing $f(x)$ for the unique $y \in Y$ such that $x \; f \; y$. The same applies to g.

Now note that $x \; (g \circ f) \; z$ holds if and only if there is some $y \in Y$ such that $x \; f \; y$. But then $f(x) = y$ and $g(y) = z$, so $g(f(x)) = z$. This proves that $(g \circ f)(x) = g(f(x))$. Seriality and determinacy follow readily from this description. ■

Recall that in Lemma 18 we proved composition to be associative, so $f \circ (g \circ h) = (f \circ g) \circ h$ for functions f, g, h with appropriate domains and codomains. Consequently, we will drop the brackets whenever it suits us.

116 Example
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 $\sqrt{x} + 2$.

117 Example
Let $\mathcal{L}_{\mathsf{PROP}}$ be the set of propositional formulas, and $f, g \in \mathcal{L}_{\mathsf{PROP}}^{\mathcal{L}_{\mathsf{PROP}}}$ defined by $f(\varphi) = \neg\varphi$ and $g(\varphi) = \varphi \vee p$. Then $(g \circ f)(\varphi) = \neg\varphi \vee p$ and $(f \circ g)(\varphi) = \neg(\varphi \vee p)$.

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

119 Example
Let $\mathcal{W}$ be the set of finite sequences of 0's and 1's, and $f, g \in \mathcal{W}^{\mathcal{W}}$ given by $f(w) = 0w0$ and $g(w) = ww$. Then $gf(w) = 0w00w0$.

120 Example
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 $h \circ g \circ f = f$.

3.1 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

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

$$f : \mathbb{Z} \to \mathbb{Z} \quad f(n) = 7n.$$

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.

3.2 Injections, surjections and bijections

There are function that do not map different elements to the same element. For example, the function $f : \mathbb{N} \to \mathbb{N}$ with $f(n) = n + 1$ as discussed in Example 66 and 46. Such functions are called injections.

26 Definition (Injective)
A function $f : X \to Y$ is said to be injective when for all $a, b \in X$ we have $x = y$ whenever $f(x) = f(y)$.

121 Example
The identity function id_X is injective. Indeed, suppose that $a = f(a) = f(b) = b$, then $a = b$ holds as desired.

122 Example
The function $f : \mathbb{N} \to \mathbb{N},\ x \mapsto x + 1$ is injective. For suppose that $x + 1 = f(x) = f(y) = y + 1$. Subtracting 1 from both sides of the equality gives $x = y$, proving f to be injective.

123 Example
The function $f : \mathbb{R} \to \mathbb{R}, x \mapsto x^2$, as discussed in Example 109 is not injective at all. This can easily be seen, because

$$f(-1) = (-1)^2 = 1 = 1^2 = f(1)$$

holds whereas $1 = -1$ defininately does not.

This also nicely illustrates the importance of the domain of a function in the definition of injectivity. For whereas f is not injective, the function $g : \mathbb{R}_{\geq 0} \to \mathbb{R},\ x \mapsto x^2$ surely is.

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, $f(n) = 0$, is an example of this since $\mathrm{rng}(f) = \{0\} \subset \mathbb{N}$. Functions that do reach all of B are called surjections.

27 Definition (Surjection)
A function $f : X \to Y$ is said to be surjective for each $y \in Y$ there is a $x \in X$ such that $f(x) = y$.

There are many equivalent definitions of a surjection. Let us mention a two.

22 Lemma
Let $f : X \to Y$ be a function. The following are logically equivalent:

(i) f is a surjection

(ii) the range of f equals its codomain

Proof. First assume (i). To prove that $f(X) = Y$, we need to show that $f(X) \subseteq Y$ and $Y \subseteq f(X)$. Well, if $x \in X$ then $f(x) \in Y$ by definition, so the former certainly holds. To prove the latter, suppose $y \in Y$. Surjectivity ensures some $x \in X$ such that $f(x) = y$, and $f(x) \in f(X)$ certainly holds. This proves (ii).

Now assume (ii). Take some arbitrary $y \in Y$. Now we know that $y \in f(X)$ as $Y = f(X)$, so we get some $x \in X$ such that $f(x) = y$. This proves (i). ■

124 Example
The identity function $\mathrm{id}_X : X \to X$ is surjective. Indeed, each $x \in X$ is reached by x, because $\mathrm{id}_X(x) = x$.

125 Example
The function $f : \mathbb{Z} \to \mathbb{Q}$ with $f(n) = 1/n$ is not surjective. For suppose that it were, then there would have to be some $n \in \mathbb{N}$ such that $2 = \frac{1}{n}$. We derive that $1 = 2n$, a clear contradiction.

126 Example
The function f as define below is injective nor surjective.

$$f : \Big\{\{a,b\}, \{c\}, \{d\}\Big\} \to \Big\{0, 1, 2\Big\}, \qquad f\big(\{a,b\}\big) = 0 \text{ and } f\big(\{c\}\big) = f\big(\{d\}\big) = 2.$$

It is not injective because $\{c\}$ and $\{d\}$ are mapped to the same element. Its failure of surjectivity stems from the fact that there is no x such that $f(x) = 1$.

127 Example
Let R be an equivalence relation on some set X. Consider the canonical projection $p : X \to X/R$ as discussed in Example 107. This map certainly is surjective.

Due to Lemma 15 we know X/R to be a partition, every $A \in X/R$ contains at least one element. Moreover, if $a \in A$ then $[a] = A$ due to Lemma 14 and the fact that $a \in [a]$. This proves that $p(a) = A$, so p is surjective. In Exercise 125 you are asked to characterize those equivalence relations for which the canonical projection is injective.

