Logic, Sets and Integer Arithmetic

An Introduction to the Mathematical Language

Hans Cuypers

First release, August 2023

Parts of these notes are based on
Algebra Interactive
Arjeh M. Cohen, H. Cuypers and H. Sterk,
Springer Verlag 1999, ISBN 978-3-540-65368-4

Contents

List of Figures

List of Tables

Introduction

Most probably, your experience of mathematics has been about using formulas and doing calculations. High school mathematics focuses on mathematical tasks like solving equations, computing derivatives, finding extreme values of functions, or calculating integrals. However, this is only one tiny part of mathematics. Mathematics is much more.

Doing mathematics means that you have to read mathematical texts, do calculations, experiment, make smart guesses, come up with definitions and statements, reason about and prove these statements to obtain new results and theorems, and eventually communicate about your results.

One of the main goals of these notes is to teach you how to do mathematics, not only how to compute, but also how to experiment, how to formulate definitions and statements, how to prove them, and how to communicate about them.

This is not an easy task. Doing mathematics is a creative process for which there is no algorithm. The best way to learn to do mathematics is by doing it yourself. However, we can give you lots of good examples, and guidelines, and of course explain you the rules for doing mathematics and provide you with basic theories and results that you can use, such as logic, set theory, and some number theory.

We will start by giving you some hints on how to communicate Mathematics.

A mathematical text usually consists of text divided into chapters, sections and paragraphs some of which are included in special mathematical environments such as Definitions, Theorems, Propositions, Lemmas, Corollaries, Examples and Proofs.

These environments have special meanings.

- *Definition* : a precise and unambiguous description of the meaning of a mathematical term. It characterizes the meaning of a word by giving all the properties and only those properties that must be true.
- *Theorem* : a mathematical statement that is proved to be true using rigorous mathematical reasoning. In a mathematical text, the term theorem is often reserved for the most important results.
- *Proposition* : an often interesting result, but generally less important than a theorem.
- *Lemma* : a minor result whose purpose is to help in proving a theorem. It is a stepping stone on the path to proving a theorem.
- *Corollary* : a result in which the (usually short) proof relies heavily on a given theorem (we often say that *this is a corollary to Theorem A*).
- *Proof* : a convincing argument that a certain mathematical statement is necessarily true. A proof generally uses deductive reasoning and logic but also contains some amount of ordinary language.
- *Examples* : examples help to understand the meaning of a definition, or the impact of a result.

- *Algorithms*: recipes to do calculations.

Within such text the author tries to guide the reader through the material in order to convince him or her of some mathematical results. This implies that the text should be well organized, arguments should be sound and complete and the language crystal clear.

In particular, this implies that the text may contain some formulas and computations, but certainly should be phrased in complete (English) sentences. The logical connection between these sentences is important. Phrases like "Therefore", "Then", "Hence", "Thus", "Because", "If ... then ... ", connect sentences and provide information about their logical connection. Their use is very important.

Even the smallest mathematical text, such as a solution to an exercises, should obey the above rules. So, when solving an exercise, and writing up your solution, keep in mind that it is your job to guide the reader through this solution. Provide him or her with the question you want to solve, write in clear and complete sentences. Explain which results you are using, and indicate clearly what your conclusions are.

The example below shows you how you might solve an exercise from Calculus.

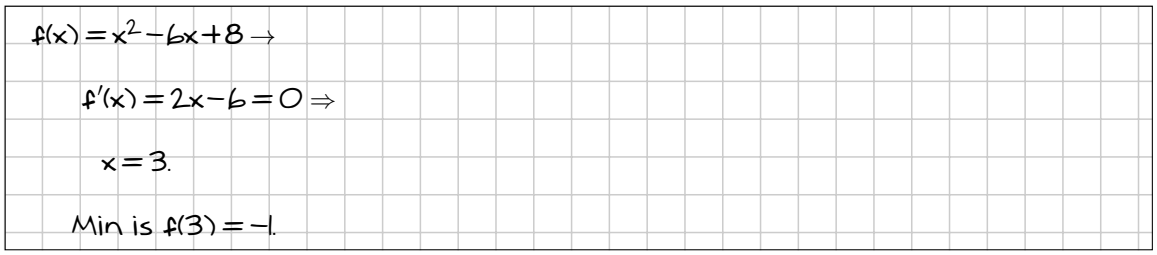
Example 0.0.1. What is the minimum value of the function f given by

$$f(x) = x^2 - 6x + 8$$

for all real numbers x?

Before we provide a proof, first have a look at a proof as many high school students will give.

Proof.



□

This we do not consider to be correct. One can only understand this proof if one knows the context as well as the various steps in the solution. One may ask the following questions:

- What is f and what is x? Is $f(x) = x^2 - 6x + 8$ an assumption or a conclusion?
- What is the relation between the first and second line? Is the second line a consequence of the first? Or is it just an assumption?
- Why is $f'(x) = 0$?
- Do we assume $x = 3$, or do we conclude that from the above lines?
- What is Min?
- ...

All these questions need answers.

Now a proof, as we expect from you.

Proof. Let f be the function given by

$$f(x) = x^2 - 6x + 8$$

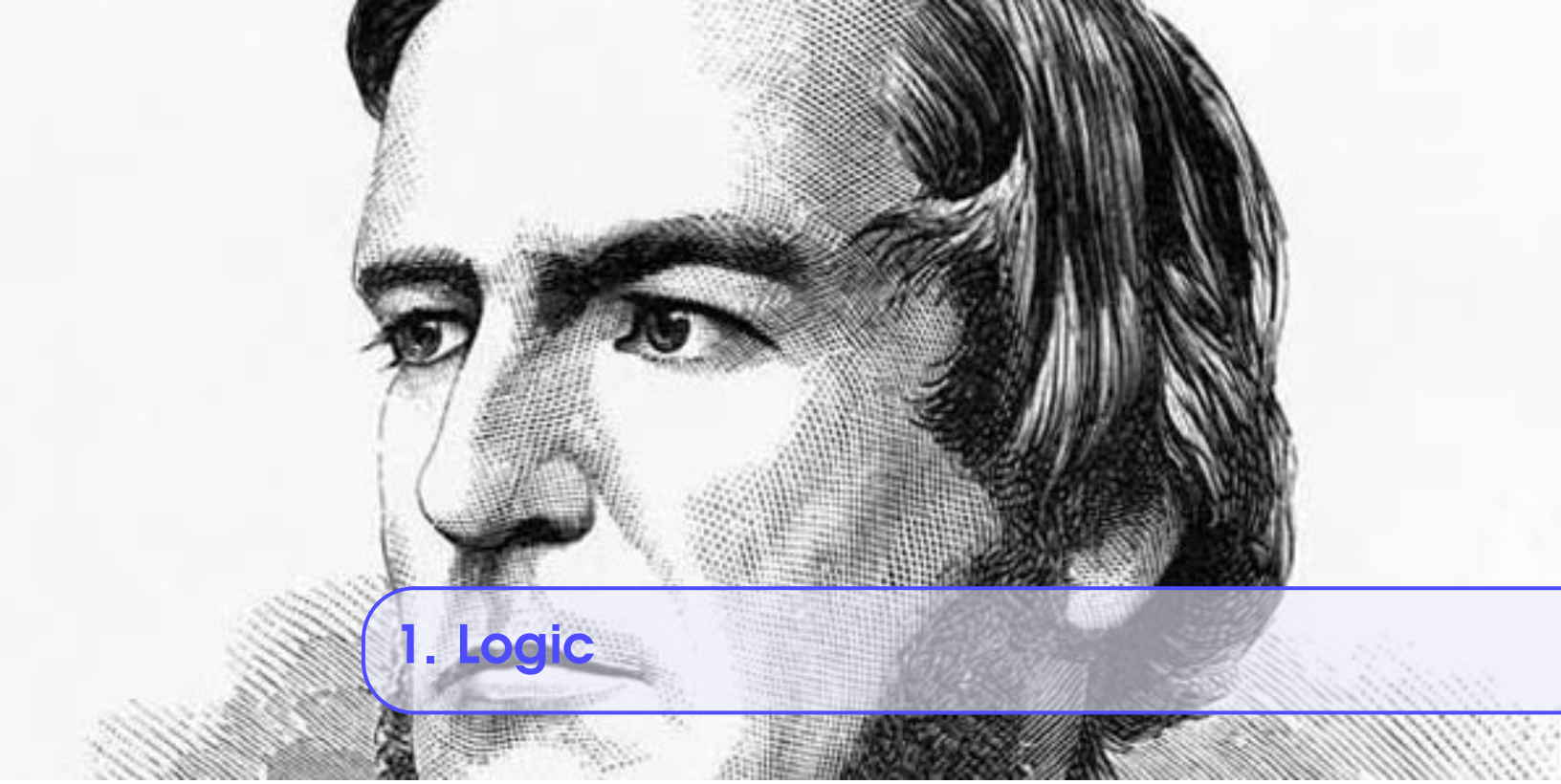
for all real numbers x.

Then its derivative f' satisfies $f'(x) = 2x - 6$. If the function f attains its minimum in x, then $f'(x) = 0$ and hence $2x - 6 = 0$, implying $x = 3$.

As the graph of the function f is an upwards parabola, f indeed attains a minimum for $x = 3$. The value of the minimum is then $f(3) = 9 - 18 + 8 = -1$. □

Notice that we start our proof with the definition of the function f. We then argue that the function having a minimum at a value x implies that $x = 3$. Then we notice that for $x = 3$, the function has indeed a minimum and that its value is -1. All of this is stated in full sentences.

In the sequel of these notes one finds many theorems, lemmas, definitions, algorithms (with implementations in Python) and so on, which you not only should use as information, but also as examples on how to communicate mathematics. Moreover, we introduce various concepts from Logic, Set Theory and Integer Arithmetic, which are basic in mathematics. They provide you with new tools to calculate, provide arguments and communicate in mathematics.



1. Logic

1.1 Statements

In the introduction, we already introduced you to some of mathematical terms, such as Theorem, Lemma, Definition, Proof, etc. But to be able to phrase Definitions, Theorems or Proofs, we first have to look at the basics of logic. Logic is concerned with mathematical statements and assertions we want to state. These statements should be either true or false.

Definition 1.1.1. A *statement* is a sentence that is either true or false but never both.

We will also use *proposition*, *logical statement* or *assertion*, when referring to a statement.

Example 1.1.2. Here you find some statements:

- All cars are either black or white.
- There are cars which are black.
- There exists an integer x with $x^2 = 9$.
- There exists an integer x with $x^2 = -9$.

But the following sentences are not statements:

- It will be sunny tomorrow.
- p is prime (What is p?)
- PSV is the best football team.
- Is it raining?
- Do you like coffee or tea?

1.2 Logical operators

In this section we will combine various statements to new statements. We will (usually) denote statements with capital letters.

George Boole, one of the founders of Logic

Definition 1.2.1 — Logical operators. Let A and B be assertions.
The assertion A *and* B (notation $A \wedge B$) is true, if and only if both A and B are true.
The assertion A *or* B (notation $A \vee B$) is true, if and only if at least one of A and B is true.
The negation of A is denoted by $\neg A$. This negation is true if and only if A is false.

The above definition can be summarized in the following table:

A	B	$A \wedge B$	$A \vee B$	$\neg A$
true	true	true	true	false
true	false	false	true	false
false	true	false	true	true
false	false	false	false	true

Table 1.1: Logical operators

Example 1.2.2. Let x be a real number with

$$(0 < x) \wedge (x < 5).$$

This means that x is a real number between 0 and 5.

Example 1.2.3. Let x be a real number with

$$(x < 0) \vee (x > 5)$$

means that x is a real number which is negative or at least 5.

Example 1.2.4. Let x be a real number with

$$\neg(x > 5)$$

means that x is a real number which is *not* greater than 5, so $x \leq 5$.

Definition 1.2.5 — Implies. If A and B are assertions, then the assertion *if* A *then* B (notation $A \Rightarrow B$) is true if and only if one of the following occurs:
- A is true and B is true;
- A is false and B is true;
- A is false and B is false.

Example 1.2.6. Let x be a real number. Then consider the following true conditional statements.
- If $x^2 > 4$ then $(x < -2) \vee (x > 2)$.
- If $x^2 \leq 4$ then $(x \geq -2) \wedge (x \leq 2)$.
- If $x^2 \leq -4$ then $(x \geq -2) \wedge (x \leq 2)$.

Notice that the last statement is indeed true. As $x < -4$ is false for every real x, any statement of the form $(x^2 < -4) \Rightarrow Q$ is true.

The following statements are false:
- If $x^2 > 4$ then $(x < -2) \wedge (x > 2)$.
- If $x^2 \leq 4$ then $(x \geq -2) \vee (x \leq 2)$.

Definition 1.2.7 — If and only if. By $A \Leftarrow B$ we denote *if* B *then* A and by

$$A \Leftrightarrow B$$

we denote

$$(A \Leftarrow B) \wedge (A \Rightarrow B).$$

This is expressed as *A if and only if B*. This leads to the following table.

A	B	$A \Rightarrow B$	$A \Leftarrow B$	$A \Leftrightarrow B$
true	true	true	true	true
true	false	false	true	false
false	true	true	false	false
false	false	true	true	true

Table 1.2: Truth table for *if ... then*, and *if and only if*.

Example 1.2.8. Several statements in theorems, propositions or lemmas are in the form "if ... then ..." or can be stated in such a way. For example:

- If a and b are odd integers, then their product ab is odd.
- If a and b are odd integers, then their sum $a+b$ is even.

Example 1.2.9. Suppose P and Q are two propositions, and we want to prove that $P \Rightarrow Q$ is true, then it suffices to prove that in case P is true, the statement Q is also true. For, in case P is false, the implication $P \Rightarrow Q$ is always true.

For example, here is a proof of the statement

If a and b are odd integers, then their sum is even.

Suppose a and b are odd integers. Then there exist integers m and n such that

$$a = 2m+1$$

and

$$b = 2n+1.$$

But then

$$a+b = (2m+1)+(2n+1) = 2(m+n+1)$$

which is clearly even.

Warning. 1.2.10 Many students use $\Rightarrow$ in an incorrect way. For example:

Find the minimum of $f(x) = x^2 - 8x + 15$.

$x^2-8x+15 = (x-4)^2-16+15 \Rightarrow$
$(x-4)^2-1 \geq -1 \Rightarrow$
$\min = -1$

Here the symbol $\Rightarrow$ is used instead of "so", "hence" or "therefore". If P then Q is, however, different from P holds true and therefore Q is also true.

If we prove that P implies Q, then to conclude that Q holds true, we still have to assume (or know and state) that P is true. We should phrase a solution as follows:

Suppose $f(x) = x^2 - 8x + 15$. Then

$$\begin{aligned} f(x) &= x^2 - 8x + 15 \\ &= (x-4)^2 - 16 + 15 \\ &= (x-4)^2 - 1 \\ &\geq -1. \end{aligned}$$

So, the minimal value of f is -1, which is attained for $x = 4$.

Remark 1.2.11. Notice that the definitions of $\dots$ *or* $\dots$ and of *if* $\dots$ *then* $\dots$ are a bit different from what we are used to in common language.

In common language the *or* is usually an exclusive *or*. If we say "*would you like to have a cup of coffee or tea?*", we do not expect the answer yes, but a choice.

Also statements involving *if* $\dots$ *then* $\dots$ are often used in a different way than in logic. Indeed, a statement like "*if London is the capital of Germany, then Paris is the capital of France*" is not always considered to be true. In logic, however, it is a true statement.

1.3 Proposition Calculus

In proposition calculus we study the various statements obtained by using the operators $\wedge, \vee, \neg$ and $\Rightarrow$.

We use these operators and assertions $P_1, \dots, P_k$ to form new assertions, and analyze them. A very helpful tool is then a truth table.

Example 1.3.1. Let P, Q and R be assertions and consider the assertion

$$((P \vee Q) \wedge R) \Leftrightarrow ((P \wedge R) \vee (Q \wedge R)).$$

We claim this assertion to be true. We can check that using the following truth table, where $L = (P \vee Q) \wedge R$ and $M = (P \wedge Q) \vee (Q \wedge R)$.

P	Q	R	$P \vee Q$	L	$P \wedge R$	$Q \wedge R$	M	$L \Leftrightarrow M$
true	true	true	true	true	true	true	true	true
true	true	false	true	false	false	false	false	true
true	false	true	true	true	true	false	true	true
true	false	false	true	false	false	false	false	true
false	true	true	true	true	false	true	true	true
false	true	false	true	false	false	false	false	true
false	false	true	false	false	false	false	false	true
false	false	false	false	false	false	false	false	true

Table 1.3: Truth table

Proposition 1.3.2. Suppose P, Q and R are assertions. Then the following assertions are true:

(a) $P \vee \neg P$;
(b) $P \Leftrightarrow \neg(\neg P)$;
(c) $\neg(P \wedge \neg P)$;
(d) $(P \Rightarrow Q) \Leftrightarrow (\neg P) \vee Q)$;
(e) $(\neg(P \vee Q)) \Leftrightarrow ((\neg P) \wedge (\neg Q))$
(f) $(\neg(P \wedge Q)) \Leftrightarrow ((\neg P) \vee (\neg Q))$
(g) $(P \Rightarrow Q) \Leftrightarrow ((\neg Q) \Rightarrow (\neg P))$;
(h) $((P \vee Q) \wedge R) \Leftrightarrow ((P \wedge R) \vee (Q \wedge R))$;
(i) $((P \wedge Q) \vee R) \Leftrightarrow ((P \vee R) \wedge (Q \vee R))$;
(j) $(P \vee Q) \Rightarrow R) \Leftrightarrow (P \Rightarrow R) \wedge (Q \Rightarrow R)$.

Proof. A proof of each of the above statements can be given by the use of a truth table. In particular, (h) has been proven in Example 1.3.1. □

Definition 1.3.3. Suppose P and Q are assertions.
We say P *implies* Q if $P \Rightarrow Q$ is true. We call P and Q *equivalent*, if P implies Q and Q implies P.

In Proposition 1.3.2 above we encounter various equivalent statements in terms of arbitrary statements P, Q and R. Here are some more concrete examples.

Example 1.3.4. Let n be an integer. Then n is even if and only if its square n^2 is even. So the statement that n is even is equivalent with the statement that n^2 is even.

Example 1.3.5. Let ℓ and m be straight lines in the plane $\mathbb{R}^2$. Then ℓ meets m in a unique point if and only if the slope of ℓ is different from the slope of m.

The statement that ℓ meets m in a unique point is equivalent to the slopes of the lines being different.

1.4 Methods of proof

Many mathematical statements are of the form

If P then Q.

Such statements are called *conditional statements*. If P is false, then the conditional statement $P \Rightarrow Q$ is true. So, in case P is false, there is nothing to prove. But then, for proving $P \Rightarrow Q$, we only have to consider the case where P is true and deduce the truth of statement Q. This approach to proving $P \Rightarrow Q$ is called a *direct proof* of $P \Rightarrow Q$.

So, a direct proof of $P \Rightarrow Q$ starts with something like:

Assume that P is true.

Then we have some arguments implying that also Q is true. We end the proof with something like:

Hence Q is true.

We provide some examples.

Example 1.4.1. Let m and n be integers. We provide a direct proof of the following conditional statement: if both n and m are odd, then nm is odd.

Proof. Assume that both n and m are odd. So, $n = 2k+1$ and $m = 2\ell+1$ for some integers k and ℓ. But then

$$nm = (2k+1)\cdot(2\ell+1) = 4k\ell + 2k + 2\ell + 1 = 2(2k\ell + k + \ell) + 1,$$

which is odd. So, indeed nm is odd.

As our initial elements n and m are arbitrary integers, we have proven the statement. □

Example 1.4.2. Let m and n be integers.

If n or m is even , then nm is even.

Proof. Assume that at least one of n or m is even. Without loss of generality we can assume that n is even and equals $2k$ for some integer k.

Then

$$nm = (2k)\cdot m = 2(k\cdot m),$$

which is even. So, indeed nm is even. This proves our statement. □

In the previous section we have seen that a proposition $P \Rightarrow Q$ is equivalent with $\neg Q \Rightarrow \neg P$. We use this equivalence to introduce two proving techniques:

- *Proof by contraposition*.

- *Proof by contradiction.*

We start with some examples.

Example 1.4.3. Consider the following statement.

If n and m are integers with nm even, then n or m is even.

A direct proof of this statement is not so easy. Suppose n and m are integers with nm even. How do you deduce that n or m is even? For this you need more knowledge about how integers factor.

We will not give a direct proof, but use our previous Example 1.4.1. Indeed, if not (n or m is even), then they are both odd and their product is odd.

So if P denotes the statement "n and m are integers with nm even" and Q denotes the statement "n or m is even" we prove $\neg Q \Rightarrow \neg P$, which is equivalent to $P \Rightarrow Q$.

So, we have proven the statement

If n and m are integers with nm even, then n or m is even.

by proving the equivalent statement

If both n and m are odd, then nm is odd

as in the Example 1.4.1 above.

Proving a statement $P \Rightarrow Q$ to be true by showing that $\neg Q \Rightarrow \neg P$ is true is called a *proof by contraposition*.

Here is another example of such a proof.

Example 1.4.4. Consider the following statement:

If an integer n is equal to $3m+2$ for some integer m, then n is not a square.

This statement is equivalent to the following statement:

If an integer n is a square, then it is not of the form $3m+2$ for some integer m.

We prove the latter statement and thus also the first. So we provide a proof by contraposition.

Proof. Suppose $n = k^2$ for some integer k. Then k is of the form $3l+i$ for some i equal to 0, 1, or 2. Hence $n = k^2 = (3l+i)^2 = 9l^2+6l+i^2$. If $i = 0$, we find n to be a multiple of 3, and hence not of the form $3m+2$ for some integer m. If $i = 1$, then $n = 3(3l^2+2l)+1$ and again not of the form $3m+2$ for some m. And finally, if $i = 2$, then $n = 3(3l^2+2l+1)+1$ which again is not of the form $3m+2$ for some integer m. □

Another way of using the equivalence of $P \Rightarrow Q$ and $\neg Q \Rightarrow \neg P$ in proving statements is the so-called *proof by contradiction*.