128 Example
Let $\mathcal{L}_{\text{PROP}}$ be the set of propositional formulas, and let R be the equivalence relation discussed in Example 77 and 23. This relation was defined as

$$\varphi \; R \; \psi \text{ if and only if } \varphi \leftrightarrow \psi \text{ is a tautology.}$$

Consider $f \in \mathcal{L}_{\text{PROP}}^{\mathcal{L}_{\text{PROP}}}$ given by $f(\varphi) = \neg\varphi$ and the function g

$$g : \mathcal{L}_{\text{PROP}} \to \mathcal{L}_{\text{PROP}}/R, \quad \varphi \mapsto [\neg\varphi]\,.$$

Then f is injective, as for no two different formulas φ and ψ, $\neg\varphi$ equals $\neg\psi$. The function g on the other hand is not injective: $g(\varphi) = g(\neg\neg\varphi)$. Also note that f is not surjective, yet g is.

Observe that the surjectivity of a function depends on the choice of the codomain. 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.

The following characterization of surjections is quite beautiful. It describes what it means for a function to be surjective, purely in terms of equality and functions.

23 Lemma
A function $f : X \to Y$ is surjective if and only if for all functions $g, h : Y \to Z$ such that that $g \circ f = h \circ f$ we have $g = h$.

Proof. Assume that f is surjective, and let $g, h : Y \to Z$ be functions such that $g \circ f = h \circ f$. To prove $g = h$ we prove that $g(y) = h(y)$ for all $y \in Y$. By surjectivity we know that to each such y there exists a $x \in X$ with $f(x) = y$. Now observe that

$$g(y) = g(f(x)) = (g \circ f)(x) = (h \circ f)(x) = h(f(x)) = h(y),$$

proving the desired.

We now prove the other direction. We assume that for all functions $g, h : Y \to Z$ such that $g \circ f = h \circ f$ we actually have $g = h$. To reach the desired we reason by contradiction, so assume that f is not surjective. This gives us some $y \in Y$ such that $y \neq f(x)$ for all $x \in X$. Now consider the functions $g, h : Y \to \{0, 1\}$ defined by

$$g(a) = \begin{cases} 0 & \text{if } a = y \\ 1 & \text{otherwise} \end{cases}, \qquad h(a) = 1.$$

Note that $g(y) = 0 \neq 1 = h(y)$, so g and h are not equal. But for all $x \in X$ we have $(g \circ f)(x) = (h \circ f)(x)$, so $g \circ f = h \circ f$. This gives a contradiction, so g must be surjective. ■

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

129 Example
The function $f(x) = x - 1$ on the reals is bijective.

130 Example
The function $f : \mathbb{N} \to \mathbb{N}$ given by $f(n) = n + 7$ is not bijective, as it is not surjective. This is easily seen; no number between 0 and 6 is in the range of f.

131 Example
Let $\mathcal{W}_n$ be the set of finite sequences of 0's and 1's of length n, and let $\{a_1, \ldots, a_n\}$ be a finite set. The function $f : \mathcal{W} \to P(A)$ given by

$$f(w) = \{a_i \in A \mid w_i = 1\},$$

where w_i is the i-th element of w, is a bijection. You will be asked to prove this in Exercise 105.

132 Example
Let X and Y both be singletons. The set $X \times Y$ as a relation between X and Y is serial and deterministic, so it is a function. Moreover, it is both injective and surjective. This proves that all singletons are in bijection with one another.

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 $f : X \to Y$ is a bijection, then we can define the function $g : Y \to X$ by setting $g(y) = x$ if and only if $f(x) = y$ for each $x \in X$ and $y \in Y$. Note that then the following equalities hold.

$$f \circ g = \mathrm{id}_B \text{ and } g \circ f = \mathrm{id}_A \tag{3.1}$$

For example, 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.

4 Theorem

A function $f : A \to B$ is bijective if and only if there exists a function $g : B \to A$ such that (4.1) holds.

Proof. We have to prove two implications, let us start with the implication from left to right. Assume that $f : A \to B$ is bijective. We need to prove the existence of a function $g : B \to A$ satisfying all constraints. Recall that functions are sets of pairs, that is, $f \subseteq A \times B$. Therefore we can define g according to the intuition of "turning f around":

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

We have to show that g is a function from B to A and that (4.1) holds. This is left to you as Exercise 111

We now skip to the other direction. We assume the existence of a function $g : B \to A$ such that (4.1) holds. Our goal is to prove that f is both injective and surjective. But this follows directly from Exercise 123, so we are done. ∎

24 Lemma

Let $f : A \to B$ and $g_1, g_2 : B \to A$ be functions such that f and g_1 together satisfy (4.1), as to f and g_2. Now $g_1 = g_2$.

Proof. We simply compute as follows

$$g_1 = g_2 \circ \mathrm{id}_B = g_2 \circ (f \circ g_1) = (g_2 \circ f) \circ g_1 = \mathrm{id}_A \circ g_1 = g_1.$$

The first equality follows from Example 99, the second is (4.1). The equality in the middle is associativity of composition, proven in Lemma 18. We finish the proof by applying (4.1) and Example 99 once again. ∎

If $f : A \to B$ is a bijection, we write $f^{-1} : B \to A$ for the inverse, fulfilling the role of g in (4.1). By the above Theorem 4 we know such a function to exist, and Lemma 24 guarantees us that there is but one inverse.

133 Example

The inverse of id_X is id_X again. Formulated in symbols, $\mathrm{id}_X^{-1} = \mathrm{id}_X$.

134 Example

Let X be the set $\{\, n \in \mathbb{N} \mid \text{there exists an } m \in \mathbb{N} \text{ such that } 2m = n\}$. Consider the function f defined as

$$f : \mathbb{N} \to X, \quad x \mapsto 2x.$$

Its inverse $f^{-1} : X \to \mathbb{N}$ is given by $f^{-1}(x) = \frac{1}{2}x$.

135 Example

The inverse of the function $\sqrt{x}$ on the positive reals $\mathbb{R}_{\geq 0}$ is the function x^2.

136 Example

The only bijections on $\{0, 1\}$ are $\{\langle 0, 0\rangle, \langle 1, 1\rangle\}$ and $\{\langle 0, 1\rangle, \langle 1, 0\rangle\}$. Note that there are no injections on this set except bijections.

3.3 Exercises

94 Exercise
Give a set-notation for the function that maps real numbers m different from 0 to their multiplicative inverse, and 0 to 0. What are the domain and range of this function?

95 Exercise
What is the domain and what is the range of the function $f : n \mapsto 7n$ on the natural numbers?

96 Exercise
Consider the function $f(x) = \sqrt{x}$ on the positive reals. Write down its set-notation. What is the image of $\mathbb{R}_{\geq 4}$ under f? And what is $f^{-1}(\mathbb{R}_{\leq 4})$?

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

98 Exercise
Show that the number of functions from $\{0, 1\}$ to $\{0, 1\}$, i.e. the size of $\{0, 1\}^{\{0,1\}}$, is 2^2, by giving all the functions explicitly, as sets.

99 Exercise
Given functions $f, g : \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}$ defined by $f(x) = \sqrt{x}$ and $g(x) = x^3$, describe the functions $f \circ g$ and $g \circ f$.

100 Exercise
Let $\mathcal{W}$ be the set of finite sequences of 0's and 1's, and $f, g \in \mathcal{W}^{\mathcal{W}}$ given by $f(w) = www$ and $g(w) = ww^R$, where w^R is the reverse of w. Give domain and range of these functions, and gf and fg.

101 Exercise
Let $\mathcal{W}$ be the set of finite sequences of 0's and 1's, and $f, g \in \mathcal{W}^{\mathcal{W}}$ given by $f(w) = ww$ and $g(w) = w^R$, does $fg = gf$ hold? Prove your answer.

102 Exercise
Let $\mathcal{L}_{\mathsf{PROP}}$ be the set of propositional formulas, and consider the functions $f(\varphi) = \varphi \to p$ and $g(\varphi) = p \to \varphi$ on $\mathcal{L}_{\mathsf{PROP}}$. Give $f \circ g$ and $g \circ f$. Are there φ for which $(f \circ g)(\varphi) \leftrightarrow (g \circ f)(\varphi)$? Prove your answer.

103 Exercise
Prove Theorem 3.

104 Exercise
Consider the function $f : \mathbb{Z} \to \mathbb{Z}$ defined by $f(n) = n+1$. Prove or disprove:

(i) The function f is surjective.

(ii) The function $g : \mathbb{N} \to \mathbb{N}$ defined as $g(n) = n + 1$ is surjective.

105 Exercise

Let $\mathcal{W}_n$ be the set of finite sequences of 0's and 1's of length n, and let $\{a_1, \ldots, a_n\}$ be a finite set. The function $f : \mathcal{W} \to P(A)$ is given by

$$f(w) = \{a_i \in A \mid w_i = 1\},$$

where w_i is the i-th element of w. Prove that f is a bijection.

106 Exercise

Consider the the exponentiation function $f : \mathbb{R} \to \mathbb{R},\ x \mapsto 2^x$.

(i) Is the function f injective;

(ii) Is it surjective?

(iii) Describe the image of $\{\, x \in \mathbb{R} \mid -2 \leq x \leq 2\}$ under f;

(iv) Describe the inverse image of $\{\, x \in \mathbb{R} \mid 4 \leq x \leq 16\}$ under f.

107 Exercise

Let $\{a_1, \ldots, a_n\}$ be a finite set, let $p_1, \ldots, p_n$ be n propositional variables, and let $\mathcal{P}$ be the set of all propositional formulas in $p_1, \ldots, p_n$ and $\perp$. The function f is given by:

$$f : \mathcal{P}(A) \to \mathcal{P}, \quad X \mapsto \begin{cases} \perp & \text{if } X \text{ is empty} \\ \displaystyle\bigwedge_{a_i \in X} p_i & \text{otherwise,} \end{cases}$$

where $\bigwedge_{a_i \in X} p_i$ denotes the conjunction of those p_i for which $a_i \in X$.

For example, $f(\{a_1, a_7\}) = p_1 \wedge p_7$ and $f(\emptyset) = \perp$. Prove that f is an injection, but not a bijection.

108 Exercise

We continue from Exercise 107 and define a function

$$g : \mathcal{P}(A) \to \mathcal{P}, \quad X \mapsto \begin{cases} \perp & \text{if } X \text{ is empty} \\ p_i & \text{if } i \text{ is the smallest number with } a_i \in X \end{cases}$$

Is g an injection or a surjection?

109 Exercise

Are the sine and cosine functions on the real numbers injective? And surjective?

110 Exercise

Let X be a non-empty set and let Y be a singleton. Prove that each function $f : X \to Y$ is a surjection. Describe those sets X such that each function $f : X \to Y$ with Y a singleton is an injection.

111 Exercise

Look again at the situation of Theorem 4. Prove that the relation g constructed in the first half of the proof is actually a function, and that (4.1) is satisfied.

112 Exercise

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

113 Exercise

Let $f : X \to Y$ be a function. Prove that the function $g : X \to \text{rng}(f)$ defined as $g(x) = f(x)$ for all $x \in X$ is a bijection whenever f is an injection.

114 Exercise

Prove that all injections on a finite set X are bijections.

115 Exercise

Let $f : X \to Y$ be an injection, and assume that $|Y| = |X|$. Prove that f is a bijection.

116 Exercise

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 reals to -1.