Suppose one wants to prove an assertion P. Then a way to do that is to assume that P is not true and deduce a contradiction with some obviously true statement Q.

Thus, one proofs $\neg P \Rightarrow \neg Q$, and by the above the equivalent statement $Q \Rightarrow P$. But then the obvious truth of Q implies P to be true.

Here an example of a proof by contradiction:

Example 1.4.5. Consider the proposition P: there are no positive integers x, y with $x^2 - y^2 = 1$.

Proof. As we want to prove P by contradiction, we assume the assertion P to be not true. So, assume that there exist positive integers x and y with $x^2 - y^2 = 1$.

We will show that this implies that x or y is not positive, a clear contradiction with the statement that an integer can not be both positive and not positive at the same time.

Since $x^2 - y^2 = (x-y)\cdot(x+y) = 1$ it follows that either $x-y = 1$ and $x+y = 1$ or $x-y = -1$ and $x+y = -1$.

In the first case we can add the two equations to get $2x = 2$, from which we deduce that $x = 1$ and $y = 0$, contradicting our assumption that x and y are positive. In the second case we find in a similar way that $x = -1$ and $y = 0$, again contradicting our assumption.

These contradictions imply that our assumption that there exist positive integers x and y with $x^2 - y^2 = 1$ is false. There are no such positive integers. □

We finish with a *proof by cases*, which makes use of the equivalence of

$$(P \vee Q) \Rightarrow R$$

and

$$(P \Rightarrow R) \wedge (Q \Rightarrow R).$$

This equivalence implies that we can divide a proof in cases, which together cover all situations under consideration.

Example 1.4.6. We prove that if n is an integer, then $3n^2 + n + 12$ is even.

The proof is divided into the case where n is even and the case where n is odd.

First assume n is even. So, $n = 2m$ for some integer m. Then

$$\begin{aligned} 3n^2 + n + 12 &= 3(2m)^2 + 2m + 12 \\ &= 12m^2 + 2m + 12 \\ &= 2(6m^2 + m + 12) \end{aligned}$$

which is even.

Next assume n is odd, so $n = 2m + 1$ for some integer m. Then

$$\begin{aligned} 3n^2 + n + 12 &= 3(2m+1)^2 + 2m + 1 + 12 \\ &= 3(4m^2 + 4m + 1) + 2m + 1 + 12 \\ &= 12m^2 + 14m + 16 \\ &= 2 \cdot (6m^2 + 7m + 8) \end{aligned}$$

which is also even. Combining both cases we find that if n is an integer, then $3n^2 + n + 12$ is even.

Notice that we already made use of a proof by cases in Example 1.4.4 as well as Example 1.4.5.

1.5 Exercises

Exercise 1.5.1. Suppose p is true and q is false. What about

(a) $p \Rightarrow (p \Rightarrow q)$;
(b) $p \Rightarrow (q \Rightarrow p)$;
(c) $q \Rightarrow (p \Rightarrow q)$;
(d) $q \Rightarrow (q \Rightarrow p)$.

Exercise 1.5.2. For assertions p, q and r we have

$$((p \wedge q) \vee r) \Leftrightarrow ((p \vee r) \wedge (q \vee r))$$

and

$$((p \vee q) \wedge r) \Leftrightarrow ((p \wedge r) \vee (q \wedge r)).$$

Prove these two statements with and without the use of a truth table.

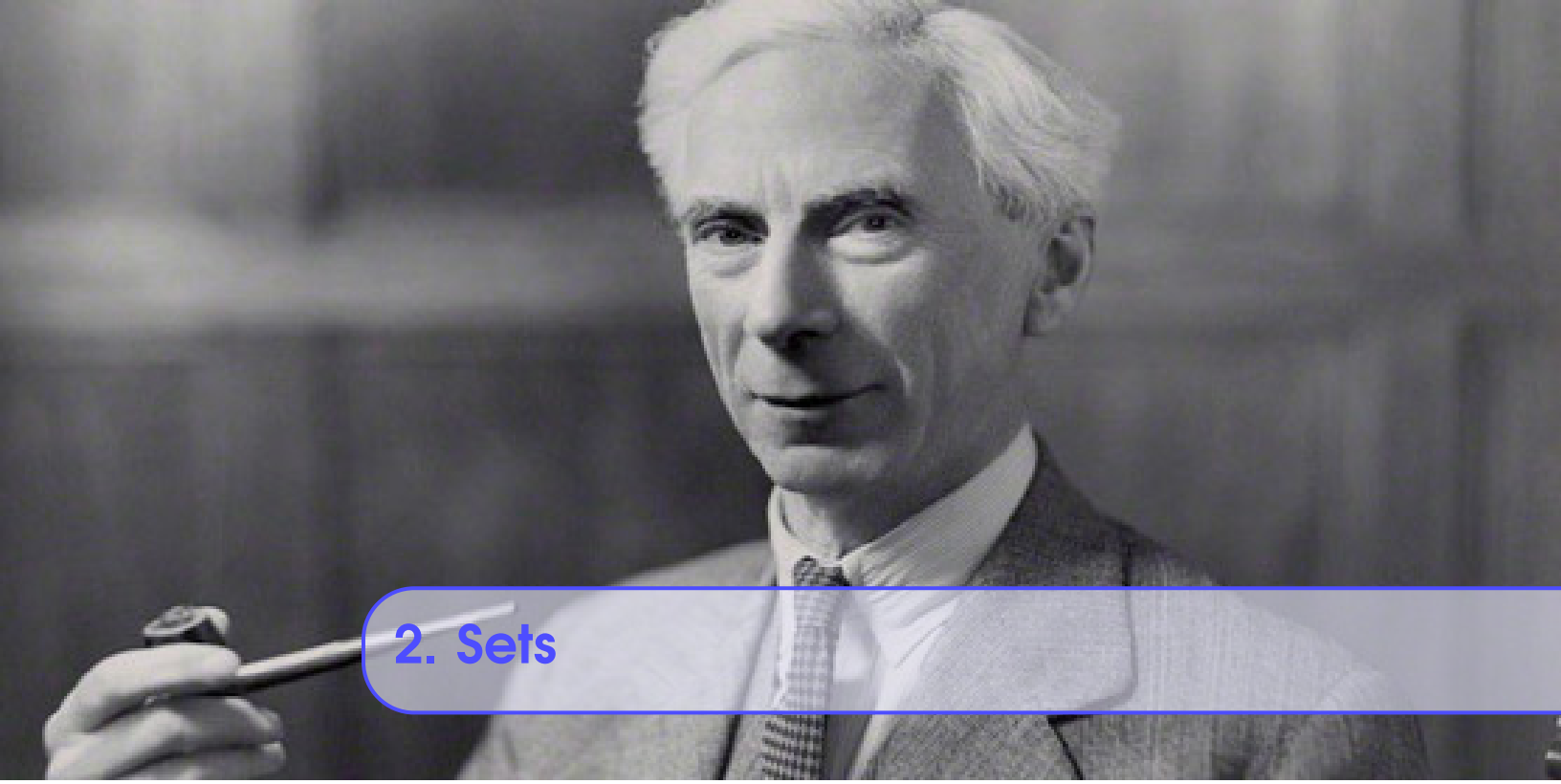
Exercise 1.5.3. . If n is an odd integer, then $n^2 - 1$ is a multiple of 4.

Prove this statement with a direct proof.

Exercise 1.5.4. If $n^2 - 1$ is odd, then n is even.
Prove this statement with a proof by contraposition.

Exercise 1.5.5. Provide a proof of the statements (e), (f) and (g) of Proposition 1.3.2.

Exercise 1.5.6. Prove that if n is an integer, then $2n^2 + n + 1$ is not divisible by 3. Use a proof by division into cases.



2. Sets

2.1 Sets and Subsets

A set is any collection of "things" or "objects". Your immediate family is a set. A shopping list is a set of items that you wish to buy when you go to the store. The collection of cars in a dealership parking lot is a set. The only thing that matters to a set is what is in it. There is no notion of order or how many of a particular item. A thing that is in a set is called an element or member of the set. A set is *uniquely defined by its elements*.

In Set Theory the notions of *set*, *element* and *is an element of* are basic. We assume these notions to be known.

Mathematical examples of sets are $\mathbb{N}$, the set of natural numbers, $\mathbb{Z}$, the set of integers, $\mathbb{Q}$, the set of all rational numbers (i.e., fractions) and $\mathbb{R}$, the set of all real numbers.

We use the following notation: If V is a set, then by $v \in V$ we mean that v is an element from the set V. We also say "v is in V", or "v belongs to V". By $v \notin V$ we denote that the element v is *not* in V.

Remark 2.1.1. The set $\mathbb{N}$ is the set of natural numbers. It contains 1, 2, 3 and so on. So, it contains the positive integers. Some consider the number 0 also to be a natural number, while others do not. In these notes we leave it open whether we consider 0 to be in $\mathbb{N}$ or not. Depending on the context we assume $0 \in \mathbb{N}$ or not. If it is of importance whether $0 \in \mathbb{N}$ or not, then we will explicitly mention that 0 is in $\mathbb{N}$ or not.

A common way to describe a set is by enumerating its elements and write them between curly brackets. The elements are separated by commas. The order in which elements are given is irrelevant. Also the multiplicity in which elements occur does not matter. For example

$$\{1,2,3\},\ \{2,1,3\},\ \text{and}\ \{1,1,1,1,2,2,3\}$$

denote the same set.

Definition 2.1.2. Suppose A and B are sets. Then A is called a *subset* of B, if for every element $a \in A$ we also have that $a \in B$.

If A is a subset of B, then we write $A \subset B$ or $A \subseteq B$. We also say that B contains A.

Bertrant Russell

By $B \supset A$ or $B \supseteq A$ we mean $A \subset B$ or $A \subseteq B$.

Example 2.1.3. It is true that $1 \in \{1,2,3\}$ and $\{1\} \subseteq \{1,2,3\}$, but *not* that $1 \subseteq \{1,2,3\}$ or $\{1\} \in \{1,2,3\}$.

Example 2.1.4. Notice that $\emptyset \in \{\emptyset\}$ and $\emptyset \subseteq \{\emptyset\}$.

Example 2.1.5. The following inclusions are proper:

$$\mathbb{N} \subsetneq \mathbb{Z} \subsetneq \mathbb{Q} \subsetneq \mathbb{R}.$$

For each set B we find B to be a subset of itself. So $B \subseteq B$. Moreover, the *empty set* $\emptyset$, that is the set with no elements, is a subset of B. A subset A of a set B which is not the empty set nor the full set B is called a *proper* subset of B. To indicate that a subset A of B is not the full set B we write $A \subsetneq B$. Some authors use $A \subset B$ to indicate that A is a subset of B but not equal to B, others allow that $A = B$. We prefer the use of $\subsetneq$ and $\subseteq$.

Definition 2.1.6. If B is a set, then by $\mathscr{P}(B)$ we denote the set of all subsets A of B. The set $\mathscr{P}(B)$ is called the *power set* of B.

Notice that the power set of a set is never empty. Indeed, it always contains the empty set $\emptyset$ as an element.

Example 2.1.7. Suppose $A = \{x,y,z\}$, then $\mathscr{P}(A)$ consists of the following 8 subsets of A:

$$\emptyset, \{x\}, \{y\}, \{z\}, \{x,y\}, \{x,z\}, \{y,z\}, \{x,y,z\}.$$

In general we have:

Proposition 2.1.8. Let A be a set with n elements. Then its power set $\mathscr{P}(A)$ contains 2^n elements.

Proof. Let A be a set with n elements.

A subset B of A is completely determined by its elements. For each element $a \in A$ we have two choices, it is in B or it is not. So, there are 2^n choices and thus 2^n different subsets B of A. □

Proposition 2.1.9. Suppose A, B and C are sets. Then the following hold:
(a) If $A \subseteq B$ and $B \subseteq C$ then $A \subseteq C$.
(b) If $A \subseteq B$ and $B \subseteq A$ then $A = B$.

Proof. We prove the first statement. Suppose that $A \subseteq B$ and $B \subseteq C$. Let $a \in A$. Since $A \subseteq B$, we find $a \in B$. Now, since we also have $B \subseteq C$, the element a is also in C.

This shows that for every element $a \in A$, we also have $a \in C$. Hence $A \subseteq C$.

As for the second statement. Every element of A is in B and every element of B in A. But as a set is uniquely determined by its elements, we find $A = B$. □

The second statement "If $A \subseteq B$ and $B \subseteq A$, then $A = B$" may seem to be a trivial observation, but it will prove to be very useful. It provides a way to show that two sets are equal!

Indeed, to prove that two sets A and B are equal, we first show that $A \subseteq B$ by proving that each element $a \in A$ is also an element from B and then that $B \subseteq A$ by proving that each $b \in B$ is also in A.

This leads to the following set up of a proof that two sets A and B are equal.

Skeleton of a proof: A proof that two sets are equal can be given in the following form:

Let $a \in A$. Then … [here an argument to show that $a \in B$]. So $a \in B$. This proves that $A \subseteq B$.

Now let $b \in B$. Then … [by some arguments] $b \in A$. Hence $B \subseteq A$.

As $A \subseteq B$ and $B \subseteq A$, we find $A = B$.

Figure 2.1: John Venn (1834-1923)

Example 2.1.10. Let A be the set of all integers x for which there are $a,b \in \mathbb{Z}$ with $x = 9a+15b$. By B we denote the set of all integers which are multiples of 3. We will show that $A = B$.

First we prove that $A \subseteq B$. So, let $x \in A$. Then $x = 9a+15b = 3(3a+5b)$ for some $a,b \in \mathbb{Z}$ and hence x is a multiple of 3 and therefore $x \in B$. So indeed, $A \subseteq B$.

Now we show that $B \subseteq A$. So, assume $x \in B$, then x equals $3m$ for some m. But as $3 = 2 \cdot 9 - 15$ we find $x = (2 \cdot 9 - 15)m = (2m)9 + (-m)15$ and hence $x \in A$. So, also $B \subseteq A$.

But as $A \subseteq B$ and $B \subseteq A$ we have $A = B$.

Many statements and assertions on sets are illustrated by so-called Venn diagrams. The philosopher and mathematician John Venn (1834-1923) introduced the Venn diagram in 1881. Below you find an example illustrating the fact that if $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C$.

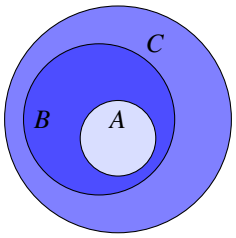


Figure 2.2: If $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C$.

2.2 How to describe a set?

If V is a set, then we can describe V by enumerating all its elements and put them in between curly brackets. This, however, is a nontrivial task if V is large or even impossible if V has infinitely many elements.

In this section we offer some new ways of how to describe a set. Think, for example, of the following description of a set: Let X be the set of all real numbers x satisfying $0 \leq x$ and $x \leq 1$.

To describe this set we make use of a known set, the set of real numbers (the *reference set*), and a *predicate*, in this case "$0 \leq x$ and $x \leq 1$". For every value of the variable x the predicate provides a *statement* or *proposition* on x which is either true or false.

An element x from the real numbers is in the set if and only if the predicate yields a true statement for that particular x.

The way to use these predicates to define and describe sets is the following.

Definition 2.2.1. Let P be a predicate with reference set X, then

$$\{x \in X \mid P(x)\}$$

denotes the subset of X consisting of all elements $x \in X$ for which the statement $P(x)$ is true.

Other ways to denote this set are

$$\{x \in X : P(x)\} \text{ and } \{x \in X; P(x)\}.$$

The name of the variable, in our example x, is of no importance outside the definition of the set. So

$$\{x \in X \mid P(x)\} = \{y \in X \mid P(y)\}.$$

We say that the variable is *bounded* to the definition of the set.

Example 2.2.2. The set $\{x \in \mathbb{R} \mid x > 0\}$ consists of the positive real numbers.

The set $\{z \in \mathbb{Z} \mid z \text{ is divisible by } 2\}$ is the set of all even integers.

Besides enumeration of all elements and the use of predicates, there are still other ways of describing sets. Examples are: the set of even integers; the set of points on a line; the set of all citizens of New York. Here a set is given by its objects. But we will also encounter notions like $\{1,3,5,7,9,11,\dots\}$ to denote the set of odd natural numbers, or $\{\dots,-2,0,2,4,\dots\}$ to denote the set of all even integers.

Example 2.2.3. Consider the set $X = \{1,4,9,16,\dots\}$ of squares. This set can be described as follows:

$$X = \{x \in \mathbb{N} \mid \text{there is a y} \in \mathbb{N} \text{ with } x = y^2\}$$

Another way of describing a set is the following:

$$X = \{n^2 \mid n \in \mathbb{N}\}.$$

Example 2.2.4. Let $A = \{x \in \mathbb{Z} \mid \text{there are integers } y,z \text{ such that } x = 6y+9z\}$ and $B = \{3n \mid n \in \mathbb{Z}\}$. Then a quick check shows that these sets might be the same. How do we prove that?

We show that $A \subseteq B$ and $B \subseteq A$.

First $A \subseteq B$. So let $a \in A$, then there are $y,z \in \mathbb{Z}$ with $a = 6y+9z = 3(2y+3z)$. So with $n = 2y+3z$ we find $a = 3n \in B$. This shows that $A \subseteq B$.

Now $B \subseteq A$. Let $b \in B$, then there is an $n \in \mathbb{Z}$ such that $b = 3n$. But then $b = 3n = (-6+9)n = 6\cdot(-n)+9\cdot n$ and with $y = -n$ and $z = n$ we find $b = 6y+9z \in A$. We also have shown that $B \subseteq A$.

But then we can conclude that $A = B$

2.3 Operations on Sets

Definition 2.3.1. Let A and B be sets.

The *intersection* of A and B, notation $A \cap B$, is the set of all elements contained in both A and B.

The *union* of A and B, notation $A \cup B$, is the set of elements that are in at least one of A or B.

Two sets A and B are called *disjoint*, if their intersection $A \cap B$ is the empty set.

In Figure 2.3 you see a Venn diagram for the intersection and union of two sets.

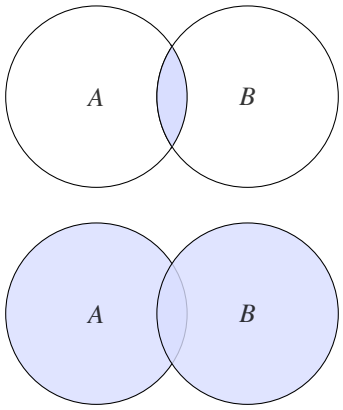


Figure 2.3: The intersection $A \cap B$ and union $A \cup B$ of the two sets A and B.

Proposition 2.3.2. Let A, B and C be sets. Then the following hold:
(a) $A \cup B = B \cup A$;
(b) $A \cup \emptyset = A$;
(c) $A \subseteq A \cup B$;
(d) If $A \subseteq B$, then $A \cup B = B$;
(e) $(A \cup B) \cup C = A \cup (B \cup C)$;
(f) $A \cap B = B \cap A$;
(g) $A \cap \emptyset = \emptyset$;
(h) $A \cap B \subseteq A$;
(i) If $A \subseteq B$, then $A \cap B = A$;
(j) $(A \cap B) \cap C = A \cap (B \cap C)$.

Proof. We prove (e).

First we show that $(A \cup B) \cup C \subseteq A \cup (B \cup C)$. Therefore, let $x \in (A \cup B) \cup C$. Then, by definition of the union, $x \in A \cup B$ or $x \in C$. If $x \in C$, then, again by definition of the union, $x \in B \cup C$ and thus also in $A \cup (B \cup C)$. If $x \in A \cup B$, then $x \in A$ and hence in $A \cup (B \cup C)$, or $x \in B$ and then also in $B \cup C$ and in $A \cup (B \cup C)$. Thus, if $x \in (A \cup B) \cup C$, then $x \in A \cup (B \cup C)$. We have shown that $(A \cup B) \cup C \subseteq A \cup (B \cup C)$.

Similarly we find that $x \in A \cup (B \cup C)$ implies $x \in (A \cup B) \cup C$, from which we deduce $(A \cup B) \cup C \supseteq A \cup (B \cup C)$.

Combining the above, we find $(A \cup B) \cup C = A \cup (B \cup C)$.

□

Due to property (a) and (f) we call the operators $\cap$ and $\cup$ *commutative*. This in analogy with the commutative law for addition or multiplication for real numbers or integers.

Property (e) and (j) are the *associative* laws for the intersection and union. Due to these properties we do not have to put brackets in expressions like $A \cap B \cap C$ or $A \cup B \cup C$. We simply can define the union $A_1 \cup \cdots \cup A_k$ of a finite number of sets $A_1, \ldots, A_k$ to be $(\ldots (A_1 \cup A_2) \cdots \cup A_{k-1}) \cup A_k$. Similarly, the intersection $A_1 \cap \cdots \cap A_k$ is well defined, it equals $(\ldots (A_1 \cap A_2) \cdots \cap A_{k-1}) \cap A_k$. But these unions and intersections can also be taken over an infinite index set:

Definition 2.3.3. Suppose I is a set and for each element i there exists a set A_i, then

$$\bigcup_{i \in I} A_i := \{x \mid \text{ there is an } \ i \in I \text{ with } x \in A_i\}$$

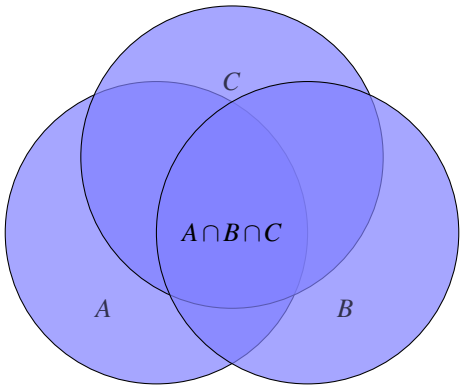


Figure 2.4: $A \cap B \cap C$

and

$$\bigcap_{i \in I} A_i := \{x \mid \text{ for all } \ i \in I \text{ we have } x \in A_i\}.$$

(The set I is called the index set.)