117 Exercise

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

118 Exercise

Let $f : X \to Y$ be a function. We define a relation $\equiv$ on X as

$$a \equiv b \text{ if and only if } f(x) = f(y).$$

Prove the following:

(i) The relation $\equiv$ is an equivalence relation on X;

(ii) There is an injection $X/{\equiv} \to Y$.

119 Exercise

Show that for finite sets X there is no surjection from X to $\mathcal{P}(X)$.

120 Exercise

Given a function $f : \mathbb{N} \to X$, what properties does f have to satisfy in order for $g : A \to \mathbb{N}$ given by $g(a) = \min_{n \in \mathbb{N}} f(n) = a$, to be a function?

121 Exercise

Prove that the composition of two injective functions $f : X \to Y$ and $g : Y \to Z$ is injective.

122 Exercise

In this exercise we do the analogue of Lemma 23 for injective functions. Prove that $f : X \to Y$ is injective if and only if for all functions $g, h : Z \to X$ such that $f \circ g = f \circ h$ we have $g = h$.

123 Exercise

Let $f : X \to Y$ and $g : Y \to X$ be functions. Prove that if $f \circ g = \mathrm{id}_Y$ then f is surjective and g is injective.

Hint: Use Exercise 122 and Lemma 23.

124 Exercise (Cantor Pairing is Bijective)

Recall the function $\mathbb{N} \times \mathbb{N} \to \mathbb{N}$ from Exercise 124. Prove that this function is a bijection.

125 Exercise (Injective Canonical Projections)

Let R be an equivalence relation on some set X. Recall the canonical projection $p : X \to X/R$ as discussed in Example 107 and 127. Prove that R is injective if and only if $R = \mathrm{id}_X$.

Answers

Below answers to selected exercises. These answers are merely suggestions of a potential answer, there are often numerous distinct yet correct answers. Do not read the solutions before solving the exercises yourself. It is quite possible, probable even, that there are some mistakes below. If you stumble upon something strange or wrong, please notify the lecturer.

1 Answer (Set Notation)

The set of squares of natural numbers is

$$\left\{ n \in \mathbb{N} \;\middle|\; \text{there is a } m \in \mathbb{N} \text{ with } n = m^2 \right\}.$$

2 Answer (Divisibility)

Three ways to write the sets of non-negative integers divisible by three are:

$$\left\{ n \in \mathbb{N} \;\middle|\; \text{there is a } m \in \mathbb{N} \text{ with } n = 3m \right\}, \left\{ n \in \mathbb{N} \;\middle|\; \frac{n}{3} \in \mathbb{N} \right\}, \left\{ 0, 3, 6, 9, 12, \ldots \right\}$$

3 Answer (More Set Notation)

The set in (i) is the set of rational numbers strictly between 0 and 1. The set of real numbers that are the square of a rational number is described in (ii). Note that this is the same set as

$$\left\{ x \in \mathbb{Q} \;\middle|\; \exists y \in \mathbb{Q}.\, x = y^2 \right\},$$

as the square of a rational number is rational. In (iii) we described the set of real numbers that are the square of a rational number bigger than 2. This is equal to the set of real numbers bigger than 4 that are the square of a rational number. Finally, (iv) consists of all natural numbers whose square is strictly larger than the number itself. This is the same as the set $\mathbb{N}_{\geq 2} = \{2, 3, 4, \ldots\}$.

6 Answer (Elements & Counting)

The statement $\{0\} \in \mathbb{N}$ is false. Indeed, $\{0\}$ is not a natural number, so it is not an element of the set of natural numbers. The statement $\{0\} \subseteq \mathbb{N}$ would have been true. The set $\{\{\mathbb{N}\}\}$ has exactly one element, namely the set $\{\mathbb{N}\}$. This set, in turn, has exactly one element, the set $\mathbb{N}$.

8 Answer (Non-Empty)

Lemma

Let X be any set. If $X \neq \emptyset$ then there is some x such that $x \in X$.

Proof. We proceed by contraposition. Suppose that there is no x such that $x \in X$. With this assumption we can prove that $X = \emptyset$. This proof can be done directly via extensionality.

Let y be arbitrary. It is never the case that $y \in \emptyset$, so for all $y \in \emptyset$ anything goes. In particular, if $y \in \emptyset$ then $y \in X$. Conversely, if $y \in X$ then we reach a contradiction with the assumption that there is no element in X. Again, from a contradiction we may conclude anything at all, so if $y \in X$ then $y \in \emptyset$ is valid.

This proves that $y \in X$ if and only if $y \in \emptyset$, whence $X = \emptyset$. ∎

10 Answer (Properties of Intersection)

Lemma (Exercise 10.(i))
Let X be an arbitrary set. Now $X \cap X = X$.

Proof. Let x be arbitrary. If $x \in X \cap X$ then $x \in X$ and $x \in X$. In particular $x \in X$ holds. Conversely, if $x \in X$ holds then $x \in X$ and $x \in X$, so $x \in X \cap X$. This proves the desired via extensionality. ∎

Lemma (Exercise 10.(ii))
Let X be an arbitrary set. Now $X \cap \emptyset = \emptyset$.

Proof. We prove this via Lemma 3. It is clear that $\emptyset \subseteq X \cap \emptyset$, so we need only prove the other direction.

Let x be such that $x \in X \cap \emptyset$. This ensures that $x \in X$ and $x \in \emptyset$. The latter is what we meant to derive. This proves that $X \cap \emptyset \subseteq \emptyset$, finishing the proof. ∎

Lemma (Exercise 10.(iii))
Let X and Y be sets such that $X \subseteq Y$. Now $X \cap Y = X$.

Proof. We proceed via Lemma 3. To prove $X \cap Y \subseteq X$, assume that $x \in X \cap Y$. This immediately yields $x \in X$ and $x \in Y$, proving $x \in X$ as desired.

To prove that $X \subseteq X \cap Y$, assume $x \in X$. From the assumption $X \subseteq Y$ we derive that $x \in Y$. We now know that $x \in X$ and $x \in Y$, so $x \in X \cap Y$ must follow. This completes the proof. ∎

12 Answer (Distributive Laws)

Lemma
Let A, B and C be arbitrary sets. Now $(A \cap B) \cup C = (A \cup C) \cap (B \cup C)$ holds.

Proof. We prove this using Lemma 3. First we prove that $(A \cap B) \cup C \subseteq (A \cup C) \cap (B \cup C)$. So let $x \in (A \cap B) \cup C$ be arbitrary. This entails that $x \in A \cap B$ or $x \in C$. Let us treat the latter case first. We now know that $x \in C$, so it certainly is true that $x \in A$ or $x \in C$. Likewise, $x \in B$ or $x \in C$ holds. These two facts entail that $x \in A \cup C$ and $x \in B \cup C$. From this we in turn can conclude $x \in (A \cup C) \cap (B \cup C)$.

We now cover the case where $x \in A \cap B$. It follows that $x \in A$ and $x \in B$. From these observations we derive that $x \in A$ or $x \in C$, and similarly we see that $x \in B$ or $x \in C$. Analogous to the above argument this proves $x \in (A \cup C) \cap (B \cup C)$ This completes the proof of $(A \cap B) \cup C \subseteq (A \cup C) \cap (B \cup C)$.

We now prove that $(A \cup C) \cap (B \cup C) \subseteq (A \cap B) \cup C$. Assume that $x \in (A \cup C) \cap (B \cup C)$. This means that $x \in A \cup C$ and $x \in B \cup C$. There are four cases to consider here: $x \in A$ and $x \in B$, $x \in A$ and $x \in C$, $x \in C$ and $x \in B$ and finally $x \in C$ and $x \in C$. In the first case we see that $x \in A \cap B$, and in the other cases we conclude that $x \in C$. Both of these entail that $x \in (A \cap B) \cup C$, proving the desired. ∎

14 Answer (Symmetry)

The first two equalities hold, the last one does not hold. Formal proofs attesting to these facts follow below.

Lemma
Let A and B be sets. Now $A \cap B = B \cap A$.

Proof. We prove equality via extensionality. To this end, let x be arbitrary. Suppose that $x \in A \cap B$. Then $x \in A$ and $x \in B$. This entails that $x \in B$ and $x \in A$, so $x \in B \cap A$ follows.

Conversely, suppose that $x \in B \cap A$. Then $x \in B$ and $x \in A$. This entails that $x \in A$ and $x \in B$, so $x \in A \cap B$ follows. ∎

Lemma
Let A and B be sets. Now $A \cup B = B \cup A$.

Proof. We prove this via Lemma 3. To prove that $A \cup B \subseteq B \cup A$, let $x \in A \cup B$ be arbitrary. This entails that $x \in A$ or $x \in B$. In the first case we know that $x \in A$, so $x \in B$ or $x \in A$ certainly holds. In the second case we know $x \in B$, so $x \in B$ or $x \in A$ holds as well. In both cases we know enough to conclude that $x \in B \cup A$, so $x \in B \cup A$ follows. As the other direction is analogous we omit it here. ∎

Lemma
There exist sets A and B such that $A \setminus B \neq B \setminus A$.

Proof. Take $A = \{\emptyset\}$ and $B = \emptyset$. We can now compute:

$$\begin{array}{lllllll} A \setminus B & = & \{x \in A \mid x \notin B\} & = & \{x \in \{\emptyset\} \mid x \notin \emptyset\} & = & \{\emptyset\}, \\ B \setminus A & = & \{x \in B \mid x \notin A\} & = & \{x \in \emptyset \mid x \notin \{\emptyset\}\} & = & \emptyset. \end{array}$$

It is quite clear that $\{\emptyset\} \neq \emptyset$, proving the stated. ∎

16 Answer (More Properties of Difference)

Lemma (Exercise 16.(i))
Let X and Y be sets. If $X \subseteq Y$ then $X \cup (Y \setminus X) = Y$.

Proof. As usual, we proceed via Lemma 3. To prove that $X \cup (Y \setminus X) \subseteq Y$, let $a \in X \cup (Y \setminus X)$ be arbitrary. This entails that either $a \in X$ or $a \in Y \setminus X$. In the first case we obtain $a \in Y$ via $X \subseteq Y$. In the second case, note that $a \in Y$ and $a \notin X$, so $a \in Y$ definitely holds.

To prove the other inclusion, let $a \in Y$ be arbitrary. We distinguish two cases, either $a \in X$ or $a \notin X$. In the former case $a \in X$ holds, so $a \in X \cup (Y \setminus X)$ is immediate. In the latter case we observe that $a \in Y$ and $a \notin X$, so $a \in Y \setminus X$. This in turn entails $a \in X \cup (Y \setminus X)$, proving the desired. ∎

20 Answer (Some More Distributivity)

Lemma

Let A and B be arbitrary sets. The following equality holds:

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

Proof. As is so often the case, we proceed by Lemma 3. Let $z \in A \cap \bigcup B$ be arbitrary. This ensures that $z \in A$ and $z \in \bigcup B$. The latter means that $z \in b$ for some $b \in B$. Pick such a $b \in B$, and note that $z \in b \cap A$. As a consequence we see that $z \in \bigcup \{\, x \cap A \mid x \in B \,\}$. This line of reasoning proved the inclusion from left to right.