If $\mathscr{C}$ is a set (also called collection) of sets, then we can define

$$\bigcup_{A \in \mathscr{C}} A := \{x \mid \text{ there is an } A \in \mathscr{C} \text{ with } x \in A\}$$

and

$$\bigcap_{A \in \mathscr{C}} A := \{x \mid \text{ for all } \ A \in \mathscr{C} \text{ we have } x \in A\}.$$

Example 2.3.4. Suppose for each $i \in \mathbb{N}$ the set A_i is defined as $\{x \in \mathbb{R} \mid 0 \leq x \leq i\}$. Then

$$\bigcap_{i \in \mathbb{N}} A_i = \{0\}$$

(here we assume $0 \in \mathbb{N}$) and

$$\bigcup_{i \in \mathbb{N}} A_i = \mathbb{R}_{\geq 0} = \{x \in \mathbb{R} \mid x \geq 0\}.$$

Definition 2.3.5. Let A and B be sets. The *difference* of A and B, notation $A \setminus B$, is the set of all elements from A that are *not* in B.

The *symmetric difference* of A and B, notation $A \triangle B$, is the set consisting of all elements that are in *exactly one of* A or B.

Proposition 2.3.6. Let A, B and C be sets. Then the following hold:

(a) $A \setminus B \subseteq A$;
(b) If $A \subseteq B$, then $A \setminus B = \emptyset$;
(c) $A = (A \setminus B) \cup (A \cap B)$;
(d) $A \triangle B = (A \setminus B) \cup (B \setminus A)$;
(e) $A \triangle B = B \triangle A$;
(f) If $A \subseteq B$, then $A \triangle B = B \setminus A$;
(g) $A \triangle (B \triangle C) = (A \triangle B) \triangle C$.

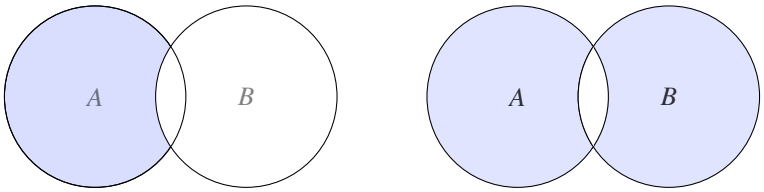


Figure 2.5: The difference $A \setminus B$ and symmetric difference $A \triangle B$ of the sets A and B.

Proof. We prove (f).

Suppose $A \subseteq B$. If $x \in A \Delta B$, then $x \in A \setminus B = \emptyset$, which is not possible, or $x \in B \setminus A$. Hence $x \in B \setminus A$. So $A \setminus B \subseteq B \setminus A$.

On the other hand, $B \setminus A$ is by definition contained in $A \Delta B$.

We can conclude that $A \Delta B = B \setminus A$. □

Below you find some statements involving more than one of the operators $\cap$, $\cup$, $\setminus$ or $\triangle$.

Proposition 2.3.7. Let A, B and C be sets. Then the following hold:
(a) $(A \cup B) \cap C = (A \cap C) \cup (B \cap C)$;
(b) $(A \cap B) \cup C = (A \cup C) \cap (B \cup C)$;
(c) $A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C)$;
(d) $A \setminus (B \cap C) = (A \setminus B) \cup (A \setminus C)$.

Proof. We prove (a).

Let $x \in (A \cup B) \cap C$. Then $x \in A \cup B$ and $x \in C$. So $x \in A$ and $x \in C$, or $x \in B$ and $x \in C$ and hence $x \in A \cap C$ or $x \in B \cap C$, implying that $x \in (A \cap C) \cup (B \cap C)$. So $(A \cup B) \cap C \subseteq (A \cap C) \cup (B \cap C)$.

Now assume that $x \in (A \cap C) \cup (B \cap C)$. The $x \in A \cap C$ or $x \in B \cap C$. In both cases $x \in A \cup B$ and $x \in C$. So $x \in (A \cup B) \cap C$. This implies that $(A \cup) \cap C \subseteq (A \cap C) \cup (B \cap C)$.

We conclude that $(A \cup B) \cap C = (A \cap C) \cup (B \cap C)$. □

Definition 2.3.8. If one is working inside a fixed set U and only considering subsets of U, then the difference $U \setminus A$ is also called the *complement* of A in U. We write A^* or A^c for the complement of A in U. In this case the set U is also called the *universe*.

Proposition 2.3.9. For subsets A, B and C of the universe U we have:
(a) $A \cup A^* = U$;
(b) $B \setminus C = B \cap C^*$;
(c) $(A^*)^* = A$;
(d) If $A \subseteq B$ then $B^* \subseteq A^*$;
(e) $(A \cup B)^* = A^* \cap B^*$;
(f) $(A \cap B)^* = A^* \cup B^*$.

2.4 Cartesian products

Suppose $a_1, a_2, \ldots, a_k$ are elements from some set, then the ordered k-tuple of $a_1, a_2, \ldots, a_k$ is denoted by $(a_1, a_2, \ldots, a_k)$.

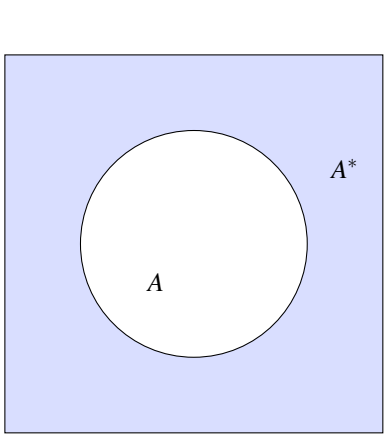


Figure 2.6: The complement A^* of a set A in the universe U.

Definition 2.4.1. The Cartesian product $A_1 \times \cdots \times A_k$ of sets $A_1, \ldots, A_k$ is the set of all ordered k-tuples $(a_1, a_2, \ldots, a_k)$ where $a_i \in A_i$ for $1 \leq i \leq k$.

In particular, if A and B are sets, then

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

Notice that taking the Cartesian product is not associative. The sets $A \times (B \times C)$, $(A \times B) \times C$ and $A \times B \times C$ are all different. However, there is a canonical way of identifying all three sets. Indeed, leave out all brackets except for the outer ones.

If for all $1 \leq i \leq k$ we have $A_i = A$, then $A_1 \times \cdots \times A_k$ is also denoted by A^k. In this way we also encounter $\mathbb{R}^2$ as the coordinate system for the real plane.

Figure 2.7: René Descartes (1596-1650).

Cartesian means relating to the French mathematician and philosopher René Descartes (Latin: Cartesius), who, among other things, worked to merge algebra and Euclidean geometry. His work was influential in the development of analytic geometry, calculus, and cartography.

The idea of a Cartesian product was developed in 1637 in two writings by Descartes. In part two of his Discourse de la Méthode, Descartes introduces the new idea of specifying the position of a point or object on a surface, using two intersecting axes as measuring guides. This is exactly the way one nowadays uses $\mathbb{R}^2$ as a coordinate system for the real plane. In La Géométrie, he further explores the above-mentioned concepts.

2.5 Partitions

Definition 2.5.1. Let S be a nonempty set. A collection Π of subsets of S is called a *partition* if and only if
(a) $\emptyset \notin \Pi$;
(b) $\bigcup_{X\in\Pi} X = S$;
(c) for all $X \neq Y \in \Pi$ we have $X \cap Y = \emptyset$.

Example 2.5.2. The set $\{1,2,\ldots,10\}$ can be partitioned into the sets $\{1,2,3\}$, $\{4,5\}$ and $\{6,7,8,9,10\}$.

Example 2.5.3. Suppose $\mathscr{L}$ is the set of all lines in $\mathbb{R}^2$ parallel to a fixed line ℓ. Then $\mathscr{L}$ partitions $\mathbb{R}^2$.

Example 2.5.4. Let $n > 1$ be an integer. Then the set $\mathbb{Z}$ can be partitioned into the following subsets:

$$\begin{gathered}\{z \in \mathbb{Z} \mid z = 0 + nx \text{ for some } x \in \mathbb{Z}\}\\ \{z \in \mathbb{Z} \mid z = 1 + nx \text{ for some } x \in \mathbb{Z}\}\\ \vdots\\ \{z \in \mathbb{Z} \mid z = (n-1) + nx \text{ for some } x \in \mathbb{Z}\}.\end{gathered}$$

2.6 Quantifiers

In many statements and assertions we find phrases like "For all x we have ..." or "There exists an x with ...". This kind of phrases can be expressed using quantifiers.

Definition 2.6.1. Let P be a predicate on a reference set X. Then by

$$\forall x \in X\ [P(x)]$$

we denote the assertion "For all $x \in X$ the assertion $P(x)$ is true".
$\forall$ is called the *for all*-quantifier or *universal quantifier*.
By

$$\exists x \in X\ [P(x)]$$

we denote the assertion " There exists an $x \in X$ with $P(x)$ true".
$\exists$ is called the *existential* quantifier.

Sometimes we might also encounter the quantifier $\exists!$, which represents "there is a unique".

Example 2.6.2. The following statements are true:

$$\forall x \in \mathbb{R}\ [x \geq 0 \Rightarrow |x| = x],$$

$$\exists x \in \mathbb{R}\ [|x| = x],$$

$$\forall x \in \mathbb{Q}\ [-1 < \sin(x) < 1].$$

Here a few statements that are false:

$$\forall x \in \mathbb{R}\ [|x| = x],$$

$$\forall x \in \mathbb{R}\ [-1 < \sin(x) < 1].$$

Example 2.6.3. We can make combinations of quantifiers to create various assertions. For example

$$\forall x \in \mathbb{Z}\, \exists y \in \mathbb{Z}\ [x + y = 0]$$

which reads as: for all $x \in \mathbb{Z}$ there exists a $y \in \mathbb{Z}$ such that $x + y = 0$. Clearly this statement is true, since for each $x \in \mathbb{Z}$ we can take y to be equal to $-x$.

Proposition 2.6.4 — DeMorgan's rule. The statement

$$\neg(\forall x \in X[P(x)])$$

is equivalent with the statement

$$\exists x \in X\ [\neg(P(x))].$$

The statement

$$\neg(\exists x \in X[P(x)])$$

is equivalent with the statement

$$\forall x \in X\ [\neg(P(x))].$$

Example 2.6.5. Let $X = \{1,2,\ldots,9\}$ and consider the following statements.

$$P = \forall x \in X\, \exists y \in X\ [x+y = 10]$$

and

$$Q = \exists x \in X\, \forall y \in X\ [x+y = 10].$$

The assertion P is true. Indeed, for $x = 1$ we can choose $y = 9$, for $x = 2$ we choose $y = 8$ and so on. In general, for $x \in X$ we can choose y to be equal to $10 - x$.

The assertion Q is false. We prove $\neg Q$. By DeMorgan's rule 2.6.4 the assertion $\neg Q$ is equivalent with

$$R = \forall x \in X \exists y \in X\ [x+y \neq 10].$$

So it suffices to prove the latter assertion. Let $x \in X$ and choose $y = 1$ if $x \neq 9$ and 2 otherwise. Then $x+y \neq 10$. This proves R and hence $\neg Q$.

To prove statements of the form

$$\forall x \in X\ [P(x)]$$

or

$$\exists x \in X\ [P(x)]$$

one can proceed as follows.

First a statement of the form $\forall x \in X\ [P(x)]$. A proof usually starts then with the assumption that $x \in X$, without specifying the value of x. Then one argues that $P(x)$ is a true statement. As x is not specified, one has proven $P(x)$ for all x.

Here is an example.

Example 2.6.6. We prove

$$\forall x \in \mathbb{R}\ [x > 0 \Rightarrow x + \frac{1}{x} \geq 2].$$

Let $x \in \mathbb{R}$. Then $(x-1)^2 = x^2 - 2x + 1 \geq 0$ and hence $x^2 + 1 \geq 2x$. So, if $x > 0$, then dividing by x yields $x + \frac{1}{x} \geq 2$.

We conclude that for all $x \in \mathbb{R}$ we have $x > 0 \Rightarrow x + \frac{1}{x} \geq 2$.

To prove a statement of the form

$$\exists x \in X\ [P(x)],$$

one has to provide an explicit $x \in X$ for which $P(x)$ is true.

Example 2.6.7. We show

$$\exists x \in \mathbb{R}\ [x + \frac{4}{x} = 4].$$

Take $x = 1$, then $x + \frac{4}{x} = 2 + \frac{4}{2} = 2 + 2 = 4$. So, indeed, there is an $x \in \mathbb{R}$, namely $x = 2$ with $x + \frac{4}{x} = 4$.

Notice that you do not need to explain how $x = 4$ has been found, but only that it does satisfy $x + \frac{4}{x} = 2$.

Example 2.6.8. To prove that a function $f : \mathbb{R} \to \mathbb{R}$ is continuous in a, we need to prove

$$\forall \varepsilon > 0\ \exists \delta > 0\ \forall x \in \mathbb{R}\ [0 < |x-a| < \delta \Rightarrow |f(x) - f(a)| < \varepsilon].$$

We will show that if $f(x) = x^2$ for all $x \in \mathbb{R}$, then f is continuous for all $a \in \mathbb{R}$. So we prove

$$\forall a \in \mathbb{R}\ \forall \varepsilon > 0\ \exists \delta > 0\ \forall x \in \mathbb{R}\ [0 < |x-a| < \delta \Rightarrow |f(x) - f(a)| < \varepsilon].$$

So, let $a \in \mathbb{R}$ and take an $\varepsilon > 0$. (We take a and ε without specifying their value). Now let $\delta = \min(1, \frac{\varepsilon}{|2a|+1})$. (We take a specific value for δ.)

Then for all x with $0 < |x-a| < \delta$ we have

$$\begin{aligned} |f(x) - f(a)| &= |x^2 - a^2| \\ &= |x-a| \cdot |x+a| \\ &< \delta \cdot (|x| + |a|) \\ &\leq \delta \cdot (2|a| + 1) \\ &\leq \varepsilon \end{aligned} \quad .$$

So, for all $a \in \mathbb{R}$ and $\varepsilon > 0$ there is an element $\delta > 0$, namely $\delta = \min(1, \frac{\varepsilon}{|2a|+1})$, such that for all $x \in \mathbb{R}$ we have that if $0 < |x-a| < \delta$, then $|f(x) - f(a)| < \varepsilon$.

We have proven the function f to be continuous on $\mathbb{R}$.

Warning. 2.6.9 In the above example it is important that you work from start to finish in the order as indicated. Often the following type of "proof" is given.

$|x^2 - a^2| < \varepsilon$

$|x-a| \cdot |x+a| < \varepsilon$

$\delta \cdot |x+a| < \varepsilon$

$\delta \cdot (|x| + |a|) < \varepsilon$ when $\delta < 1$

$\delta \cdot (2 \cdot |a| + 1) < \varepsilon$

So, choose $\delta = \min(1, \frac{\varepsilon}{2 \cdot |a| + 1})$.

Even when the relation between the various lines of this computation is explained, this is not the right way to write it down. This is what you can do on scratch paper. In the final proof, you should work as in the example above.

2.7 Exercises

Exercise 2.7.1. Which of the following sets are equal to each other: $\emptyset$, $\{0\}$, $\{\emptyset\}$?

Exercise 2.7.2. What are the sets that have no proper subset?

Exercise 2.7.3. How many elements does the set $\{\emptyset, \{\emptyset\}, \emptyset\}$ have?

Exercise 2.7.4. Suppose $A = \{\{1\}, \{2,3\}\}$. Which of the following is true: $\{1\} \subseteq A$, $\{2,3\} \subseteq A$, $\{\{2,3\}\} \subseteq A$?

Exercise 2.7.5. Suppose $A = \{0, \{1,2\}\}$. Give all subsets of $\mathscr{P}(A)$.

Exercise 2.7.6. Suppose a set A contains n elements. How many elements does $\mathscr{P}(A)$ have?

Exercise 2.7.7. Which of the following statements is true for all sets A, B and C? Give a proof or a counter example.

(a) $A \subseteq ((A \cap B) \cup C)$.

(b) $(A \cup B) \cap C = (A \cap B) \cup C$.
(c) $(A \setminus B) \cap C = (A \cap C) \setminus (B \cap C)$.

Exercise 2.7.8. Let A, B and C be sets. Prove the following.
(a) If $A \subseteq B$, then $(A \cup C) \subseteq (B \cup C)$.
(b) If $A \subseteq C$ and $B \subseteq C$, then $(A \cup B) \subseteq C$.
(c) If $A \cup B = A \cap B$, then $A = B$.

Exercise 2.7.9. Suppose A and B are sets. Show the following.
(a) $A \setminus (B \setminus A) = A$.
(b) $A \cup B = (A \setminus B) \cup (A \cap B) \cup (B \setminus A)$
(c) If $A \triangle B = A$, then $B = \emptyset$.

Exercise 2.7.10. Suppose T is a set of sets with the property that for all $A, B \in T$ also $(A \setminus B) \in T$. Prove that for $A, B \in T$ also $A \cap B \in T$.

Exercise 2.7.11. Which of the following sets is empty?
(a) $\{x \in \mathbb{R} \mid x^2 = 9 \text{ and } 2x = 4\}$.
(b) $\{x \in \mathbb{R} \mid x \neq x\}$.
(c) $\{x \in \mathbb{R} \mid x + 8 = 8\}$.
(d) $\{x \in \mathbb{R} \mid x^2 = 3 \text{ or } x^2 = 1\}$.
(e) $\{x \in \mathbb{R} \mid x^2 \geq -1\}$.

Exercise 2.7.12. Give a description of the form $\{x \in X \mid P(x)\}$ for each of the following sets.
(a) the even integers.
(b) the circles in $\mathbb{R}^2$ with radius 2.
(c) the lines in $\mathbb{R}^2$ parallel to the y-axis.

Exercise 2.7.13. Describe the following sets using assertions involving $x \in A$, $x \in B$, $x \in C$ and the symbols $\neg$, $\wedge$ and $\vee$
(a) $(A \setminus B) \cap C$;
(b) $(A \cup B) \cap C^*$;
(c) $(A \setminus C) \cup (B \cap C)$.

Exercise 2.7.14. Express the following sets using the symbols A, B, C and operators $\cap$, $\cup$, * and $\setminus$.
(a) $\{x \mid ((x \in A) \wedge (x \in B)) \vee (x \in C)\}$;
(b) $\{x \mid (x \in A) \vee ((x \in B) \wedge (x \in C))\}$
(c) $\{x \mid ((x \notin A) \wedge (x \notin B)) \vee (x \notin C)\}$.

Exercise 2.7.15. Which of the following is true?
(a) $\forall x \in \mathbb{R}\, \exists y \in \mathbb{R}\, [x^2 \geq y]$;
(b) $\exists x \in \mathbb{R}\, \forall y \in \mathbb{R}\, [x^2 \geq y]$;
(c) $\forall y \in \mathbb{R}\, \exists x \in \mathbb{R}\, [x^2 \geq y]$;
(d) $\exists y \in \mathbb{R}\, \forall x \in \mathbb{R}\, [x^2 \geq y]$.

Exercise 2.7.16. (a) Give an infinite sequence $a_1, a_2, \ldots$ such that

$$\forall m \in \mathbb{N}\, \exists k \in \mathbb{R}\, \forall n \geq m\, [a_n \geq k].$$

Also provide a sequence for which the above statement is false.
(b) Same question for the statement

$$\exists m \in \mathbb{N}\, \forall k \in \mathbb{R}\, \exists n \geq m\, [a_n \geq k].$$

(c) Same questions for

$$\neg(\exists m \in \mathbb{N}\, \forall k \in \mathbb{R}\, \exists n \geq m\, [a_n \geq k]).$$

Exercise 2.7.17. Provide a finite set $V \subseteq \mathbb{N}$ for which

$$\forall z \in \mathbb{N}\, \exists x \in V\, \forall y \in V\ [x + y \neq z].$$

Also provide a finite set $V \subseteq \mathbb{N}$ for which

$$\neg(\forall z \in \mathbb{N}\, \exists x \in V\, \forall y \in V\ [x + y \neq z]).$$

3. Relations

3.1 Binary relations

Definition 3.1.1. A (binary) *relation* R between the sets S and T is a subset of the Cartesian product $S \times T$.

Suppose R is a relation between the sets S and T. If $(a,b) \in R$, we say a is in relation R to b. We denote this by aRb. The set S is called the *domain* of the relation R and the set T the *codomain*. If $S = T$ we say R is a relation on S.

Example 3.1.2. We give some examples:

(a) "Is the mother of" is a relation between the set of all females and the set of all people. It consists of all the pairs $(\text{person } 1, \text{person } 2)$ where person 1 is the mother of person 2.

(b) "There is a train connection between" is a relation between the cities of the Netherlands.

(c) The identity relation "$=$" is a relation on a set S. This relation is often denoted by I. So,

$$I = \{(s,s) \mid s \in S\}.$$

(d) We say an integer n divides an integer m, notation $n \mid m$, if there is an element $q \in \mathbb{Z}$ such that $qn = m$. Divides $\mid$ is a relation on $\mathbb{Z}$ consisting of all the pairs $(n,m) \in \mathbb{Z} \times \mathbb{Z}$ with $n \mid m$.

(e) "Greater than" $>$ or "less than" $<$ are relations on $\mathbb{R}$.

(f) $R = \{(0,0),(1,0),(2,1)\}$ is a relation between the sets $S = \{0,1,2\}$ and $T = \{0,1\}$.

(g) $R = \{(x,y) \in \mathbb{R}^2 \mid y = x^2\}$ is a relation on $\mathbb{R}$.