Let us now focus on the inclusion from right to left. To prove it, let $z \in \bigcup \{\, x \cap A \mid x \in B \,\}$ be arbitrary. By definition we know of some $y \in \{\, x \cap A \mid x \in B \,\}$ such that $z \in y$. Again by definition it follows that $y = x \cap A$ for some $x \in B$. To re-iterate, we know that $z \in x \cap A$, so $z \in x$ for some $x \in B$ and $z \in A$. From this we can conclude that $z \in \bigcup B$, and remember that $z \in A$. These two facts ensure that $z \in A \cap \bigcup B$, proving the desired inclusion. ■

22 Answer (Empty Subset)

Lemma

Let A be a set. Now $\emptyset \subseteq A$ holds.

Proof. We need only to prove that for all $x \in \emptyset$ we know $x \in A$. But there are no such x, whence we are immediately done. ■

Note that with this small piece of data we can immediately re-prove many of the earlier exercises. This is a a nice methods to generate exercise and understanding. For example, Exercise 10.(ii) may be proven from the above observation, Exercise 10.(ii) and Exercise 14.

Lemma

Let X be any set. Now $X \cap \emptyset = \emptyset$.

Proof. By Exercise 10.(iii) we know that if $A \subseteq B$ then $A \cap B = A$. We know that $\emptyset \subseteq X$ holds, so $\emptyset \cap X = \emptyset$ must hold as well. The desired follows from $\emptyset \cap X = X \cap \emptyset$, as was proven in greater generality in Exercise 14. ■

23 Answer (Powerset of Empty Set)

We know that $\emptyset \subseteq \emptyset$ for at least two reasons, both follow from Exercise 26. Any $X \in \mathcal{P}(\emptyset)$ satisfies $X \subseteq \emptyset$. But as we know that $\emptyset \subseteq X$, this would entail $X = \emptyset$ by Lemma 3. Consequently, the only element of $\mathcal{P}(\emptyset)$ is $\emptyset$.

24 Answer (Describing the Powerset)

The powerset is described below, this set clearly has 4 elements.

$$\mathcal{P}(\{\text{appel}, \text{moes}\}) = \big\{\emptyset, \{\text{appel}\}, \{\text{moes}\}, \{\text{appel}, \text{moes}\}\big\}$$

25 Answer (Subsets)

A comprehensive listing of the subsets of $\{1,2,3,4\}$ follows below, it consists of precisely $2^4 = 16$ sets. $\emptyset$, $\{1\}$, $\{2\}$, $\{3\}$, $\{4\}$, $\{1,2\}$, $\{1,3\}$, $\{1,4\}$, $\{2,3\}$, $\{2,4\}$, $\{3,4\}$, $\{1,2,3\}$, $\{1,2,4\}$, $\{1,3,4\}$, $\{2,3,4\}$, $\{1,2,3,4\}$.

26 Answer (Elements of the Powerset)

By Exercise 22 we know that $\emptyset \subseteq X$ for any set X. This ensures that $\emptyset \in \mathcal{P}(X)$ also holds. The set X also is an element of $\mathcal{P}(X)$, because $X \subseteq X$ holds for any set. Indeed, suppose that $x \in X$, then $x \in X$ follows.

35 Answer (Inequality Reflected in Powerset)

We give two different proofs of the exercise. The first proof proceeds via already derived generalities on subsets, whereas the second proof directly unravels what it means to "not be equal". Both are equally valid arguments.

Lemma
Let X and Y be sets. If $X \neq Y$, then $\mathcal{P}(X) \neq \mathcal{P}(Y)$.

Proof (Proof via Generalities). Assume that $X \neq Y$. We furthermore assume that $\mathcal{P}(X) = \mathcal{P}(Y)$ holds, and derive a contradiction from this, thus forcing the conclusion that $\mathcal{P}(X) \neq \mathcal{P}(Y)$ must hold. Note that $X \in \mathcal{P}(X)$ and $Y \in \mathcal{P}(Y)$, as proven in Exercise 26. By our assumption that $\mathcal{P}(X) = \mathcal{P}(Y)$ we now see that $X \in \mathcal{P}(Y)$ and $Y \in \mathcal{P}(X)$. Expanding the definition of the powerset now yields $X \subseteq Y$ and $Y \subseteq X$. By the ever so familiar Lemma 3 we now know that $X = Y$, a contradiction. ■

Proof (Proof via Intricacies). Assume that $X \neq Y$. From this we derive that there is some z such that either $z \in X$ and $z \notin Y$ or $z \notin X$ and $z \in Y$.

In the first case we see that $\{z\} \subseteq X$, so $\{z\} \in \mathcal{P}(X)$. But $\{z\} \in \mathcal{P}(Y)$ can not possibly hold, for this would entail that $z \in Y$ which we know to be false. We now know of a set, namely $\{z\}$, which is an element of $\mathcal{P}(X)$ but not an element of $\mathcal{P}(Y)$. This means that $\mathcal{P}(X) \neq \mathcal{P}(Y)$.

The argument in the second case is analogous. Indeed, observe that $\{z\} \in \mathcal{P}(Y)$ but $\{z\} \notin \mathcal{P}(X)$, proving $\mathcal{P}(X) \neq \mathcal{P}(Y)$ as desired. ■

37 Answer (Intersections)

Lemma (Exercise 37.(i))
Let X and Y be sets. The equality $\bigcap\{X,Y\} = X \cap Y$ holds.

Proof. We proceed via Lemma 3. Assume that $a \in \bigcap\{X,Y\}$. This simply means that $a \in b$ for all $b \in \{X,Y\}$. Unfolding this yields $a \in X$ and $a \in Y$. But this entails $a \in X \cap Y$. This line of reasoning proves $\bigcap\{X,Y\} \subseteq X \cap Y$.