(h) Let Ω be a set, then "is a subset of" $\subseteq$ is a relation on the set $S = \mathscr{P}(\Omega)$ of all subsets of Ω.

Besides binary relations one can also consider n-ary relations with $n \geq 0$. An n-ary relation R on the sets $S_1, \ldots, S_n$ is a subset of the Cartesian product $S_1 \times \cdots \times S_n$. In these notes we will restrict our attention to binary relations. Unless stated otherwise, a relation will be assumed to be binary.

Leonard Euler, founder of graph theory, painting by J. Darbes, State Tretyakov Gallery, Moskou ©Public Domain

Definition 3.1.3. Let R be a relation from a set S to a set T. Then for each element $a \in S$ we define $[a]_R$ to be the set

$$[a]_R := \{b \in T \mid aRb\}.$$

(Sometimes this set is also denoted by $R(a)$.) This set is called the *(R-) image* of a.

For $b \in T$ the set

$$_R[b] := \{a \in S \mid aRb\}$$

is called the (R-) *pre-image* of b or *R-fiber* of b.

Relations between finite sets can be described using matrices.

Definition 3.1.4. If $S = \{s_1, \ldots, s_n\}$ and $T = \{t_1, \ldots, t_m\}$ are finite sets and $R \subseteq S \times T$ is a binary relations, then the *adjacency matrix* A_R of the relation R is the $n \times m$ matrix whose rows are indexed by S and columns by T defined by

$$A_{s,t} = \begin{cases} 1 & \text{if } (s,t) \in R; \\ 0 & \text{otherwise.} \end{cases}$$

Notice that a presentation of the adjacency matrix of a relation is defined up to permutations of the rows and columns of the matrix. If the sets S and T are equal, then it is customary to put the rows in the same order as the columns.

If $s \in S$, then $[s]_R$ consists of those $t \in T$ such that the entry t of the row s in A_R equals 1. For $t \in T$ the set $_R[t]$ consists of the elements $s \in S$ for which the entry s in the column t is nonzero.

Example 3.1.5. (a) The adjacency matrix of the relation $R = \{(0,0),(1,0),(2,1)\}$ between the sets $S = \{0,1,2\}$ and $T = \{0,1\}$ equals

$$\begin{pmatrix} 1 & 0 \\ 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

(We number rows from top to bottom and columns from left to right.)

(b) The adjacency matrix of the identity relation on a set S of size n is the $n \times n$ identity matrix

$$I_n = \begin{pmatrix} 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & & \ddots & & \vdots \\ 0 & 0 & \cdots & 1 & 0 \\ 0 & 0 & \cdots & 0 & 1 \end{pmatrix}.$$

(c) The adjacency matrix of relation $\leq$ on the set $\{1,2,3,4,5\}$ is the upper triangular matrix

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

A graphical presentation of a relation R between a set S and a set T can be given as follows. We draw the two sets S and T as Venn diagrams and draw an arrow from an element $s \in S$ to an element t in T if and only if sRt.

Example 3.1.6. Let $S = \{1,2,3,4,5\}$ and $T = \{a,b,c,d,e\}$. The relation $R = \{(1,b),(2,a),(2,c),(3,c),(5,d)\}$ can be described by the drawing in Figure 3.1.

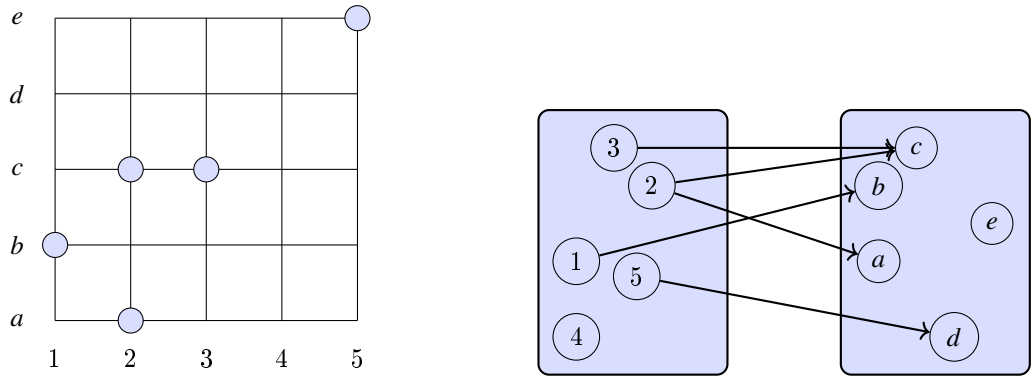


Figure 3.1: Graphical presentations of the relation R

Some relations have special properties:

Definition 3.1.7. Let R be a relation on a set S. Then R is called
- *Reflexive* if for all $x \in S$ we have $(x,x) \in R$;
- *Irreflexive* if for all $x \in S$ we have $(x,x) \notin R$;
- *Symmetric* if for all $x,y \in S$ we have xRy implies yRx;
- *Antisymmetric* if for all $x,y \in S$ we have that xRy and yRx implies $x = y$;
- *Transitive* if for all $x,y,z \in S$ we have that xRy and yRz implies xRz.

Example 3.1.8. We consider some of the examples given above:
(a) "Is the mother of" is a relation on the set of all people. This relation is irreflexive, antisymmetric and not transitive.
(b) "There is a train connection between" is a symmetric and transitive relation.
(c) "$=$" is a reflexive, symmetric and transitive relation on a set S.
(d) Divides $|$ is a reflexive, antisymmetric and transitive relation on $\mathbb{N}$.
(e) "Greater than" $>$ or "less than" $<$ on $\mathbb{R}$ are irreflexive, antisymmetric and transitive.
(f) The relation $R = \{(x,y) \in \mathbb{R}^2 \mid y = x^2\}$ is not reflexive nor irreflexive.

If R is a relation on a finite set S, then special properties like reflexivity, symmetry and transitivity can be read of from the adjacency matrix A. For example, the relation R on a set S is reflexive if and only if the main diagonal of A only contains 1's, i.e., $A_{s,s} = 1$ for all $s \in S$.

The relation R is symmetric if and only if the transposed matrix $A^\top$ of A equals A. (The *transposed matrix* $M^\top$ of an $n \times m$ matrix M is the $m \times n$ matrix with entry i,j equal to $M_{j,i}$.)

3.2 Relations and Directed Graphs

Definition 3.2.1. A *directed edge* of a set V is an element of $V \times V$. If $e = (v,w)$ is a directed edge of V, then v is called its *tail* and w its *head*. Both v and w are called *end points* of the edge e. The *reverse* of the edge e is the edge (w,v). A *loop* is an edge from a vertex to itself.

A *directed graph* (also called *digraph*) $\Gamma = (V,E)$ consists of a set V of *vertices* and a subset E of $V \times V$ of (directed) *edges*. The elements of V are called the *vertices* of Γ and the elements of E the *edges* of Γ.

Clearly, the edge set of a directed graph is a relation on the set of vertices. Conversely, if R is a binary relation on a set S, then R defines a *directed graph* (S,R) on the set S, which we denote by Γ_R. Hence there is

a one-to-one correspondence between directed graphs and relations on a set V (or S). It is often convenient to switch from a relation to the corresponding digraph or back.

In this subsection we introduce some graph theoretical language and notation to be used in the sequel.

Suppose $\Gamma = (V,E)$ is a digraph. A *walk* from v to w, where $v,w \in V$, is a sequence $v_0, v_1, \ldots, v_k$ of vertices with $v_0 = v$, $v_k = w$ and $(v_i, v_{i+1}) \in E$ for all $0 \leq i < k$. A *path* from v to w is a walk from v to w in which all vertices, except possibly the first vertex v and the last vertex w are different.

An *undirected walk* from v to w is a sequence $v_0, v_1, \ldots, v_k$ of vertices with $v_0 = v$, $v_k = w$ and (v_i, v_{i+1}) or $(v_{i+1}, v_i) \in E$ for all $0 \leq i < k$, while an *undirected path* from v to w is an undirected walk in which all vertices except possibly the first and last. are different. The *length* of the (directed or undirected) walk or path is k. A *cycle* is a path form v to v of length at least 1.

If $v,w \in V$ are vertices of the digraph Γ, then the *distance* from v to w is the minimum of the lengths of the paths from v to w. The distance is set to ∞ (infinity) if there is no path from v to w.

The digraph is called *weakly connected* if for any two vertices v and w there is an undirected path between v and w. It is called *strongly connected* if there exist paths in both directions.

If W is a subset of V, then the induced subgraph of Γ on W is the digraph $(W, E \cap (W \times W))$. A *(weakly) connected component* C of Γ is a maximal subset of V such that the induced subgraph is (weakly) connected.

If we define the relation R on V by vRw if and only if there is an undirected path from v to w, then R is an equivalence relation. The weakly connected components of Γ are then the R-equivalence classes.

A *strongly connected component* is a maximal subset of V such that the induced subgraph is strongly connected.

Let S be the relation on the set V where vSw if there is an directed path from v to w and from w to v.

Then S is an equivalence relation. (Proof this!) The strongly connected components are then the S-equivalence classes.

As we can identify a directed graph with the corresponding relation, we can of course represent the graph by its adjacency matrix as well as by a diagram as in 3.1.6. However, as a directed graph $\Gamma = (V,E)$ defines a relation on a set V, there is no need to draw this set twice. The usual way that we draw the graph Γ is to draw the vertices of V with arrows from a vertex $v \in V$ to a vertex $w \in V$ if and only if $(v,w) \in E$.

Example 3.2.2. Here we draw a graph on the vertex set $V = \{1,2,3,4,5,6,7,8\}$. The edge set is

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

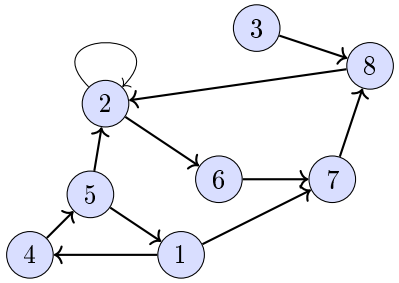


Figure 3.2: Drawing of a directed graph

The graph $\Gamma = (V,E)$ is weakly connected, but not strongly connected. For example, there is no path from 8 to 3. The strongly connected components are $\{1,4,5\}$, $\{2,6,7,8\}$ and $\{3\}$.

The distance between the vertex 4 and 8 is equal to 4. A shortest path from 4 to 8 is $4,5,1,7,8$.

We connect various properties of a relation with those of the related digraph.

Proposition 3.2.3. Let (V,E) be a directed graph. Then we have the following.
(a) E is reflexive if and only if every vertex $v \in V$ is in a loop.
(b) E is symmetric if and only if for every edge $e \in E$, also its reverse is in E.
(c) E is transitive if and only if for each walk of length at least 1 starting in x and ending in y we have that $(x,y) \in E$

Proof. We provide a proof of (c).

Suppose R is a transitive relation on V.

Let $x,y \in V$ be two vertices and suppose there is a shortest path $x = x_0, x_1, \ldots, x_n = y$ between x and y of length $n > 1$.

Then $x_0 R x_1$ and $x_1 R x_2$. So, by transitivity, $x_0 R x_2$ and we find a path $x = x_0, x_2, \ldots, x_n = y$ of length $n-1$ from x to y, contradicting that $x = x_0, x_1, \ldots, x_n = y$ is a shortest path between x and y of length $n > 1$.

Hence all shortest paths have length at most 1.

Assume that in Γ two vertices are either adjacent or their distance is ∞, implying that there is no path between them.

Then suppose $x,y,z \in V$ with xRy and yRz. Inside Γ we find that there is a path x,y,z of length two from x to z. So, the distance between x and z is at most 2, and by assumption equal to one. But that implies xRZ and we find the relation R to be transitive. □

Example 3.2.4. The complete directed graph on a vertex set V is the graph in which all vertices are adjacent to each other and themselves. This graph is clearly strongly connected.

So, the corresponding relation is reflexive, symmetric and transitive.

Proposition 3.2.5. Let R be a relation on the set V which is reflexive, symmetric and transitive. Then all (weakly) connected components of the graph $\Gamma = (V,R)$ are complete graphs.

Proof. Let R be a reflexive, symmetric and transitive relation on the set V and consider the graph $\Gamma = (V,R)$.

By reflexivity, all vertices are adjacent to themselves.

Suppose v and w are vertices that are in the same weakly connected component C of Γ. Then by transitivity and the above proposition, there is an edge between them, and by symmetry, even an edge in both directions. But that implies that in the connected component C all vertices are adjacent to each other and themselves. The component C is a complete graph. □

Definition 3.2.6. Let $\Gamma = (V,E)$ be a digraph and $v \in V$ a vertex. The *indegree* of v is the number of edges with v as head. The *outdegree* of v is the number of edges with v as tail.

Example 3.2.7. Let $\Gamma = (V,E)$ be a finite digraph in which all vertices have indegree and outdegree equal to 1. Then Γ is a disjoint union of cycles.

To prove this, let $v_0 \in V$. As v_0 has outdegree 1, there is a unique neighbor v_1 of v_0 (which can be equal to v_0). Add then v_2 the unique neighbor of v_1. Continue in this way to find a (unique) walk $v_0, v_1, v_2, \ldots, v_n$. As $|V| = n$ is finite there needs to be a vertex that appears at least twice in this walk. Let v_i be that vertex with i minimal, and suppose $v_i = v_k$ for some $k > i$. If $i > 0$, then the vertex v_{i-1} and v_{k-1} both are tails of an edge to $v_i = v_k$. However, as the indegree of v_i equals 1 we have $v_{i-1} = v_{k-1}$, contradicting minimality of i. We conclude that $i = 0$ and find v_0 to be in a cycle, which clearly is unique.

This implies that every vertex of Γ is in a unique cycle and not adjacent to any other vertex of Γ outside the cycle. So Γ is a disjoint union of such cycles.

Next to digraphs, we will also encounter *graphs* in these notes. A *graph* is a pair (V,E) of sets V of vertices and E of edges, where edges are subsets of V of size at most 2. Edges of size 1 are called *loops*. An ordinary graph is a graph without loops.

To each digraph we can associate the corresponding graph by replacing the directed edges (v,w) by the corresponding subset $\{v,w\}$.

3.3 Equivalence relations

As we noticed in Example 3.1.8, "being equal" is a reflexive, symmetric and transitive relation on any set S. Relations having these three properties deserve some special attention.

Definition 3.3.1. A relation R on a set S is called an *equivalence relation* on S if and only if it is reflexive, symmetric and transitive.

Example 3.3.2. Consider the plane $\mathbb{R}^2$ and in it the set S of straight lines. We call two lines parallel in S if and only if they are equal or do not intersect. Notice that two lines in S are parallel if and only if their slopes are equal. Being parallel defines an equivalence relation on the set S.

Example 3.3.3. Fix $n \in \mathbb{Z}$, $n \neq 0$, and consider the relation R on $\mathbb{Z}$ by aRb if and only if $a-b$ is divisible by n. We also write $a = b \pmod{n}$.

The relation R is an equivalence relation. Indeed, suppose $a,b,c \in \mathbb{Z}$. Then

(a) aRa as $a-a=0$ is divisible by n.
(b) If aRb, then $a-b$ is divisible by n and hence also $b-a$. Thus bRa.
(c) If aRb and bRc, then n divides both $a-b$ and $b-c$ and then also $(a-b)+(b-c)=a-c$. So aRc.

Example 3.3.4. Let Π be a partition of the set S, i.e., Π is a set of nonempty subsets of S such that each element of S is in a unique member of Π. In particular, the union of all members of Π yields the whole set S and any two members of Π have empty intersection.

We define the relation R_Π as follows: $a,b \in S$ are in relation R_Π if and only if there is a subset X of S in Π containing both a and b. We check that the relation R_Π is an equivalence relation on S.

- Reflexivity. Let $a \in S$. Then there is an $X \in \Pi$ containing a. Hence $a,a \in X$ and $aR_\Pi a$
- Symmetry. Let $aR_\Pi b$. Then there is an $X \in \Pi$ with $a,b \in X$. But then also $b,a \in X$ and $bR_\Pi a$.
- Transitivity. If $a,b,c \in S$ with $aR_\Pi b$ and $bR_\Pi c$, then there are $X,Y \in \Pi$ with $a,b \in X$ and $b,c \in Y$. However, then b is in both X and Y. But then, as Π partitions S, we have $X = Y$. So $a,c \in X$ and $aR_\Pi c$.

The following theorem implies that every equivalence relation on a set S can be obtained from a partition of the set S. But first a lemma:

Lemma 3.3.5. Let R be an equivalence relation on a set S. If $b \in [a]_R$, then $[b]_R = [a]_R$.

Proof. Suppose $b \in [a]_R$. Thus aRb. If $c \in [b]_R$, then bRc and, as aRb, we have by transitivity aRc. In particular, $[b]_R \subseteq [a]_R$.

Since, by symmetry of R, aRb implies bRa and hence $a \in [b]_R$, we similarly get $[a]_R \subseteq [b]_R$. □

Definition 3.3.6. Let R be an equivalence relation on a set S. Then the sets $[s]_R$, where $s \in S$ are called the *R-equivalence classes* on S.

We denote the set of R-equivalence classes by S/R.

If we consider the directed graph $\Gamma = (S,R)$, then as we have seen in 3.2.5, we can identify the equivalence class of an element $a \in S$ with the connected component of Γ in which a lies. The equivalence classes are then the connected components of Γ. No surprise that we have the following:

Theorem 3.3.7. Let R be an equivalence relation on a set S. Then the set S/R of R-equivalence classes partitions the set S.

Proof. Let Π_R be the set of R-equivalence classes. Then by reflexivity of R we find that each element $a \in S$ is inside the class $[a]_R$ of Π_R.

If an element $a \in S$ is in the classes $[b]_R$ and $[c]_R$ of Π, then by the previous lemma we find $[b]_R = [a]_R$ and $[c]_R = [a]_R$. In particular $[b]_R$ equals $[c]_R$. Thus each element $a \in S$ is inside a unique member of Π_R, which therefore is a partition of S. □

Example 3.3.8 — Construction of $\mathbb{Q}$. The rational numbers can be constructed from the integers with the help of an equivalence relation.

We consider the set $V = \mathbb{Z} \times \mathbb{Z} \setminus \{0\}$. On V we define the relation $\equiv$ by

$$(a,b) \equiv (c,d) \Leftrightarrow a \cdot d = b \cdot c$$

for all (a,b) and (c,d) in V.

Now we denote the $\equiv$-equivalence class of a pair (a,b) by $\frac{a}{b}$. Then $\frac{a}{b} = \frac{c}{d}$ if and only if $ad = bc$. Clearly we have $(1,2) \equiv (2,4)$ and hence $\frac{1}{2} = \frac{2}{4}$. More generaly, we have

$$\frac{mp}{mq} = \frac{p}{q}$$

for all $p,q,m \in \mathbb{Z}$ with $q \cdot m$ different from 0.

By $\mathbb{Q}$ we denote the set of all $\equiv$-classes of V, so $\mathbb{Q} = V/\equiv$. This is indeed the set of all rational numbers as we are used to. So, we constructed the set of all rational numbers. But of course, we also want to compute with them.

How can we define addition, multiplication and division on $\mathbb{Q}$?

We start with addition. Consider two $\equiv$-equivalence classes $\frac{a}{b}$ and $\frac{c}{d}$. We define

$$\frac{a}{b} + \frac{c}{d} = \frac{ad+cb}{bd}.$$

This is what we want. However, we still have to check that this is well-defined. Indeed, this definition depends on the particular elements (a,b) in class $\frac{a}{b}$ and (c,d) in the class $\frac{c}{d}$. If we choose other elements in the same $\equiv$-classes, do we get the same class after addition?

For example, $\frac{2}{3} = \frac{4}{6}$ and $\frac{1}{2} = \frac{2}{4}$, but is

$$\frac{2}{3} + \frac{1}{2} = \frac{7}{6}$$

equal to

$$\frac{4}{6} + \frac{2}{4} = \frac{28}{24}?$$

Is

$$(7,6) \equiv (28,24)?$$

Yes,

$$(7,6) \equiv (28,24),$$

as we can easily check.

But we have to show that this definition in general is independent of the choices of (a,b) and (c,d) in their $\equiv$-classes. So, suppose $(a',b') \equiv (a,b)$ and $(c',d') \equiv (c,d)$ is then

$$\frac{a'}{b'} + \frac{c'}{d'} = \frac{a}{b} + \frac{c}{d}?$$

We have to check that $(a'd' + c'b', b'd') \equiv (ad + cb, bd)$. But this follows from

$$\begin{aligned} (a'd' + c'b') \cdot bd &= (a'd')(bd) + (c'b')(bd) \\ &= (a'b)(d'd) + (c'd)(b'b) \\ \text{(using } a'b = ab' \text{ and } c'd = cd') \quad &= (ab')(d'd) + (cd')(b'b) \\ &= (ad + bc)(b'd'). \end{aligned}$$

We have constructed $\mathbb{Q}$ as well as the sum and product of rational numbers. Similarly we check that division can also be defined properly on $\mathbb{Q}$.

3.4 Composition of Relations

If R_1 and R_2 are two relations between a set S and a set T, then we can form new relations between S and T by taking the intersection $R_1 \cap R_2$ or the union $R_1 \cup R_2$. Also the complement of R_2 in R_1, $R_1 \setminus R_2$, is a new relation. Furthermore we can consider a relation $R^\top$ (sometimes also denoted by R^{-1}, $R^\sim$ or $R^\vee$) from T to S as the relation $\{(t,s) \in T \times S \mid (s,t) \in R\}$.

Another way of making new relations out of old ones is the following. If R_1 is a relation between S and T and R_2 is a relation between T and U then the *composition or product* $R = R_1;R_2$ (sometimes denoted by $R_2 \circ R_1$ or $R_1 * R_2$) is the relation between S and U defined by sRu for $s \in S$ and $u \in U$, if and only if there is a $t \in T$ with sR_1t and tR_2u.