Now to prove that $X \cap Y \subseteq \bigcap\{X,Y\}$, take an arbitrary $a \in X \cap Y$. Unfolding the definition tells us that $a \in X$ and $a \in Y$. But this means that for all $b \in \{X,Y\}$ we have that $a \in b$. So $a \in \bigcap\{X,Y\}$ as desired. ■

Lemma (Exercise 37.(ii))
Let X and Y be sets, and assume X to be non-empty. The equality below holds.

$$Y \cup \bigcap X = \bigcap \{ x \cup Y \mid x \in X \}$$

Proof (Proof with Contraposition). We again proceed via Lemma 3. To prove that $Y \cup \bigcap X \subseteq \bigcap \{ x \cup Y \mid x \in X \}$, let $a \in Y \cup \bigcap X$ be arbitrary. We know that $a \in Y$ or $a \in \bigcup X$.

We want to prove that $a \in \bigcap \{ x \cup Y \mid x \in X \}$. By definition, this holds when $a \in x \cup Y$ for all $x \in X$. There are two cases to consider. In the first case, we know that $a \in Y$, so $a \in x \cup Y$ holds for any $x \in X$. In the second case we first unfold $a \in \bigcap X$ to see that $a \in x$ holds for all $x \in X$. From this we derive that for any $x \in X$ one has $a \in x \cup Y$. This proves that $a \in \bigcap \{ x \cup Y \mid x \in X \}$ as desired.

Now to prove the other direction, we proceed by contraposition. That is, we prove that if $a \notin Y \cup \bigcap X$ then $a \notin \bigcap \{ x \cup Y \mid x \in X \}$. So let a be such that $a \notin Y \cup \bigcap X$. This means that a is neither an element of Y nor an element of $\bigcap X$. In symbols, $a \notin Y$ and $a \notin \bigcap X$. The latter statement means that there is some $b \in X$ such that $a \notin b$. For suppose there would be no such b, then $a \in x$ holds for all $x \in X$. But then $a \in \bigcap X$, which we know not to be the case.

To re-iterate, we know that $a \notin Y$, and we know that there exists at least some $b \in X$ such that $a \notin b$. Fix such a b, and and see that $a \notin b \cup Y$. Now if $a \in \bigcap \{ x \cup Y \mid x \in X \}$ were to hold, it would follow that $a \in x \cup Y$ for all $x \in X$. In particular, $a \in b \cup Y$ must hold. But this is blatantly false, as we just demonstrated.

We now have proven that if $a \notin Y \cup \bigcap X$ then $a \notin \bigcap \{ x \cup Y \mid x \in X \}$. This fact comes in handy when proving $\bigcap \{ x \cup Y \mid x \in X \} \subseteq Y \cup \bigcap X$. Let $a \in \bigcap \{ x \cup Y \mid x \in X \}$ be arbitrary. There are two cases, either $a \in Y \cup \bigcap X$ or $a \notin Y \cup \bigcap X$. If the latter case were to hold, then by the previously proven we know $a \notin \bigcap \{ x \cup Y \mid x \in X \}$. This is a clear contradiction with our assumption, so this case never holds. We are thus left with the case that $a \in Y \cup \bigcap X$, which is what we wanted to prove. ■

Proof. Let us prove $\bigcap \{ x \cup Y \mid x \in X \} \subseteq Y \cup \bigcap X$ in a different way. Take $a \in \bigcap \{ x \cup Y \mid x \in X \}$ to be arbitrary. We distinguish two cases, either $a \in \bigcap X$ or $a \notin \bigcap X$. In the first case we immediately are done, because here it is clear that $a \in Y \cup \bigcap X$.

In the second case we know of a $b \in X$ such that $x \notin b$. For if no such b existed we knew that $a \in x$ for all $x \in X$, which is not the case. But by assumption we know that $a \in \bigcap \{ x \cup Y \mid x \in X \}$, so it follows that $a \in b \cup Y$ as $b \in X$. From $a \in b \cup Y$ we again get two cases, either $a \in b$ or $a \in Y$. In the former case we have $a \in b$, which contradicts the already derived fact that $a \notin b$, so this case never holds. The latter case shows that $a \in Y$, so $a \in Y \cup \bigcap X$ clearly holds. In all (possible) cases we have reached the desired conclusion, thus proving the inclusion to hold. ■

Lemma (Exercise 37.(iii))
Let X and A be sets. If $A \in X$ then $\bigcap X \subseteq A$.

Proof. Let $a \in \bigcap X$ be arbitrary. By definition we know that $a \in x$ for all $x \in X$. We also know that $A \in X$. These facts conspire to prove that $a \in A$, which is what we needed to show. ■

38 Answer (Writing out the Cartesian Product)
The set $\{a,b\}\times\{a,c,d\}$ consists of the elements $\langle\, a,a\,\rangle$, $\langle\, a,c\,\rangle$, $\langle\, a,d\,\rangle$, $\langle\, b,a\,\rangle$, $\langle\, b,c\,\rangle$ and $\langle\, b,d\,\rangle$.

39 Answer (Coding Pairs)
Lemma
Let a, b, c and d be arbitrary. Now $\langle\, a,b\,\rangle = \langle\, c,d\,\rangle$ holds precisely if $a=c$ and $b=d$.

Proof. The direction from right to left is immediate, so we focus on the proof from left to right. Assume that $\langle\, a,b\,\rangle = \langle\, c,d\,\rangle$. It follows that

$$\big\{\{a\},\{a,b\}\big\} = \langle\, a,b\,\rangle = \langle\, c,d\,\rangle = \big\{\{c\},\{c,d\}\big\}.$$

Let us distinguish two cases, namely $a=b$ and $a\neq b$. In the former case, the left-hand side equals $\big\{\{a\},\{a,a\}\big\} = \{\{a\}\}$. We now know that $\{c\}$ and $\{c,d\}$ are elements of $\big\{\{a\}\big\}$, which entails that $\{c\}=\{a\}=\{c,d\}$. From this we gather that $c=a=d$, proving the desired.