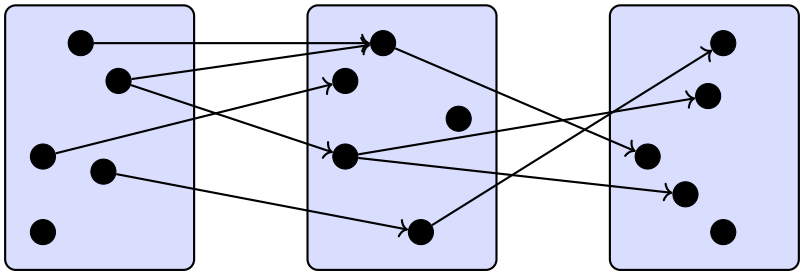


Figure 3.3: Product of two relations

Example 3.4.1. Suppose R_1 is the relation $\{(1,2),(2,3),(3,3),(2,4)\}$ from $\{1,2,3\}$ to $\{1,2,3,4\}$ and R_2 the relation $\{(1,a),(2,b),(3,c),(4,d)\}$ from $\{1,2,3,4\}$ to $\{a,b,c,d\}$. Then $R_1;R_2$ is the relation

$$\{(1,b),(2,c),(3,c),(2,d)\}$$

from $\{1,2,3\}$ to $\{a,b,c,d\}$.

Suppose R_1 is a relation from S to T and R_2 a relation from T to U with adjacency matrices A_1 and A_2, respectively. Consider the matrix product $M = A_1A_2$. An entry $M_{s,u}$ is obtained by multiplying row s from A_1 with column u from A_2 and equals the number of $t \in T$ with $(s,t) \in R_1$ and $(t,u) \in R_2$.

Notice, if $R_1 = R_2$, then entry s,t equals the number of paths of length 2 in Γ_R starting in s and ending in t.

The adjacency matrix A of $R_1;R_2$ can be obtained from M by replacing every nonzero entry by a 1.

Example 3.4.2. Suppose $R_1 = \{(1,2),(2,3),(3,3),(2,4),(3,1)\}$ from $\{1,2,3\}$ to $\{1,2,3,4\}$ and $R_2 = \{(1,1),(2,3),(3,1),(3,3),(4,2)\}$ from $\{1,2,3,4\}$ to $\{1,2,3\}$. Then the adjacency matrices A_1 and A_2 for R_1 and R_2 are

$$A_1 = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 \end{pmatrix}, A_2 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}.$$

The product of these matrices equals

$$M = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 1 & 1 \\ 2 & 0 & 1 \end{pmatrix}.$$

So, the adjacency matrix of $R_1;R_2$ is

$$\begin{pmatrix} 0 & 0 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix}.$$

Proposition 3.4.3. Suppose R_1 is a relation from S to T, R_2 a relation from T to U and R_3 a relation from U to V. Then $R_1;(R_2;R_3) = (R_1;R_2);R_3$.

Composing relations is associative.

Proof. Suppose $s \in S$ and $v \in V$ with $sR_1;(R_2;R_3)v$. Then we can find a $t \in T$ with sR_1t and $t(R_2;R_3)v$. But then there is also a $u \in U$ with tR_2u and uR_3v. For this u we have $sR_1;R_2u$ and uR_3v and hence $s(R_1;R_2);R_3v$.

Similarly, if $s \in S$ and $v \in V$ with $s(R_1;R_2);R_3v$, then we can find a $u \in U$ with $s(R_1;R_2)u$ and uR_3v. But then there is also a $t \in T$ with sR_1t and tR_2u. For this t we have $tR_2;R_3u$ and sR_1t and hence $sR_1;(R_2;R_3)v$. □

Let R be a relation on a set S and denote by I the identity relation on S, i.e., $I = \{(a,b) \in S \times S \mid a = b\}$. Then we easily check that $I;R = R;I = R$.

Let R be a relation on a set S and consider the directed graph Γ_R with vertex set S and edge set R. Then two vertices a and b are in relation $R^2 = R;R$, if and only if there is a $c \in S$ such that both (a,c) and $(c,b) \in R$. Thus aR^2b if and only if there is a path of length 2 from a to b.

For $n \in \mathbb{N}$, the n-th power R^n of the relation R is recursively defined by $R^0 = I$ and $R^{n+1} = R;R^n$. Two vertices a and b are in relation R^n if and only if, inside Γ_R, there is a path from a to b of length n.

We notice that whenever R is reflexive, we have $R \subseteq R^2$ and thus also $R \subseteq R^n$ for all $n \in \mathbb{N}$ with $n \geq 1$. Actually, a and b are then in relation R^n if and only if they are at distance $\leq n$ in the graph Γ_R.

3.5 Transitive Closure

Lemma 3.5.1. Let $\mathscr{C}$ be a collection of relations R on a set S. If all relations R in $\mathscr{C}$ are transitive (symmetric or reflexive), then the relation $\bigcap_{R\in\mathscr{C}} R$ is also transitive (symmetric or reflexive, respectively).

Proof. Let $\overline{R} = \bigcap_{R\in\mathscr{C}} R$. Suppose all members of $\mathscr{C}$ are transitive. Then for all $a,b,c \in S$ with $a\overline{R}b$ and $b\overline{R}c$ we have aRb and bRc for all $R \in \mathscr{C}$. Thus by transitivity of each $R \in \mathscr{C}$ we also have aRc for each $R \in \mathscr{C}$. Thus we find $a\overline{R}c$. Hence $\overline{R}$ is also transitive.

The proof for symmetric or reflexive relations is left to the reader. □

The above lemma makes it possible to define the *reflexive, symmetric or transitive closure* of a relation R on a set S. It is the smallest reflexive, symmetric or transitive relation containing R. This means, as follows from Lemma 3.5.1, it is the intersection $\bigcap_{R'\in\mathscr{C}} R'$, where $\mathscr{C}$ is the collection of all reflexive, symmetric or transitive relations containing R. Indeed, the above lemma implies that $\bigcap_{R'\in\mathscr{C}} R'$ is the smallest transitive (symmetric or reflexive) relation containing R if we take for $\mathscr{C}$ the appropriate set of all transitive (symmetric or reflexive) relations containing R.

Example 3.5.2. Suppose

$$R = \{(1,2),(2,2),(2,3),(5,4)\}$$

is a relation on $S = \{1,2,3,4,5\}$.

The reflexive closure of R is then the relation

$$\{(1,1),(1,2),(2,2),(2,3),(3,3),(4,4),(5,5),(5,4)\}.$$

The symmetric closure equals

$$\{(1,2),(2,1),(2,2),(2,3),(3,2),(5,4),(4,5)\}.$$

And, finally, the transitive closure of R equals

$$\{(1,2),(2,2),(2,3),(1,3),(5,4)\}.$$

One easily checks that the reflexive closure of a relation R equals the relation $I \cup R$ and the symmetric closure equals $R \cup R^\top$. The transitive closure is a bit more complicated. It contains $R, R^2, \ldots$. In particular, it contains $\bigcup_{n>0} R^n$, and, as we will show below, is equal to it.

Proposition 3.5.3. $\bigcup_{n>0} R^n$ is the transitive closure of the relation R.

Proof. Define $\bar{R} = \bigcup_{n>0} R^n$. We prove transitivity of $\bar{R}$. Let $a\bar{R}b$ and $b\bar{R}c$, then there are sequences $a_1 = a, \ldots, a_k = b$ and $b_1 = b, \ldots, b_l = c$ with $a_i R a_{i+1}$ and $b_i R b_{i+1}$. But then the sequence $c_1 = a_1 = a, \ldots, c_k = a_k = b_1, \ldots, c_{k+l-1} = b_l = c$ is a sequence from a to c with $c_i R c_{i+1}$. Hence $aR^{k+l-2}c$ and $a\bar{R}c$.

So, as the transitive closure of R contains $\bar{R}$ and the latter is transitive, and hence is contained in the transitive closure, they are equal. □

The transitive, symmetric and reflexive closure of a relation R is an equivalence relations. In terms of the graph Γ_R, the equivalence classes are the strongly connected components of Γ_R.

Example 3.5.4. If we consider the whole World Wide Web as a set of documents, then we may consider two documents to be in a (symmetric) relation R if there is a hyperlink from one document to the another.

The reflexive and transitive closure of the relation R defines a partition of the web into independent subwebs.

Example 3.5.5. Let S be the set of railway stations in the Netherlands. Two stations a and b are in relation R if there is a train running directly from a to b.

If $\bar{R}$ denotes the transitive closure of R, then the railway stations in $[a]_{\bar{R}}$ are exactly those stations you can reach by train when starting in a.

Suppose a relation R on a finite set S of size n is given by its adjacency matrix A_R. Then Warshall's Algorithm is an efficient method for finding the adjacency matrix of the transitive closure of the relation R.

In the algorithm we construct a sequence $M_0, \ldots M_n$ of $n \times n$-matrices with only 0's and 1's, starting with $M_0 = A_R$ and ending with the adjacency matrix of the transitive closure of R.

On the set of rows of a matrix we define the operation $\vee$ by

$$(s_1, \ldots, s_n) \vee (t_1, \ldots, t_n) = (\max(t_1, s_1), \ldots, \max(t_n, s_n)).$$

Now the algorithm proceeds as follows.

Algorithm 3.5.6 — Warshall's Algorithm.

- Input: adjacency matrix A_R of a relation R on n elements.
- Output: adjacency matrix of transitive closure R.

We proceed with the following steps:

- The initial step is to set M_0 equal to A_R.
- For $k \geq 1$, the matrix M_k equals M_{k-1} if the k^{th} row r is completely zero and otherwise is obtained from M_{k-1} by replacing each nonzero row s having a 1 at position k by $r \vee s$.
- The matrix M_n is given as the adjacency matrix of the transitive closure of R.

```
Warshall := procedure(M)
local variables
    | length := len(M)
    | row
    | col
for k in [1, ..., length] do
    | for row in [1, ..., length] do
    |     | for col in [1, ..., length] do
    |     |     | M[row][col] := max(M[row][col], min(M[row][k], M[k][col]))
return M
```

Proof. To prove that the resulting matrix M_n is indeed the adjacency matrix of the transitive closure of R, we argue as follows. We claim that the following holds true:

The matrix M_k has a 1 at entry i, j if and only if there is a path

$$a_i = v_0, v_1, \ldots, v_{l-1}, v_l = a_j$$

from a_i to a_j with $v_1, \ldots, v_{l-1}$ in $\{a_1, \ldots, a_k\}$ in the graph Γ_R.

Indeed, for $k = 0$ the set $\{a_1, \ldots, a_k\}$ is empty, so the claim true. In M_1 we only have a one at entry i, j if and only if (a_i, a_j) was already in R, or (a_i, a_1) and (a_1, a_j) are in R and there is a path a_i, a_1, a_j from a_i to a_j only using vertices in $\{a_1\}$.

Now suppose for some $0 \leq l \leq n-1$ an entry i, j in M_l is 1 if and only if there is a path from a_i to a_j only using vertices from $\{a_1, \ldots, a_k\}$. Then a new 1 at entry i, j in M_{l+1} is only added to M_l if there are paths from a_i to a_{l+1} and from a_{l+1} to a_j using only vertices in $\{a_1, \ldots, a_l\}$. Hence entry i, j in M_{l+1} is only 1 if there is a path from a_i to a_j only using vertices from $\{a_1, \ldots, a_{l+1}\}$.

Since for $l = 1$, our claim is true, the above shows that it is also true for $l = 2$. But then also for $l = 3$ and so on. Thus our claim holds for all k. But that means that entry i, j in the resulting matrix M_n is equal to 1 if and only if there is a path from a_i to a_j. So the resulting matrix M is indeed the adjacency matrix of the transitive closure of R. □

The above proof is an example of a *proof by induction*. Later, in Chapter 6, we will encounter more examples of proofs by induction.

Example 3.5.7. Consider the relation R on $\{1, 2, 3, 4, 5\}$ given by the adjacency matrix

$$M = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

We will run Warshall's algorithm to find the adjacency matrix of the transitive closure of R.

We start with $M_0 = A$. As only row 1 and 3 have a 1 at position 1, we get

$$M_1 = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

Now row 1, 2 and 3 have a 1 at position 2 and we find

$$M_2 = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

The first three rows do have now a 1 at position 3, so M_3 equals

$$M_3 = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

As only row 4 has a 1 at position 4, we also have $M_4 = M_3$. Finally M_5 also equals

$$M_5 = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

3.6 Exercises

Exercise 3.6.1. Which of the following relations on the set $S = \{1,2,3,4\}$ is reflexive, irreflexive, symmetric, antisymmetric or transitive?

(a) $\{(1,3),(2,4),(3,1),(4,2)\}$;
(b) $\{(1,3),(2,4)\}$;
(c) $\{(1,1),(2,2),(3,3),(4,4),(1,3),(2,4),(3,1),(4,2)\}$;
(d) $\{(1,1),(2,2),(3,3),(4,4)\}$;
(e) $\{(1,1),(2,2),(3,3),(4,4),(1,2),(2,3),(3,4),(4,3),(3,2),(2,1)\}$.

Exercise 3.6.2. Let $A = \{1,2,3,4\}$ and $R_1 = \{(1,2),(1,3),(2,4),(2,2),(3,4),(4,3)\}$ and $R_2 = \{(1,1),(1,2),(3,1),(4,3),(4,4)\}$. Compute $R_1;R_2$ and $R_2;R_1$. Is the composition of relations commutative?

Exercise 3.6.3. Compute for each of the relations R in Exercise 3.6.1 the adjacency matrix and draw the digraph Γ_R.

Exercise 3.6.4. Compute for each of the relations R in Exercise 3.6.1 the adjacency matrix of R^2.

Exercise 3.6.5. Compute for each of the relations in Exercise 3.6.1 the reflexive closure, the symmetric closure and the transitive closure.

Exercise 3.6.6. Suppose R is a reflexive and transitive relation on S. Show that $R^2 = R$.

Exercise 3.6.7. Suppose R_1 and R_2 are two relations from the finite set S to the finite set T with adjacency matrices A_1 and A_2, respectively.

What is the adjacency matrix of the relation $R_1 \cap R_2$, $R_1 \cup R_2$, or $R_1^\top$?

Exercise 3.6.8. Suppose R_1 and R_2 are two relations on a set S. Let R be the product $R_1;R_2$. Prove or disprove the following statements

(a) If R_1 and R_2 are reflexive, then so is R.
(b) If R_1 and R_2 are irreflexive, then so is R.
(c) If R_1 and R_2 are symmetric, then so is R.
(d) If R_1 and R_2 are antisymmetric, then so is R.
(e) If R_1 and R_2 are transitive, then so is R.

Exercise 3.6.9. On the set $\mathbb{N}$ we define the relation $\equiv$ by

$$x \equiv y \Leftrightarrow xy \text{ is a square}$$

for all $x, y \in \mathbb{N}$.

Prove that $\equiv$ is an equivalence relation.

Exercise 3.6.10. Consider the relation $\sim$ on $\mathbb{Z}$ where for all $x, y \in \mathbb{Z}$ we have

$$x \sim y \Leftrightarrow x + y \text{ is even.}$$

Prove that $\sim$ is an equivalence relation, and determine the equivalence classes.

Exercise 3.6.11. In this exercise we will construct the set $\mathbb{Z}$ together with addition and multiplication out of the set $\mathbb{N} \times \mathbb{N}$ on which we only have defined the sum and product.

Consider the set $Z = \mathbb{N} \times \mathbb{N}$ and on it the relation $\equiv$ defined by

$$(a,b) \equiv (c,d) \Leftrightarrow a+d = b+c$$

for all (a,b) and (c,d) in Z.

(a) Proof that $\equiv$ is an equivalence relation.

(b) For $(a,b) \in Z$ let $[(a,b)]$ denote the $\equiv$-equivalence class of (a,b).
Show that the operation $\oplus$ given by

$$[(a,b)] \oplus [(c,d)] = [(a+c,b+d)]$$

for all (a,b) and (c,d) is well defined.

(c) Show that the operation $\otimes$ given by

$$[(a,b)] \otimes [(c,d)] = [(ac+bd,bc+ad)]$$

for all (a,b) and (c,d) is also well defined.

Notice that each equivalence class $[(a,b)]$ corresponds to the integer $a-b$. The sum $[(a,b)] \oplus [(c,d)] = [(a+c,b+d)]$ corresponds to $(a-b)+(c-d) = (a+c)-(b+d)$, while the product $[(a,b)] \otimes [(c,d)] = [(ac+bd,bc+ad)]$ corresponds to $(a-b)\cdot(c-d) = (ac+bd)-(bc+ad)$.

Exercise 3.6.12. What common relations on $\mathbb{Z}$ are the transitive closures of the following relations R? Provide a proof for your answer.

(a) For all $x,y \in \mathbb{Z}$ we have $xRy \Leftrightarrow y = x+1$.

(b) For all $x,y \in \mathbb{Z}$ we have $xRy \Leftrightarrow y = x-1$ or $y = x$.

(c) For all $x,y \in \mathbb{Z}$ we have $xRy \Leftrightarrow |y-x| = 2$.

Exercise 3.6.13. Apply Warshall's algorithm to find the transitive closure of the relation R given by the adjacency matrix

$$\begin{pmatrix} 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 \end{pmatrix}.$$

Provide all matrices in the intermediate steps.

4. Maps

4.1 Definition

In this chapter we will study maps (also called functions). Examples of maps are the well known functions $f : \mathbb{R} \to \mathbb{R}$ given by $f(x) = x^2$, $f(x) = \sin x$, or $f(x) = \frac{1}{x^2+1}$. We can view these functions as relations on $\mathbb{R}$. Indeed, the function $f : \mathbb{R} \to \mathbb{R}$ can be viewed as the relation $\{(x,y) \mid x \in \mathbb{R}, y = f(x)\}$. Actually, maps (or functions) are special relations:

Definition 4.1.1. A relation F from a set A to a set B is called a *map* or *function* from A to B if for each $a \in A$ there is one and only one $b \in B$ with aFb.

If F is a map from A to B, we write this as $F : A \to B$. Moreover, if $a \in A$ and $b \in B$ is the unique element with aFb, then we write $b = F(a)$.

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

A *partial map* F from a set A to a set B is a relation with the property that for each $a \in A$ there is at most one b with aFb. In other words, it is a map from a subset A' of A to B, where A' consists of those elements $a \in A$ for which there is a $b \in B$ with aFb.

Example 4.1.2. We have encountered numerous examples of maps. Below you will find some familiar ones.

(a) polynomial functions like $f : \mathbb{R} \to \mathbb{R}$, with $f(x) = x^3$ for all x.
(b) functions like $\cos$, $\sin$ and $\tan$.
(c) $\sqrt{}\,: \mathbb{R}^+ \to \mathbb{R}$, taking square roots.
(d) $\ln : \mathbb{R}^+ \to \mathbb{R}$, the natural logarithm.

Warning. 4.1.3 The function $f : \mathbb{R} \to \mathbb{R}$ is often introduced as the function $f(x) = x^2$. This, however, is not completely correct. The function is f, while for each x we have $f(x) = x^2$ is also a real number. However, we do allow for this sloppiness, and consider the phrase "the function $f(x) = x^2$" to be short for the function $f : \mathbb{R} \to \mathbb{R}$ with $f(x) = x^2$ for all $x \in \mathbb{R}$.

Students often write the following.

Johann Bernoulli introduced the notion of maps

Consider the function $f(x) = x^2$.
Then $f(x)$ is differentiable and its derivative is $f'(x) = 2x$

Here we the use of $f(x)$ is not correct. We should use f instead. The part "the derivative is $f'(x) = 2x$" is allowed by the above convention.

A correct sentence is then:

Consider the function $f(x) = x^2$. Then f is differentiable and its derivative is $f'(x) = 2x$.

If $f : A \to B$ and $g : B \to C$, then we can consider the product $f;g$ as a relation from A to C. We also use the notation $g \circ f$ and call it the composition of f and g. We also say "g after f". We prefer the latter notation for the composition of functions, as for all $a \in A$ we have

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

Proposition 4.1.4. Let $f : A \to B$ and $g : B \to C$ be maps, then the composition $g \circ f = f;g$ is a map from A to C.

Proof. Let $a \in A$, then $g(f(a))$ is an element in C in relation $f;g$ with a. If $c \in C$ is an element in C that is in relation $f;g$ with a, then there is a $b \in B$ with afb and bgc. But then, as f is a map, $b = f(a)$ and, as g is a map, $c = g(b)$. Hence $c = g(b) = g(f(a))$ is the unique element in C which is in relation $g \circ f$ with a. In particular, we find $g \circ f$ to be a map. □

Let A and B be two sets and $f : A \to B$ a map from A to B. The set A is called the *domain* of f, the set B the *codomain*. If $a \in A$, then the element $b = f(a)$ is called the *image* of a under f. The subset of B consisting of the images of the elements of A under f is called the *image* or *range* of f and is denote by $\mathrm{Im}(f)$. So

$$\mathrm{Im}(f) = \{b \in B \mid \text{there is a } a \in A \text{ with } b = f(a)\}.$$

If A' is a subset of A, then the image of A' under f is the set $f(A') = \{f(a) \mid a \in A'\}$. So, $\mathrm{Im}(f) = f(A)$.

If $a \in A$ and $b = f(a)$, then the element a is called a *pre-image* of b. Notice that b can have more than one pre-image. Indeed if $f : \mathbb{R} \to \mathbb{R}$ is given by $f(x) = x^2$ for all $x \in \mathbb{R}$, then both -2 and 2 are pre-images of 4. The set of all pre-images of b is denoted by $f^{-1}(b)$. So,

$$f^{-1}(b) = \{a \in A \mid f(a) = b\}.$$

If B' is a subset of B then the pre-image of B', denoted by $f^{-1}(B')$ is the set of elements a from A that are mapped to an element b of B'. In particular,

$$f^{-1}(B') = \{a \in A \mid f(a) \in B'\}.$$

Example 4.1.5. (a) Let $f : \mathbb{R} \to \mathbb{R}$ with $f(x) = x^2$ for all $x \in \mathbb{R}$. Then $f^{-1}([0,4]) = [-2,2]$.

(b) Consider the map from $\mathbb{Z}$ to $\mathbb{Z}$, which maps an integer a to the unique element b in $\{0,\dots,7\}$ with $a = b \pmod 8$. The inverse image of 3 is the set $\{\dots,-5,3,11,\dots\}$. The inverse image of 11, however, is the empty set.

Theorem 4.1.6. Let $f : A \to B$ be a map.
- If $A' \subseteq A$, then $f^{-1}(f(A')) \supseteq A'$.
- If $B' \subseteq B$, then $f(f^{-1}(B')) \subseteq B'$.

Proof. Let $a' \in A'$, then $f(a') \in f(A')$ and hence $a' \in f^{-1}(f(A'))$. Thus $A' \subseteq f^{-1}(f(A'))$.

Let $a \in f^{-1}(B')$, then $f(a) \in B'$. Thus $f(f^{-1}(B')) \subseteq B'$. □

Example 4.1.7. Let $f : \mathbb{R} \to \mathbb{R}$ be defined by $f(x) = x^2$ for all $x \in \mathbb{R}$. Then $f^{-1}(f([0,1]\}))$ equals $[-1,1]$ and thus properly contains $[0,1]$. Moreover, $f(f^{-1}([-4,4])) = [0,4]$ which is properly contained in $[-4,4]$. This shows that we can have strict inclusions in the above theorem.

Theorem 4.1.8. Let $f : A \to B$ and $g : B \to C$ be maps. Then $\mathrm{Im}(g \circ f) = g(f(A)) \subseteq \mathrm{Im}(g)$.

4.2 Special Maps

Definition 4.2.1. A map $f : A \to B$ is called *surjective*, if for every $b \in B$ there is an $a \in A$ with $b = f(a)$. In other words if $\mathrm{Im}(f) = B$.

The map f is called *injective* (also called *one-to-one*) if for each $b \in B$, there is at most one a with $f(a) = b$. So the pre-image of b is either empty or consist of a unique element. In other words, f is injective if for any elements a and a' from A we find that $f(a) = f(a')$ implies $a = a'$.

The map f is *bijective* if it is both injective and surjective. So, if for each $b \in B$ there is a unique $a \in A$ with $f(a) = b$.

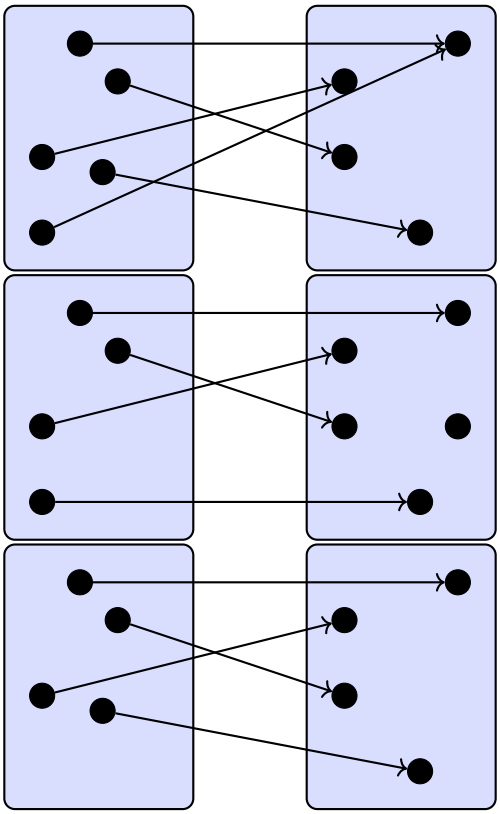


Figure 4.1: Surjective, injective and bijective map

Example 4.2.2. (a) The map $\sin : \mathbb{R} \to \mathbb{R}$ is not surjective nor injective.
(b) The map $\sin : [-\pi/2, \pi/2] \to \mathbb{R}$ is injective but not surjective.
(c) The map $\sin : \mathbb{R} \to [-1,1]$ is a surjective map. It is not injective.
(d) The map $\sin : [-\pi/2, \pi/2] \to [-1,1]$ is a bijective map.

Theorem 4.2.3 — Pigeonhole Principle. Let A be a set of size n and B a set of size m. Let $f : A \to B$ be a map between the sets A and B.
(a) If $n < m$, then f can not be surjective.
(b) If $n > m$, then f can not be injective.
(c) If $n = m$, then f is injective if and only if it is surjective.

Remark 4.2.4. The above result is called the pigeonhole principle because of the following. If one has n pigeons (the set A) and the same number of holes (the set B), then one pigeonhole is empty if and only if one of the other holes contains at least two pigeons.

Example 4.2.5. Suppose you have to pick seven distinct numbers of the set $\{1,2,\ldots,11\}$. Then among these seven numbers there is a pair that adds up to 12.

Suppose S is the set of 7 numbers picked. Now consider the following six subsets

$$\{1,11\},\{2,10\},\{3,9\},\{4,8\},\{5,7\},\{6\}$$

partitioning $\{1,\ldots,11\}$. The map that assigns to each of the seven elements of S the unique part of this partition to which it belongs can not be injective. So, there is a pair of this partition that is contained in S providing us with two numbers in S adding up to 12.

Example 4.2.6. Color all the points of $\mathbb{R}^2$ red or blue. Then for each $d > 0$ there will be two points with the same color which are at distance d.

Indeed, pick a triple of points a,b,c in $\mathbb{R}^2$ forming a equiangular triangle with sides of length d. Now the map that assigns to each point its color is not injective. That means that among a,b and c there are two points of the same color.

If $f : A \to B$ is a bijection, i.e., a bijective map, then for each $b \in B$ we can find a unique $a \in A$ with $f(a) = b$. So, also the relation $f^\top = \{(b,a) \in B \times A \mid (a,b) \in f\}$ is a map. This map is called the *inverse map* of f and denoted by f^{-1}.

Proposition 4.2.7. Let $f : A \to B$ be a bijection. Then for all $a \in A$ and $b \in B$ we have $f^{-1}(f(a)) = a$ and $f(f^{-1}(b)) = b$. In particular, f is the inverse of f^{-1}.

Proof. Let $a \in A$. Then $f^{-1}(f(a)) = a$ by definition of f^{-1}. If $b \in B$, then, by surjectivity of f, there is an $a \in A$ with $b = f(a)$. So, by the above, $f(f^{-1}(b)) = f(f^{-1}(f(a))) = f(a) = b$. □

Remark 4.2.8. Suppose $f : A \to B$ is an injective map, which however, is not surjective. Then we can restrict the codomain of f to its image. The map $f' : A \to \mathrm{Im}(f)$ with $f'(a) = f(a)$ for all $a \in A$ is then bijective and its inverse f'^{-1} is a map from Im to A.

Some authors will also call f'^{-1} the inverse of f, although for us f is not invertible if it is not surjective.

Theorem 4.2.9. Let $f : A \to B$ and $g : B \to C$ be two maps.
(a) If f and g are surjective, then so is $g \circ f$;
(b) If f and g are injective, then so is $g \circ f$;
(c) If f and g are bijective, then so is $g \circ f$.

Proof. (a) Suppose f and g are surjective. Let $c \in C$. By surjectivity of g there is a $b \in B$ with $g(b) = c$. Moreover, since f is surjective, there is also an $a \in A$ with $f(a) = b$. In particular, $g \circ f(a) = g(f(a)) = g(b) = c$. This proves $g \circ f$ to be surjective.
(b) Suppose f and g are injective. Let $a,a' \in A$ with $g \circ f(a) = g \circ f(a')$. Then $g(f(a)) = g(f(a'))$ and by injectivity of g we find $f(a) = f(a')$. Injectivity of f implies $a = a'$. This shows that $g \circ f$ is injective.
(c) (a) and (b) imply (c).

□

Proposition 4.2.10. If $f : A \to B$ and $g : B \to A$ are maps with $f \circ g = I_B$ and $g \circ f = I_A$, where I_A and I_B denote the identity maps on A and B, respectively. Then f and g are bijections. Moreover, $f^{-1} = g$ and $g^{-1} = f$.

Proof. Suppose $f : A \to B$ and $g : B \to A$ are maps with $f \circ g = I_B$ and $g \circ f = I_A$.

Let $b \in B$, then $f(g(b)) = b$. Thus the map f is surjective. If $a, a' \in A$ with $f(a) = f(a')$, then $a = g(f(a)) = g(f(a')) = a'$. Hence f is also injective. In particular, f is bijective. By symmetry we also find g to be bijective, and it follows that $f^{-1} = g$ and $g^{-1} = f$. □

Lemma 4.2.11. Suppose $f : A \to B$ and $g : B \to C$ are bijective maps. Then the inverse of the map $g \circ f$ equals $f^{-1} \circ g^{-1}$.

Proof. Suppose $f : A \to B$ and $g : B \to C$ are bijective maps. Then for all $a \in A$ we have $(f^{-1} \circ g^{-1})(g \circ f)(a) = f^{-1}(g^{-1}(g(f(a)))) = f^{-1}(f(a)) = a$. So, the inverse of $g \circ f$ equals $f^{-1} \circ g^{-1}$. □

4.3 Permutations and the Symmetric Groups

In this section we are mainly concerned with bijections of a finite set X to itself. Often we work with the set X of integers from 1 to n, thus $X = \{1, \ldots, n\}$. There is no loss of generality, since we will see soon that there is no essential difference in the naming of the elements.

The advantage of the natural numbers as names of the elements of X is twofold:

- they have a natural ordering (this is convenient since we often intend to write the elements in a row);
- there is an infinite number of them (in contrast with, for example, the letters of the alphabet).

We will use no arithmetic properties of the natural numbers (as names of elements of X) apart from the ordering.

We introduce permutations and describe multiplication of permutations as composition of maps.

Definition 4.3.1. Let X be a set.

- A bijection of X to itself is also called a *permutation* of X. The set of all permutations of X is denoted by $\mathrm{Sym}(X)$. It is called the *symmetric group* on X.
- The product $g \cdot h$ of two permutations g, h in $\mathrm{Sym}(X)$ is defined as the composition $g \circ h$ of g and h. Thus, for all $x \in X$, we have $g \cdot h(x) = g(h(x))$.
- If $X = \{1, \ldots, n\}$, we also write Sym_n instead of $\mathrm{Sym}(X)$. Furthermore, a permutation f of X is often given by $[f(1), f(2), \ldots, f(n)]$.

The product of two permutations in Sym_n is again a permutation and hence an element of Sym_n. (Prove this!)

As also happens when taking the product of two reals, we often write gh instead of $g \cdot h$ for the product of the permutations g and h.

The identity map $id : X \to X$ plays a special role: $g = g \cdot id$ and $g = id \cdot g$, for all g in $\mathrm{Sym}(X)$. The inverse of $g \in \mathrm{Sym}(X)$, denoted by g^{-1}, is again a permutation and satisfies $g^{-1} \cdot g = id$ and $g \cdot g^{-1} = id$. We call id the *identity element* for the product on $\mathrm{Sym}(X)$. We often use e to denote the identity element. For every positive integer m, we denote by g^m the product of m factors g. Instead of $(g^{-1})^m$ we also write g^{-m}.

We call $\mathrm{Sym}(X)$ the *symmetric group on* X and Sym_n the *symmetric group of degree* n.

Example 4.3.2. Let g and h be the permutations of $\{1, \ldots, 4\}$ with $g(1)=2$, $g(2)=3$, $g(3)=1$, $g(4)=4$, and $h(1)=1$, $h(2)=3$, $h(3)=4$, $h(4)=2$. So $g=[2,3,1,4]$ and $h=[1,3,4,2]$. Then $g \cdot h$ is the permutation with $g \cdot h(1) = g(1) = 2$, $g \cdot h(2) = g(3) = 1$, $g \cdot h(3) = g(4) = 4$, and $g \cdot h(4) = g(2) = 3$, so $g \cdot h = [2,1,4,3]$.

Similarly, $h \cdot g$ is the permutation with $h \cdot g(1) = h(2) = 3$, $h \cdot g(2) = h(3) = 4$, $h \cdot g(3) = h(1) = 1$, and $h \cdot g(4) = h(4) = 2$, so $h \cdot g = [3,4,1,2]$.

In particular, $g{\cdot}h$ and $h{\cdot}g$ are not the same. The official terminology is that g and h do not commute.

The inverse of g is the map that sends 1 to 3, 2 to 1, 3 to 2, and 4 to 4, so $g^{-1}=[3,1,2,4]$.

We will shortly describe notations for permutations that are more convenient for our purposes than the lists we have seen so far: matrices and disjoint cycles.

Remark 4.3.3. Sometimes the product $g{\cdot}h$ is defined the other way around: as $h{\circ}g$.

In other words, the product is the right composition of functions instead of left composition.

Right composition is convenient when writing mappings at the right-hand side of their arguments: for $x{\in}X$, the element $g{\cdot}h(x)$ is then as well the image under $g{\cdot}h$ of x as the image under h of the image under g of x. In formula: $g{\cdot}h(x){=}h(g(x))$.

Right composition is standard in the computer algebra packages GAP and Magma. One should be aware of this fact!

A permutation can be described in matrix notation by a 2 by n matrix with the numbers $1,\ldots,n$ in the first row and the images of $1,2,\ldots,n$ (in that order) in the second row. Since there are $n!$ possibilities to fill the second row, the following theorem holds.

Theorem 4.3.4. Sym_n has exactly $n!$ elements.

The first row of the 2 by n matrix describing a permutation in Sym_n is always $1,2,\ldots,n$ and hence yields no essential information. Therefore, we often omit the first row; the permutation is then given in list notation. For example, $\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$ becomes $[3,1,2]$ in list notation.

Nevertheless, the matrix notation is useful for calculating products and inverses.

- Product: To calculate $g{\cdot}h$ for two permutations g,h in Sym_n, we first look up, for each $i{\in}\{1,\ldots,n\}$, the value $h(i)$, then we look for this value in the first row of the g matrix; below this entry you find $g{\cdot}h(i)$.
  Indeed, if $g=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$, and $h=\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}$ then $gh=\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}$.
- Inverse: If g is written as the 2 by n matrix M, then the inverse of g is described by the matrix obtained from M by interchanging the two rows and sorting the columns in such a way that the first row is again $1,2,\ldots,n$.
  Indeed if $g=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$, then $g^{-1}=\begin{pmatrix}2&3&1\\1&2&3\end{pmatrix}$.

Example 4.3.5. Sym_3 has the following 6 elements:

$$\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix},\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix},\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix},\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix},\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix},\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}.$$

Instead of the conventional matrix notation, we also write permutations as lists. In the so-called list notation we leave out the first row, since that row is always the same. Here are the 6 permutations again in list notation:

$$[1,2,3],[1,3,2],[2,1,3],[2,3,1],[3,1,2],[3,2,1].$$

Definition 4.3.6. The order of a permutation g is the smallest positive integer m such that $g^m{=}e$.

Example 4.3.7.

- The order of the identity is 1.
- The order of the permutation $[2,1,3]$ (in list notation) in Sym_3 is 2.
- The order of the permutation $g{=}[2,3,4,1]$ (in list notation) in Sym_4 is 4 :

$$g^2{=}[3,4,1,2],g^3{=}[4,1,2,3],g^4{=}e.$$

Remark 4.3.8. Of course we must justify that the notion order makes sense. If g is a permutation in Sym_n, then the permutations $g, g^2, g^3, \ldots$ can not all be distinct, because there are only finitely many permutations in Sym_n ($n!$ to be precise). So there must exist positive numbers $r < s$ such that $g^r = g^s$. Since g is a bijection, we find $g^{s-r} = e$. So there exist positive numbers m with $g^m = e$, and in particular a smallest such number. Therefore each permutation g has a well-defined order.

4.4 Cycles

Let g be a permutation of $\mathrm{Sym}(X)$. We distinguish between the points which are moved and the points which are fixed by g.

Definition 4.4.1. The *fixed points* of g in X are the elements of x of X for which $g(x) = x$ holds. The set of all fixed points is $\mathrm{fix}(g) = \{x \in X \mid g(x) = x\}$.

The *support* of g is the complement in X of $\mathrm{fix}(g)$. It is denoted by $\mathrm{support}(g)$.

Example 4.4.2. Consider the permutation $g = [1,3,2,5,4,6] \in \mathrm{Sym}_6$. The fixed points of g are 1 and 6. So $\mathrm{fix}(g) = \{1,6\}$. Thus the points moved by g form the set $\mathrm{support}(g) = \{2,3,4,5\}$.

Cycles are elements in Sym_n of special importance.

Definition 4.4.3. Let $g \in \mathrm{Sym}_n$ be a permutation with $\mathrm{support}(g) = \{a_1, \ldots, a_m\}$, where the a_i are pairwise distinct. We say g is an *m-cycle* if $g(a_i) = g(a_{i+1})$ for all $i \in \{1, \ldots, m-1\}$ and $g(a_m) = a_1$. For such a cycle g we also use the cycle notation $(a_1, \ldots, a_m)$.

2-cycles are called *transpositions*.

Example 4.4.4.

- In Sym_3 all elements are cycles. The identity element e is a 0 - or 1-cycle, the other elements are 2 - or 3-cycles: $(1,2), (1,3), (2,3), (1,2,3)$ and $(1,3,2)$. No two of these 5 cycles are disjoint.
- In Sym_4, the element (in list notation) $[2,1,4,3]$ is not a cycle, but it is the product $(1,2)\cdot(3,4)$ of the transpositions $(1,2)$ and $(3,4)$.

Remark 4.4.5.

- The cycle notation of a permutation g does not tell us in which Sym_n we are working in. This is in contrast to the matrix notation. So $(1,2)$ might belong to Sym_2 just as well as to Sym_3. This yields no real confusion because of the natural identification of Sym_{n-1} with the part of Sym_n consisting of all permutations fixing n :

$$\mathrm{Sym}_{n-1} = \{g \in \mathrm{Sym}_n \mid g(n) = n\}.$$

- The composition of permutations in Sym_n (where $n > 2$) is not commutative. This means that the products $g \cdot h$ and $h \cdot g$ are not always the same. If $g \cdot h = h \cdot g$, then we say that g and h commute. Two cycles c and c' are called disjoint if the intersection of their supports is empty. Two disjoint cycles always commute. (Prove this!) A cycle $(a_1, a_2, \ldots, a_n)$ also commutes with its inverse $(a_n, \ldots, a_2, a_1)$

Every element in Sym_n is a product of cycles. Even more is true:

Theorem 4.4.6. Every permutation in Sym_n is a product of disjoint cycles. This product is unique up to rearrangement of the factors.

Proof. Let $g \in \mathrm{Sym}_n$. Then define Γ to be the directed graph with vertex set $X = \{1, \ldots, n\}$ with edges $(i, g(i))$, for $i \in X$. Then as g is a map, every element i is the tail of a unique edge, and as g is bijective, it is also the head of a unique edge $(g^{-1}(i), i)$.

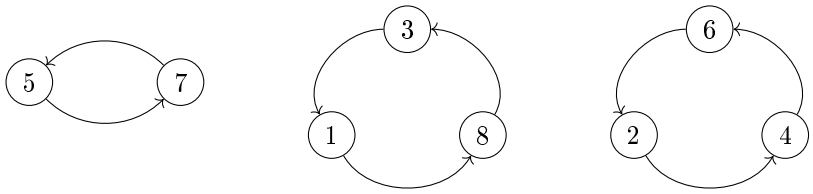


Figure 4.2: Cycles

So, Γ is a digraph in which all vertices have indegree and outdegree equal to 1. By 3.2.7, we find Γ to be a disjoint union of cycles. To each cycle $C = v_0, v_1, \ldots, v_k, v_0$ of Γ, there corresponds the permutation cycle $c = (v_0, \ldots, v_k)$ Clearly g equals the product of the various cycles c.

As Γ is uniquely determined by g, we also find that the product is unique up to rearrangement of the factors. □

If a permutation is written as a product of disjoint cycles, we say that it is given in *disjoint cycles form* or *disjoint cycles notation*. The 1-cycles are usually left out in this notation.

Example 4.4.7. The above proof actually shows how to find the disjoint cycles decomposition of a permutation. Consider the permutation (in list notation)

$$g{=}[8,4,1,6,7,2,5,3]$$

in Sym_8. The following steps lead to the disjoint cycles decomposition.

- Choose an element in the support of g, for example 1. Now construct the cycle

  $$(1, g(1), g^2(1), \ldots).$$

  In this case this cycle is $(1,8,3)$. On $\{1,3,8\}$ the permutation g and the cycle $(1,8,3)$ coincide.
- Next, choose an element in the support of g, but outside $\{1,3,8\}$, for example 2. Construct the cycle

  $$(2, g(2), g^2(2), \ldots).$$

  In the case at hand, this cycle is $(2,4,6)$. Then g and $(1,8,3)\cdot(2,4,6)$ coincide on the set $\{1,2,3,4,6,8\}$.
- Choose an element in the support of g but outside $\{1,2,3,4,6,8\}$, say 5. Construct the cycle

  $$(5, g(5), g^2(5), \ldots),$$

  i.e., $(5,7)$. Then g and $(1,8,3)\cdot(2,4,6)\cdot(5,7)$ coincide on $\{1,2,3,4,5,6,7,8\}$ and we are done.

Note that the three cycles $(1,8,3)$, $(2,4,6)$, $(5,7)$ commute, so that g can also be written as $(5,7)\cdot(1,8,3)\cdot(2,4,6)$ or as $(2,4,6)\cdot(5,7)\cdot(1,8,3)$, etc.

The above procedure can be generalized to an algorithm.

Algorithm 4.4.8 — Permutation as a product of cycles.