Now consider the second case, where $a\neq b$. We know that $\{c\}\in\big\{\{a\},\{a,b\}\big\}$, which means $\{c\} = \{a\}$ or $\{c\}=\{a,b\}$. The latter is impossible, for if it would hold then $a=c=b$ would follow, contradicting $a\neq b$. This means that $a=c$ must hold. We also know that $\{c,d\}\in\big\{\{a\},\{a,b\}\big\}$. Again there are two options, $\{c,d\}=\{a\}$ and $\{c,d\}=\{a,b\}$.

In the former case, $c=d$ follows. But as $\{a,b\}\in\big\{\{c\},\{c,d\}\big\}=\big\{\{c\}\big\}$ this would entails $a=b$, which is impossible. So this case can be safely excluded. The latter case entails that $d=a$ or $d=b$. If $d=a$ then $\{a\}=\{a,a\}=\{c,d\}=\{a,b\}$ would entail $b=a$, which remains impossible still. So $b=d$ must follow. We already know $a=b$, so this completes the proof. ■

40 Answer (Other Codings)
These codings are inappropriate because the order is lost; there is no difference between a code for the pair a, b and the pair b, c.

44 Answer (Identity in the Plane)
The set $\{\,\langle\, x,y\,\rangle \mid x=y\}$ is the diagonal line through the origin.

45 Answer (Triples)
The relation can be given as the set

$$\big\{\,\langle\, x,y,z\,\rangle \in \mathbb{Z}\times\mathbb{Z}\times\mathbb{Z} \;\big|\; x^2+y^2=z^2\big\}\,.$$

This relation has arity three, that is to say, it is a ternary relation. Two elements are $\langle\, 0,0,0\,\rangle$ and $\langle\, 3,4,5\,\rangle$, as one can readily verify through some minor computations.

49 Answer (Subset Relation is Transitive)
Lemma
Let X be any set. The relation $\subseteq$ on $\mathcal{P}(X)$ is transitive.

Proof. Suppose that $A,B,C\in\mathcal{P}(X)$ are such that $A\subseteq B$ an $B\subseteq C$. We need but prove that $A\subseteq C$. To this end, let $x\in A$ be arbitrary. By $A\subseteq B$ we know that $x\in B$. Similarly, $B\subseteq C$ ensures that $x\in C$. This is precisely what we needed to prove. ■

52 Answer (Union and Transitivity)

The statement is false. We prove the existence of a counter example.

Lemma

There exists a set X and transitive relations R and S on X such that the relation $R \cup S$ is not transitive.

Proof. Take X to be the set $\{1, 2, 3\}$ and define $R = \{\langle 1, 2 \rangle\}$ and $S = \{\langle 2, 3 \rangle\}$. Suppose that the relation

$$T = R \cup S = \{\langle 1, 2 \rangle, \langle 2, 3 \rangle\}$$

were transitive. We know that $1 \ R \ 2$ so $1 \ T \ 2$ follows. We also know $2 \ S \ 3$, so $2 \ T \ 3$ follows. Transitivity ensures that $1 \ T \ 3$. But this means that $1 \ R \ 3$ or $1 \ S \ 3$, both of which are false. We reached a contradiction, proving T to not be transitive, as desired. ■

53 Answer (Euclidian Both Ways)

Lemma

Let R be an euclidean relations R on a set X. The following holds:

$$\text{for all } a, b, c \in X, \text{ if } a \ R \ b \text{ and } a \ R \ c \text{ then } b \ R \ c \text{ and } c \ R \ b.$$

Proof. Let $a, b, c \in X$ be arbitrary. Assume that $a \ R \ b$ and $a \ R \ c$. As R was assumed euclidian, we derive $b \ R \ c$. We also know that $a \ R \ c$ and $a \ R \ b$, so for the same reason we have $c \ R \ b$. ■

56 Answer (Not a Total Order)

Lemma

The relation $R = \left\{ \langle x, y \rangle \in \mathbb{R} \times R \,\middle|\, x^2 = y \right\}$ on $\mathbb{R}$ is not a total order.

Proof. Suppose that R is a total order. This means in particular that for all $a, b \in \mathbb{R}$ one has $a \ R \ b$, $b \ R \ a$ or $a = b$. Consider -2 and 2, both clearly elements of $\mathbb{R}$. Yet $-2 \ R \ 2$ would entail $4 = (-2)^2 = 2$, which is false. Similarly, $2 \ R \ -2$ entails $4 = 2^2 = -2$, utter nonsense. The last option fares no better, because $-2 \neq 2$. All cases yield a contradiction, so R could not possibly be a total order. ■

61 Answer (Size of Union)

Lemma

Let X and Y be finite sets. The following holds:

$$|\, X \cup Y \,| \leq |\, X + Y \,|.$$

Proof. Recall from the definition of $X + Y$ that it is the union of two disjoint sets, respectively of size X and Y. We finish the proof by plugging in Exercise 27 twice:

$$\begin{aligned} \left| X \cup Y \right| &= \left| X \right| + \left| Y \right| - \left| X \cap Y \right| \\ &\leq \left| X \right| + \left| Y \right| \\ &= \left| \{ \langle x, 0 \rangle \mid x \in X \} \right| + \left| \{ \langle y, 1 \rangle \mid y \in Y \} \right| \\ &= \left| \{ \langle x, 0 \rangle \mid x \in X \} \right| + \left| \{ \langle y, 1 \rangle \mid y \in Y \} \right| - \left| \{ \langle x, 0 \rangle \mid x \in X \} \cap \{ \langle y, 1 \rangle \mid y \in Y \} \right| \\ &= \left| \{ \langle x, 0 \rangle \mid x \in X \} \cup \{ \langle y, 1 \rangle \mid y \in Y \} \right| = \left| X + Y \right|. \end{aligned}$$