- Input: permutation (e.g. in matrix or list notation).
- Output: permutation as a product of cycles.

```
ToCycles = procedure(perm)
local variables
    x := 1
    start := 1
    L := {1,...,len(perm)}
    C := []
    Cycleproduct := []
while L ≠ emptyset do
    start := L[1]
    x := start
    while perm(x) ≠ start do
        C := append(C,x)
        x := perm(x)
        L := remove(L,x)
    if C ≠ [] do
        Cycleproduct := append(Cycleproduct,C)
return Cycleproduct
```

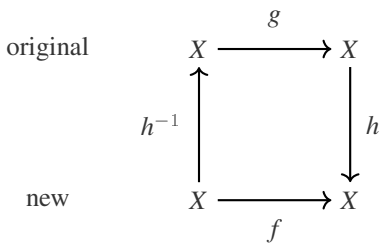
Theorem 4.4.6 justifies the following definition:

Definition 4.4.9. The cycle structure of a permutation g is the (unordered) sequence of the cycle lengths in an expression of g as a product of disjoint cycles.

So, rephrasing Theorem 4.4.6, we can say that every permutation has a unique cycle structure.

The choice $X=\{1,\ldots,n\}$ fixes the set X under consideration. Suppose someone chooses a different numbering of the elements in X. How do we compare two permutations of X with respect to these two numberings?

There is a permutation h of X, which changes our numbering in the new one; so h can be used as a change of names. We describe a given permutation g with respect to the new numbering as follows. First, we apply the 'back-transformation' h^{-1} to our own numbering, then we apply g, and, finally, we use h again to translate back to the other numbering.



As a formula, with respect to the new numbering, the transformation g 'reads' $h\cdot g\cdot h^{-1}$. The map $g\mapsto h\cdot g\cdot h^{-1}$ is called *conjugation* with h. The cycle decomposition of g yields a nice way to calculate the effect of conjugation with a permutation h:

Lemma 4.4.10. Let h be a permutation in Sym_n.

- For every cycle $(a_1,\ldots,a_m)$ in Sym_n we have

$$h\cdot(a_1,\ldots,a_m)\cdot h^{-1}=(h(a_1),\ldots,h(a_m)).$$

- If $(g_1,\ldots,g_k)$ are in Sym_n, then $h\cdot g_1\cdots g_k\cdot h^{-1}=hg_1h^{-1}\cdots hg_kh^{-1}$. In particular, if $g_1,\ldots,g_k$ are

(disjoint) cycles, then $h{\cdot}g_1{\cdots}g_k{\cdot}h^{-1}$ is the product of the (disjoint) cycles $h{\cdot}g_1{\cdot}h^{-1},\ldots,h{\cdot}g_k{\cdot}h^{-1}$.

Proof. The proofs of both items in the lemma are easy verifications if you take the following approach.

Part 1: Conjugation of a cycle.
We compute $h{\cdot}(a_1,\ldots,a_m)h^{-1}(x)$ by distinguishing two cases.

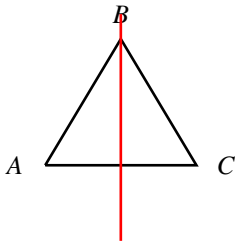
- If $x{=}h(a_i)$ for some $1{\leq}i{\leq}m$:
  $h{\cdot}(a_1,\ldots,a_m)\cdot h^{-1}(x)=h(a_1,\ldots,a_m)h^{-1}(h(a_i))=h(a_1,\ldots,a_m)(a_i))=h(a_{i+1})$ (with the convention that $a_{m+1}{=}a_1$).
- If x is not equal to $h(a_i)$ for all $1\leq i\leq m$, then $h^{-1}(x)$ is not in $\{a_1,\ldots,a_m\}$, so that $g{\cdot}h^{-1}(x){=}h^{-1}(x)$ and consequently $h{\cdot}(a_1,\ldots,a_m)\cdot h^{-1}(x)=hh^{-1}(x)=x$.

We conclude that $h{\cdot}(a_1,\ldots,a_m){\cdot}h^{-1}{=}(h(a_1),\ldots,h(a_m))$.

Part 2: Conjugation of a product of permutations.
The second item of the lemma follows once you realize that in the product $hg_1h^{-1}{\cdots}hg_kh^{-1}$ the pairs $h^{-1}h$ cancel, so that $hg_1{\cdots}g_kh^{-1}$ is what remains. In particular, for cycles g_i, the first item of the lemma then shows that the product $hg_1h^{-1}{\cdots}hg_kh^{-1}$ is the product of the cycles hg_ih^{-1}.
If cycles have disjoint supports, then their conjugates also have disjoint supports: The support of hch^{-1}, where c is a cycle, is $h(\text{support}(c))$ (see the first item of the lemma), so that the supports of $hg_1h^{-1},\ldots,hg_kh^{-1}$ are the sets $h(\text{support}(g_1))$, …, $h(\text{support}(g_k))$. Since h is a bijection, these sets are disjoint if the sets $\text{support}(g_1)$,…, $\text{support}(g_k)$ are disjoint.

□

Example 4.4.11. Let be an equilateral triangle with vertices A,B, and C. The reflection in the line L through B and the midpoint of the edge AC induces a permutation of the three vertices: $A{\mapsto}C$, $B{\mapsto}B$, $C{\mapsto}A$.



We can describe the reflection by the permutation (A,C).

If we name the three vertices $1,2,3$ for A,B,C, respectively, then we can describe the reflection by the permutation $(1,3)$. A rotation through $+120^\circ$ is also a permutation of the three vertices. This rotation is described by the permutation $(1,3,2)$.
If we choose other names for the vertices, for example $1,3,2$ for A,B,C, then the description of the reflection and the rotation change. The reflection is then for example described by $(1,2)$ and the rotation by $(1,2,3)$. This renumbering may be achieved by the permutation $k{=}(2,3)$. Indeed, we see that $k{\cdot}(1,2){\cdot}k^{-1}{=}(1,2)$ and $k{\cdot}(1,3,2){\cdot}k^{-1}{=}(1,2,3)$.
Conjugation is similar to basis transformation in linear algebra.

It follows that any two *conjugate* permutations (one permutation can be obtained from the other by conjugation) have the same cycle structure. The converse also holds.

Theorem 4.4.12. Two elements g and h in Sym_n have the same cycle structure if and only if there exists a

permutation k in Sym_n with $g{=}k{\cdot}h{\cdot}k^{-1}$.

Proof. This implication follows from the conjugation formulas from Lemma 4.4.10.

We write both g and h as a product of disjoint cycles s_i and t_j, respectively, all of length at least 2. Since g and h have the same cycle structure, we can write $g{=}s_1{\cdot}s_2{\cdot}\ldots{\cdot}s_k$ and $h{=}t_1{\cdot}t_2{\cdot}\ldots{\cdot}t_k$ in such a way that s_i and t_i have equal length for all i. Suppose $s_i{=}s_{i,1}{\cdot}s_{i,2}{\cdots}s_{i,k_i}$ and $t_i{=}t_{i,1}{\cdot}t_{i,2}{\cdots}t_{i,k_i}$. Denote by u a permutation with $u(s_{i,j}){=}t_{i,j}$ for all i from 1 to k and j from 1 to k_i. This is possible since the supports of the s_i are disjoint as well as the supports of the t_i. (Notice that there may be more than one permutation u satisfying these requirements.) The conjugation formulas yield that $ugu^{-1}{=}h$. □

Corollary 4.4.13. Being conjugate is an equivalence relation on Sym_n.

Proof. Two elements in Sym_n are conjugate if and only if they have the same cycle structure. But having the same cycle structure is of course reflexive, symmetric and transitive. So, being conjugate is an equivalence relation. □

Example 4.4.14. In Sym_4 the permutations (in list notation) $g{=}[2,1,4,3]$ and $h{=}[3,4,1,2]$ are conjugate, since both have the cycle structure $2,2$: $g{=}(1,2){\cdot}(3,4)$ and $h{=}(1,3){\cdot}(2,4)$. A permutation k such that $k{\cdot}g{\cdot}k^{-1}{=}h$ is $k{=}[1,3,2,4]$. In disjoint cycles notation this is $(2,3)$.

Transpositions play an important role among permutations.

Theorem 4.4.15. Let $n{\geq}2$. Every element of Sym_n is the product of (not necessarily disjoint) transpositions.

Proof. Since every permutation in Sym_n can be written as a product of disjoint cycles , it suffices to show that every cycle is a product of 2-cycles.

Now every m-cycle $(a_1,\ldots,a_m)$, is equal to the product

$$(a_1,a_2)(a_2,a_3)\cdots(a_{m-1},a_m),$$

and the proof is complete.

□

Example 4.4.16. Let $a{=}[a_1,\ldots,a_n]$ be a list of n integers. The algorithm 'Bubble sort' ranks the elements of a with respect to increasing value. The algorithm works as follows. Take an element a_i of the list, compare it with the predecessor a_{i-1} , and switch both elements if a_i is less than a_{i-1} . First, i decreases from n to 2 . Then the least element is in the first position of the list. Now one repeats the procedure, but only with i decreasing from n to 3 . By this time the second least element is in the second position. And so forth. Finally, the algorithm yields a sorted list. The switch of two elements of the list is a transposition $(i-1,i)$ applied to the positions $i-1$ and i of the two elements in the list. If a is filled with the numbers from 1 to n, then it yields, after applying all the transpositions $(i-1,i)$ where a_i is less than a_{i-1} a permutation with $j{=}a_j$ for all $j{\in}\{1,\ldots,n\}$. Hence we may write each permutation as a product of transpositions, in particular even of transpositions of the form $(i-1,i)$. This yields again a proof of the theorem.

4.5 Alternating groups

From the theory in Section 4.4, every permutation can be written as a product of transpositions. To be able to distinguish between products of even and odd length, we need the following result.

Theorem 4.5.1. If a permutation is written in two ways as a product of transpositions, then both products have even length or both products have odd length.

Proof. Suppose that the permutation g can be written both as the product of transpositions $c_1 \cdots c_k$ with k even, and as the product of transpositions $d_1 \cdots d_m$ with m odd. Then

$$e = c_1 \cdots c_k \cdot d_1^{-1} \cdots d_m^{-1}$$

expresses the identity as the product of an odd number of transpositions. We will show that this is impossible.

So assume that the identity element e is a product of an odd number of transpositions. We choose such a product $e = t_1 \cdots t_m$ with m minimal subject to being odd. It is obvious that $m > 0$.

Assertion. We may assume that $t_1 = (1,2)$.

If $t_1 = (i,j)$, we can conjugate left-hand side and right-hand side by $(1,i)\cdot(2,j)$.

Assertion. We may assume that there is some $l > 0$ with t_1 up to t_l all moving 1, that is, $t_i = (1,a_i)$ for all $i \leq l$, and that t_{l+1} up to t_m all fix 1.

Applying the formulas $(a,b)\cdot(1,c) = (1,c)\cdot(a,b)$ and $(a,b)\cdot(1,b) = (1,a)\cdot(a,b)$, where $1, a, b$ and c are different numbers in $\{1,\ldots,n\}$, we can shift all transpositions which contain 1 to the front without violating the minimality of m.

Assertion. There is an index i with $i \in \{2,\ldots,l\}$ such that $t_i = t_1$.

We must have $t_1 \cdot t_2 \cdots t_l(1) = 1$. Therefore $2 = t_1(1)$ lies in the support of $t_2 \cdots t_l$, and at least one of the a_i with $i > 1$ is equal to 2.

Final contradiction.

We have $t_i = t_1 = t_1^{-1}$, and, because of minimality of m, also $t_2 \neq t_1$. Hence, $e = t_1 \cdots t_m = t_1 \cdot (t_2 \cdots t_{i-1}) \cdot (t_1)^{-1} \cdot t_{i+1} \cdots t_m = s_2 \cdots s_{i-1} \cdot t_{i+1} \cdots t_m$, where $s_j = t_1 \cdot t_j \cdot (t_1)^{-1}$ for $j \in \{2,\ldots,i-1\}$ is also a transposition. We have written e as a product of $m-2$ transpositions. This contradicts the minimality of m.

□

In other words, no permutation can be written both as a product of transpositions of even length and as such a product of odd length. So if one product involves an even (odd) number of factors, then all products involve an even (odd) number of factors.

This justifies the following definition.

Definition 4.5.2. Let g be an element of S_n. The sign (signum) of g, denoted by $\operatorname{sign}(g)$, is defined as

- 1 if g can be written as a product of an even number of 2-cycles, and
- -1 if g can be written as a product of an odd number of 2-cycles.

We say that g is even if $\operatorname{sign}(g) = 1$ and odd if $\operatorname{sign}(g) = -1$.

The sign is multiplicative.

Theorem 4.5.3. For all permutations g, h in Sym_n, we have

$$\operatorname{sign}(g \cdot h) = \operatorname{sign}(g) \cdot \operatorname{sign}(h).$$

Proof. Let g and h be elements of Sym_n.

If one of the permutations is even and the other is odd, then $g \cdot h$ can obviously be written as the product of an odd number of transpositions and is therefore odd.

If g and h are both even or both odd, then the product $g \cdot h$ can be written as the product of an even number of transpositions so that $g \cdot h$ is even.

□

We also say that sign is a multiplicative map from Sym_n to $\{1,-1\}$. (The notion morphism explores this view further in a general context.)

Remark 4.5.4.
- The sign of a permutation and its inverse are the same. There are various ways to see this, one of which is based on the multiplicative property of the sign. Since $g\cdot g^{-1}=e$, we find $\mathrm{sign}(g)\cdot\mathrm{sign}(g^{-1})=\mathrm{sign}(gg^{-1})=\mathrm{sign}(e)=1$, so that $\mathrm{sign}(g)$ and $\mathrm{sign}(g^{-1})$ must both be 1 or both be -1.
- Every m-cycle $(a_1,\ldots,a_m)$ can be written as the product of $m-1$ transpositions:

$$(a_1,\ldots,a_m)=(a_1,a_2)\cdot(a_2,a_3)\cdot\ldots\cdot(a_{m-1},a_m).$$

  Since transpositions are odd, the multiplicativity of the sign implies that the sign of an m - cycle is $(-1)^{m-1}$, i.e., a cycle of even length is odd and a cycle of odd length is even.

The previous theorem implies the following way of determining the sign.

Corollary 4.5.5. If a permutation g is written as a product of cycles, then $\mathrm{sign}(g)=(-1)^w$, where w is the number of cycles of even length.

Proof. Since sign is a multiplicative mapping, the sign of g is the product of the signs of every factor. Now a cycle of odd length has sign 1, so we only need to count the number of cycles of even length.

□

The fact that sign is multiplicative implies that products and inverses of even permutations are even. This gives rise to the following definition.

Definition 4.5.6. By Alt_n we denote the set of even permutations in Sym_n. We call Alt_n the *alternating group* on n letters.

The alternating group is closed with respect to taking products and inverse elements.

Example 4.5.7. For $n=3$, the even permutations are (in cycle notation): $e,(2,3,1)$ and $(3,1,2)$.

There are just as many even as odd permutations in Sym_n.

Theorem 4.5.8. For $n>1$, the alternating group Alt_n contains precisely $\frac{n!}{2}$ elements.

Proof. An element g of Sym_n is even (respectively, odd), if and only if the product $g\cdot(1,2)$ is odd (respectively, even). Hence the map $g\mapsto g\cdot(1,2)$ defines a bijection between the even and the odd elements of Sym_n. But then precisely half of the $n!$ elements of Sym_n are even.

□

3-cycles are the smallest nontrivial even cycles. They are the building blocks for even permutations:

Theorem 4.5.9. Every even permutation is a product of 3-cycles.

Proof. Every element of $\mathrm{Alt}(X)$ is a product of an even number of transpositions. Hence it suffices to prove that each product of two transpositions, different from the identity element, can be written as a product of 3-cycles.

Let (a,b) and (c,d) be two different transpositions.

If a,b,c and d are pairwise distinct, then

$$(a,b)\cdot(c,d)=(a,b)\cdot(b,c)\cdot(b,c)\cdot(c,d)=(a,b,c)\cdot(b,c,d).$$

Without loss of generality we are left with the case where a,b,d are pairwise distinct and $b{=}c$. But then $(a,b)\cdot(b,d){=}(a,b,d)$.

This proves the theorem.

□

4.6 Exercises

Exercise 4.6.1. Which of the following relations are maps from $A=\{1,2,3,4\}$ to A?
(a) $\{(1,3),(2,4),(3,1),(4,2)\}$;
(b) $\{(1,3)(2,4)\}$;
(c) $\{(1,1),(2,2),(3,3),(4,4),(1,3),(2,4),(3,1),(4,2)\}$;
(d) $\{(1,1),(2,2),(3,3),(4,4)\}$.

Exercise 4.6.2. Suppose f and g are maps from $\mathbb{R}$ to $\mathbb{R}$ defined by $f(x)=x^2$ and $g(x)=x+1$ for all $x\in R$. What is $g\circ f$ and what is $f\circ g$?

Exercise 4.6.3. Which of the following maps is injective, surjective or bijective?
(a) $f:\mathbb{R}\to\mathbb{R}$, $f(x)=x^2$ for all $x\in\mathbb{R}$.
(b) $f:\mathbb{R}\to\mathbb{R}_{\geq 0}$, $f(x)=x^2$ for all $x\in\mathbb{R}$.
(c) $f:\mathbb{R}_{\geq 0}\to\mathbb{R}_{\geq 0}$, $f(x)=x^2$ for all $x\in\mathbb{R}$.

Exercise 4.6.4. Suppose R_1 and R_2 are relations on a set S with $R_1;R_2=I$ and $R_2;R_1=I$. Prove that both R_1 and R_2 are bijective maps.

Exercise 4.6.5. Let R be a relation from a finite set S to a finite set T with adjacency matrix A. Prove the following statements:
(a) If every row of A contains one nonzero entry, then R is a map.
(b) If moreover, every column contains at most one entry, then the map R is injective.
(c) If every row and column contain only one 1, then R is a bijection. What is the adjacency matrix of the inverse map?

Exercise 4.6.6. Let S and T be two sets. If R is a relation of $S\times T$, then for each $t\in T$ we have the pre-image

$$_R[t]=\{s\in S\mid sRt\}$$

which is a subset of S.

Prove that the relation $\{(t,_R[t])\mid t\in T\}$ is a map from T to the power set $\mathscr{P}(S)$ of S.

Moreover, show that, if $f:T\to\mathscr{P}(S)$ is a map, then $R_f=\{(s,t)\mid s\in f(t)\}$ is a relation on $S\times T$ with $_{R_f}[t]=f$.

Exercise 4.6.7. Pick four distinct integers. Show that among these four integers there will always be a pair whose difference is a multiple of 3.

Solution: Each of the four integers x chosen is of the form $3m$, $3m+1$ or $3m+2$ for some integer m. By the pigeonhole principle there are at least two integers say a and b having the same form. Their difference is then a multiple of 3.

Exercise 4.6.8. Let $a_0,\ldots,a_{100}$ be positive integers with $a_0+\cdots+a_{100}=300$.

Let $f:\{0,\ldots,100\}\to\{1,\ldots,300\}$ be given by $f(k)=a_0+\cdots+a_k$.
(a) Show that f is an injective map.
(b) Show that there is a subsequence $a_i,a_{i+1},\ldots,a_{i+j}$ of $a_0,\ldots,a_{100}$ with $a_i+\cdots+a_{i+j}=100$ or 200.

Solution: (a) Notice that f is increasing and hence injective.
(b) Consider the map that assigns to each k the number consisting of the last two digits of $f(k)$. Then this is a map between $\{0,\ldots,100\}$ and $\{0,\ldots,99\}$. By the pigeonhole principle it is not injective. So,

there exist $k_1 < k_2$ with $f(k_2) - f(k_1)$ being divisible by 100 and hence being equal to 100 or 200. So $f(k_2) - f(k_1) = a_{k_1+1} + \cdots + a_{k_2}$ equals 100 or 200.

Exercise 4.6.9. In Sym_6 we choose the permutations $a{=}(1,2,3)$, $b{=}(2,3,4,5,6)$ and $c{=}(1,4,6,3)$.
(a) Calculate $a^{-1}, a{\cdot}b{\cdot}c, a{\cdot}b{\cdot}c^2, c^{-1}{\cdot}b$ and $(a{\cdot}c{\cdot}b)^{-1}$.
(b) Calculate the sign of each of the above permutations.

Exercise 4.6.10. Let g be a permutation in Sym_n. Show that if $i{\in}\mathrm{support}(g)$, then $g(i){\in}\mathrm{support}(g)$.

Exercise 4.6.11. How many elements of Sym_5 have the cycle structure $2,3$?

Exercise 4.6.12. Let g be the permutation

$$(1,2,3){\cdot}(2,3,4){\cdot}(3,4,5){\cdot}(4,5,6){\cdot}(5,6,7){\cdot}(6,7,8){\cdot}(7,8,9)$$

in Sym_6.
(a) Write g as a product of disjoint cycles.
(b) Calculate the fixed points of g.
(c) Write g^{-1} as a product of disjoint cycles.
(d) Is g even?

Exercise 4.6.13. (a) If the permutations g and h in Sym_n have disjoint supports, then g and h commute, i.e., $g{\cdot}h{=}h{\cdot}g$. Prove this.
(b) Suppose that the permutations g and h in Sym_n commute. Prove that $(g{\cdot}h)^m{=}g^m{\cdot}h^m$ for all positive numbers m.
(c) Suppose that the permutations g and h in Sym_n have disjoint supports. Prove that $(g{\cdot}h)^m{=}1$ for some positive number m implies that $g^m{=}1$ and $h^m{=}1$.
(d) If the permutation has order t and if g^m = id for some positive number m, show that t divides m. In particular, if c is a t-cycle and $c^m = id$ for some positive number m, then m is divisible by t.

Exercise 4.6.14. (a) Prove that for $n > 4$ every permutation in Sym_n can be written as a product of 4-cycles.
(b) Prove that for $n > 5$ every even permutation can be written as a product of 5-cycles.

Exercise 4.6.15. Let $a{=}(1,2,3)(4,7,9)(5,6)$. Determine an element b in Sym_9 such that $b{\cdot}a{\cdot}b^{-1}{=}(9,8,7)(6,5,4)(3,2)$.

Exercise 4.6.16. Let g be an element of Sym_n with $n > 2$.
(a) If g commutes with the transposition (i,j), where $i{\neq}j$, then $g(i){\in}\{i,j\}$. Prove this.
(b) Show that $g{\cdot}i{=}i$, whenever g commutes with the transpositions (i,j) and (i,k), where i,j,k are mutually distinct.
(c) Prove that the identity map is the only permutation in Sym_n that commutes with all elements of Sym_n.

Exercise 4.6.17. Write all elements of Alt_4 as products of disjoint cycles.

Exercise 4.6.18. Let $a{=}(1,2)$ and $b{=}(2,\ldots,n)$.
(a) Calculate $b{\cdot}a{\cdot}b^{-1}$.
(b) Calculate $b^k{\cdot}a{\cdot}b^{-k}$, for $k{\in}\mathbb{N}$.
(c) Prove that every element of Sym_n can be written as a product of elements from $\{a, b, b^{-1}\}$.

Exercise 4.6.19. Label the vertices of a quadrangle with the numbers 1 to 4.
(a) Which permutation of the four vertices describes the rotation through + 90° whose center is the middle point of the quadrangle? And which one describes the reflection in the diagonal through the vertices 1 and 3 ?
(b) Determine the permutations g of Sym_4 satisfying: If $\{i,j\}$ is an edge of the quadrangle, then so is $\{g(i), g(j)\}$.
(c) Describe each of the permutations of the above part in geometric terms as a reflection or a rotation. Which of these permutations are even?

Exercise 4.6.20. Put the numbers $1,2,3,4$ into a 2 by 2 matrix as follows: $\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$.

(a) Suppose you are allowed to interchange two columns or two rows. Which permutations of Sym_4 can you get using these moves repeatedly? What if you allow as extra type of move a reflection in the diagonal of the matrix?

(b) Suppose you are allowed to do the following types of moves: Choose a column or row and interchange the two entries. What permutations do you get this way?

(c) Now consider the 3 by 3 matrix $\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix}$. Individual moves are: Choose two rows (or two columns) and interchange them. Show that you can label each resulting permutation with a pair of permutations from $\mathrm{Sym}_3 \times \mathrm{Sym}_3$. Conclude that you get 36 permutations.

Exercise 4.6.21. Label the vertices of a regular tetrahedron with the integers $1,2,3,4$ (see figure). Consider the following moves: For each face of the tetrahedron the corresponding move consists of turning the face 120 degrees clockwise or counter clockwise and moving the labels accordingly (so the vertex opposite the face remains fixed). After applying a number of moves, we read off the resulting permutation g in the obvious way: $g(i)$ is the new label of vertex i.

(a) List the 8 moves as permutations.

(b) Suppose, after a number of moves, we have obtained the permutation g. Show that applying a move h leads to the permutation $g \cdot h^{-1}$.

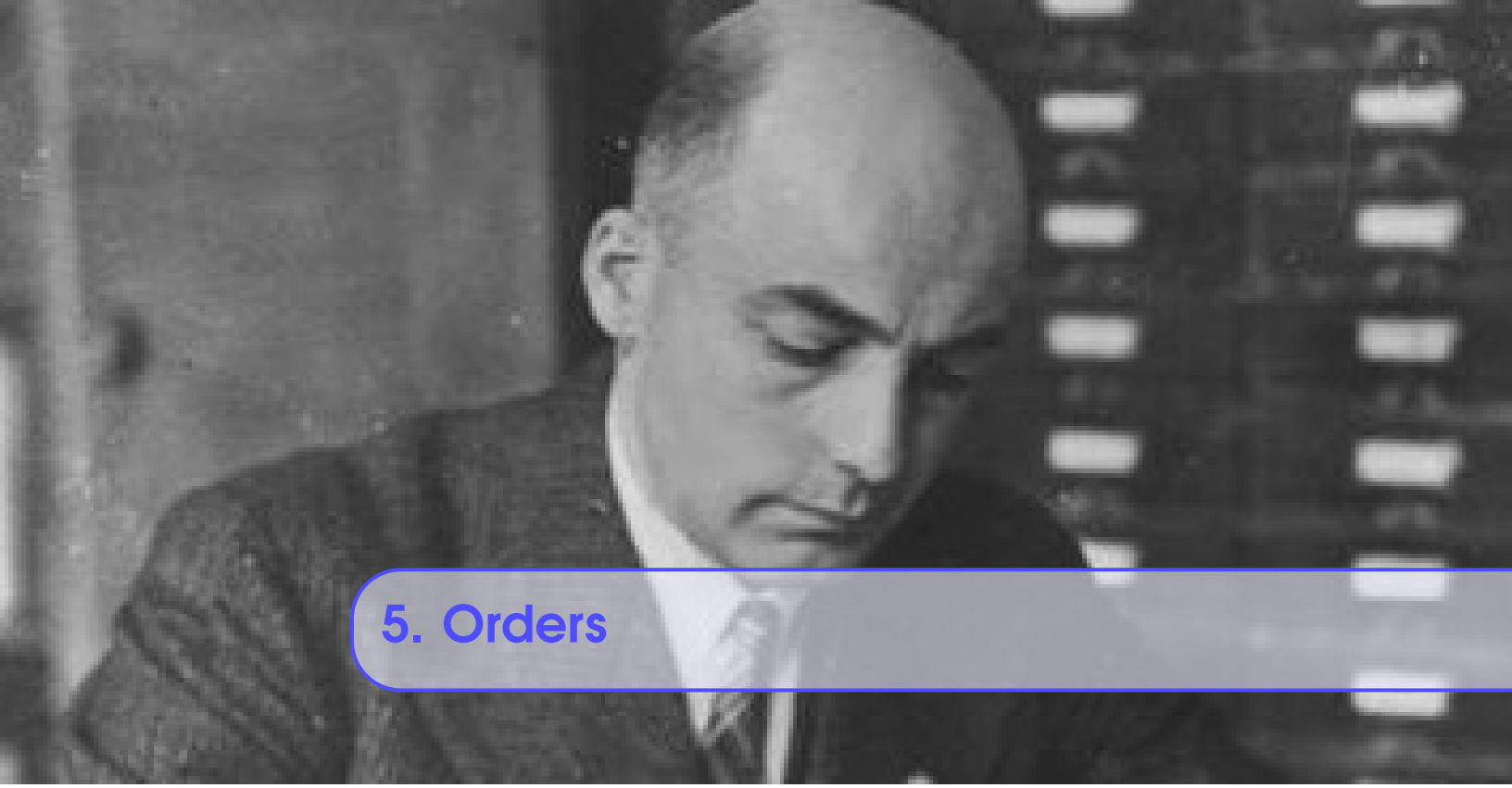
(c) Which permutations of $1,2,3,4$ can you get by using these moves?

Exercise 4.6.22. Provide algorithms for the following tasks:

(a) Find the cycle structure of a permutation given as a matrix.

(b) Find the sign of a permutation given as a matrix.

(c) Given two permutations g and h with the same cycle structure, find a permutation k with $kgk^{-1} = h$.



5. Orders

5.1 Orders and Posets

As we have seen before, the relations $\leq$ and $\geq$ on $\mathbb{R}$, or the relations $\subseteq$ and $\supseteq$ share the properties that they are reflexive, anti-symmetric and transitive. Relations sharing these properties deserve a special name:

Definition 5.1.1. A relation $\sqsubseteq$ on a set P is called an *order* if it is reflexive, antisymmetric and transitive. That means that for all x, y and z in P we have:

- $x \sqsubseteq x$;
- if $x \sqsubseteq y$ and $y \sqsubseteq x$, then $x = y$;
- if $x \sqsubseteq y$ and $y \sqsubseteq z$, then $x \sqsubseteq z$.

The pair $(P, \sqsubseteq)$ is called a *partially ordered set*, or for short, a *poset*.

Two elements x and y in a poset $(P, \sqsubseteq)$ are called *comparable* if $x \sqsubseteq y$ or $y \sqsubseteq x$. The elements are called *incomparable* if $x \not\sqsubseteq y$ and $y \not\sqsubseteq x$.

If any two elements $x, y \in P$ are comparable, so we have $x \sqsubseteq y$ or $y \sqsubseteq x$, then the relation is called a *linear* order.

Example 5.1.2.

- The identity relation I on a set P is an order.
- On the set of real numbers $\mathbb{R}$ the relation $\leq$ is an order relation. For any two numbers $x, y \in \mathbb{R}$ we have $x \leq y$ or $y \leq x$. This makes $\leq$ into a linear order. Restriction of $\leq$ to any subset of $\mathbb{R}$ is again a linear order.
- Let P be the power set $\mathscr{P}(X)$ of a set X, i.e., the set of all subsets of X. Inclusion $\subseteq$ defines a partial order on P. This poset contains a smallest element $\emptyset$ and a largest element X. Clearly, $\subseteq$ defines a partial order on any subset of P.
- The relation "Is a divisor of" $|$ defines an order on the set of natural numbers $\mathbb{N}$. We can associate this example to the previous one in the following way. For each $a \in \mathbb{N}$ denote by $D(a)$ the set of all divisors of a. Then we have

$$a \mid b \Leftrightarrow D(a) \subseteq D(b).$$

Helmut Hasse, Oberwolfach Photo Collection ©unkown

- On the set P of partitions of a set X we define the relation "refines" by the following. The partition Π_1 refines Π_2 if and only if each $\pi_1 \in \Pi_1$ is contained in some $\pi_2 \in \Pi_2$. The relation "refines" is a partial order on P.
  Notice, for the corresponding equivalence relations R_{Π_1} and R_{Π_2} we have Π_1 refines Π_2 if and only if $R_{\Pi_1} \subseteq R_{\Pi_2}$.
- If $\sqsubseteq$ is an order on a set P, then $\sqsupseteq$ also defines an order on P. Here $x \sqsupseteq y$ if and only if $y \sqsubseteq x$. The order $\sqsupseteq$ is called the *dual* order of $\sqsubseteq$.

If $\sqsubseteq$ is an order on the set P, then the corresponding directed graph with vertex set P and edges (x,y), where $x \sqsubseteq y$, is *acyclic* (i.e., contains no cycles of length > 1).

If we want to draw a picture of the poset, we usually do not draw the whole digraph. Instead we only draw an edge from x to y from P with $x \sqsubseteq y$ if there is no z, distinct from both x and y, for which we have $x \sqsubseteq z$ and $z \sqsubseteq y$. This digraph is called the *Hasse diagram* for $(P, \sqsubseteq)$, named after the German mathematician Helmut Hasse (1898-1979).

Definition 5.1.3 — Hasse diagram. Let $(P, \sqsubseteq)$ be a poset. The graph with vertex set P and two vertices $x, y \in P$ adjacent if and only if $x \sqsubseteq y$ and there is no $z \in P$ different from x and y with $x \sqsubseteq z$ and $z \sqsubseteq y$.

Usually pictures of Hasse diagrams are drawn in such a way that two vertices x and y with $x \sqsubseteq y$ are connected by an edge going upwards. For example the Hasse diagram for the poset $(\mathscr{P}(\{1,2,3\}), \subseteq)$ is drawn as below. (In computer science one usually draws the diagram up side down.)

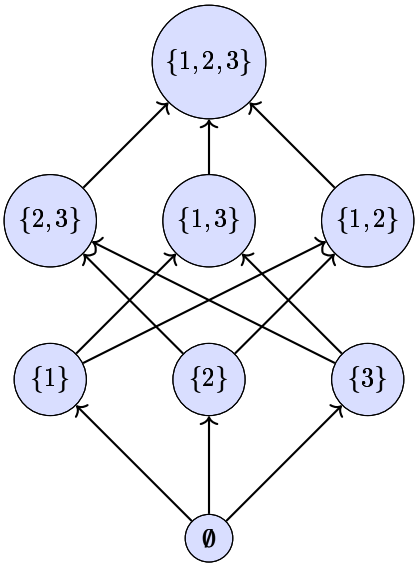


Figure 5.1: Hasse diagram of the relation $\subseteq$ on the set $\mathscr{P}\{1,2,3\}$.

5.1.4 — New posets from old ones. There are various ways of constructing new posets out of old ones. We will discuss some of them. In the sequel both P and Q are posets with respect to some order, which we usually denote by $\sqsubseteq$, or, if confusion can arise, by $\sqsubseteq_P$ and $\sqsubseteq_Q$.

- If P' is a subset of P, then P' is also a poset with order $\sqsubseteq$ restricted to P'. This order is called the *induced* order on P'.
- $\sqsupseteq$ induces the *dual* order on P.
- Let S be some set. On the set of maps from S to P we can define an ordering as follows. Let $f : S \to P$ and $g : S \to P$, then we define $f \sqsubseteq g$ if and only if $f(s) \sqsubseteq g(s)$ for all $s \in S$.

- On the Cartesian product $P \times Q$ we can define an order as follows. For $(p_1, q_1), (p_2, q_2) \in P \times Q$ we define $(p_1, q_1) \sqsubseteq (p_2, q_2)$ if and only if $p_1 \sqsubseteq p_2$ and $q_1 \sqsubseteq q_2$. This order is called the *product order*.
- A second ordering on $P \times Q$ can be obtained by the following rule. For $(p_1, q_1), (p_2, q_2) \in P \times Q$ we define $(p_1, q_1) \sqsubseteq (p_2, q_2)$ if and only if $p_1 \sqsubseteq p_2$ and $p_1 \neq p_2$ or if $p_1 = p_2$ and $q_1 \sqsubseteq q_2$. This order is called the *lexicographic order* on $P \times Q$.
  Of course we can extend this to direct products of more than two sets.

5.2 Maximal and Minimal Elements

Definition 5.2.1. Let $(P, \sqsubseteq)$ be a partially order set and $A \subseteq P$ a subset of P. An element $a \in A$ is called the *largest element* or *maximum* of A, if for all $a' \in A$ we have $a' \sqsubseteq a$. Notice that a maximum is unique, see Lemma 5.2.2 below.

An element $a \in A$ is called *maximal* if for all $a' \in A$ we have that either $a' \sqsubseteq a$ or a and a' are incomparable.

Similarly we can define the notion of *smallest element* or *minimum* and *minimal element*.

If the poset $(P, \sqsubseteq)$ has a maximum, then this is often denoted as $\top$ (top). A smallest element is denoted by $\bot$ (bottom).

If a poset $(P, \sqsubseteq)$ has a minimum $\bot$, then the minimal elements of $P \setminus \{\bot\}$ are called the *atoms* of P.

Lemma 5.2.2. Let $(P, \sqsubseteq)$ be a partially order set. Then P contains at most one maximum and one minimum.

Proof. Suppose $p, q \in P$ are maxima. Then $p \sqsubseteq q$ as q is a maximum. Similarly $q \sqsubseteq p$ as p is a maximum. But then by antisymmetry of $\sqsubseteq$ we have $p = q$. □

Example 5.2.3.

- If we consider the poset of all subsets of a set S, then the empty set $\emptyset$ is the minimum of the poset, whereas the whole set S is the maximum. The atoms are the subsets of S containing just a single element.
- If we consider $|$ as an order on $\mathbb{N}$, then 1 is the minimal element and 0 the maximal element. The atoms are those natural numbers > 1, that are only divisible by 1 and itself, i.e., the prime numbers.

Lemma 5.2.4. Let $(P, \sqsubseteq)$ be a finite poset. Then P contains a minimal and a maximal element.

Proof. Consider the directed graph associated to $(P, \sqsubseteq)$ and pick a vertex in this graph. If this vertex is not maximal, then there is an edge leaving it. Move along this edge to the neighbor. Repeat this as long as no maximal element is found. Since the graph contains no cycles, we will never meet a vertex twice. Hence, as P is finite, the procedure has to stop. This implies we have found a maximal element.

A minimal element of $(P, \sqsubseteq)$ is a maximal element of $(P, \sqsupseteq)$ and thus exists also. □

Example 5.2.5. Notice that minimal elements and maximal elements are not necessarily unique. In fact, they do not even have to exist. In $(\mathbb{R}, \leq)$ for example, there is no maximal nor a minimal element.

The proof of the above lemma provides us with an algorithm to find a minimal (or maximal) element in a finite poset.

Algorithm 5.2.6 — Find minimal element.

- Input: a finite poset $(P, \sqsubseteq)$
- Output: A minimal element.

FindMin = **procedure**$(P, \sqsubseteq)$
local variables
| $p \in P$
while indegree$(p) > 0$ **do**
| **let** $q \in P$ **with** $q \sqsubset p$
| $p := q$
return q

Given a finite poset, we want to order the elements of P in a list L such that for all elements x and y with x with $x \sqsubseteq y$ we have that x is before y in L. We call such a list L (or equivalently linear order on P) a *topological ordering* of the elements of P.

Using that we can determine minimal elements in a finite poset, we can also find a topological ordering.

Algorithm 5.2.7 — Topological sorting.
- Input: a finite poset $(P, \sqsubseteq)$
- Output: A sorted list L of elements of P such that an element x comes before an element y in L if $x \sqsubseteq y$.

TopSort = **procedure**$(P, \sqsubseteq)$
local variables
| $L := []$
| p
while $P \neq \emptyset$ **do**
| $p :=$ FindMin$(P, \sqsubseteq)$
| $L :=$ append$[L, p]$
| $P :=$ remove$[P, p]$
| $\sqsubseteq := \sqsubseteq_{|P \times P}$
return L

Example 5.2.8. Topological sort has various applications. For example consider a spreadsheet. In a spreadsheet various tasks depend on each other. In particular, some of the computations need input from other computations and therefore they can only be carried out after completion of the other computations. If there are no cycles in these computations, this puts a partial order on the set of tasks within a spreadsheet. By topological sort the task list can be linearized and the computations can be done in a linear order.

Definition 5.2.9. If $(P, \sqsubseteq)$ is a poset and $A \subseteq P$, then an *upperbound* for A is an element u with $a \sqsubseteq u$ for all $a \in A$.

A *lowerbound* for A is an element u with $u \sqsubseteq a$ for all $a \in A$.

If the set of all upperbounds of A has a minimal element, then this element is called the *least upperbound* or *supremum* of A. Such an element, if it exists, is denoted by $\sup A$. If the set of all lowerbounds of A has a maximal element, then this element is called the *largest lowerbound* or *infimum* of A. If it exists, the infimum of A is denoted by $\inf A$.

Example 5.2.10. Let S be a set. In $(\mathscr{P}(S), \subseteq)$ any set A of subsets of S has a supremum and an infimum. Indeed,

$$\sup A = \bigcup_{X \in A} X \text{ and } \inf A = \bigcap_{X \in A} X.$$

Example 5.2.11. If we consider the poset $(\mathbb{R}, \leq)$, then not every subset A of $\mathbb{R}$ has a supremum or infimum. Indeed, $\mathbb{Z} \subseteq \mathbb{R}$ has no supremum and no infimum.

Example 5.2.12. In $(\mathbb{N}, |)$ the supremum of two elements a and b is the least common multiple of a and b.

Its infimum is the greatest common divisor.

The least common multiple and greatest common divisor will be inverstigated in Chapter 8.

If $(P,\sqsubseteq)$ is a finite poset, then as we have seen above, we can order the elements from P as $p_1, p_2, \ldots, p_n$ such that $p_i \sqsubseteq p_j$ implies $i < j$. This implies that the adjacency matrix of $\sqsubseteq$ is uppertriangular, which means that it has only nonzero entries on or above the main diagonal.

Definition 5.2.13. An *ascending chain* in a poset $(P,\sqsubseteq)$ is a (finite or infinite) sequence $p_0 \sqsubseteq p_1 \sqsubseteq \ldots$ of elements p_i in P. A *descending chain* in $(P,\sqsubseteq)$ is a (finite or infinite) sequence of elements p_i, $i \geq 0$ with $p_0 \sqsupseteq p_1 \sqsupseteq \ldots$ of elements p_i in P.

The poset $(P,\sqsubseteq)$ is called *well founded* if any descending chain is finite.

Example 5.2.14. The natural numbers $\mathbb{N}$ with the ordinary ordering $\leq$ is well founded. Also the ordering $|$ on $\mathbb{N}$ is well founded.

However, on $\mathbb{Z}$ the order $\leq$ is not well founded.

5.3 Exercises

Exercise 5.3.1. Let $|$ denote the relation "is a divisor of " defined on $\mathbb{Z}$. Even if we let 0 be a divisor of 0, then this does not define an order on $\mathbb{Z}$. Prove this.

Exercise 5.3.2. Let $|$ denote the relation "is a divisor of " . This relation defines an order on the set $D = \{1,2,3,5,6,10,15,30\}$ of divisors of 30. Draw the Hasse diagram.

Draw also the Hasse diagram of the poset of all subsets of $\{2,3,5\}$. Compare the two diagrams. What do you notice?

Exercise 5.3.3. Let $\sqsubseteq$ denote an order relation on a finite set P. By H we denote the relation defining adjacency in the Hasse diagram of $\sqsubseteq$. Prove that $\sqsubseteq$ is the transitive reflexive closure of H.

Exercise 5.3.4. Let $m,n \in \mathbb{N}$. By Π_m we denote the partition of $\mathbb{Z}$ into equivalence classes modulo m. What is a necessary and sufficient condition on n and m for Π_m to be a refinement of Π_n.

Exercise 5.3.5. Suppose $\sqsubseteq_P$ and $\sqsubseteq_Q$ are linear orders on P and Q, respectively. Show that the lexicographical order $\sqsubseteq$ on $P \times Q$ is also linear.

Exercise 5.3.6. Show that the relations as defined in 5.1.4 are indeed orders.

Exercise 5.3.7. In the figure below you see three diagrams. Which of these diagrams are Hasse diagrams?

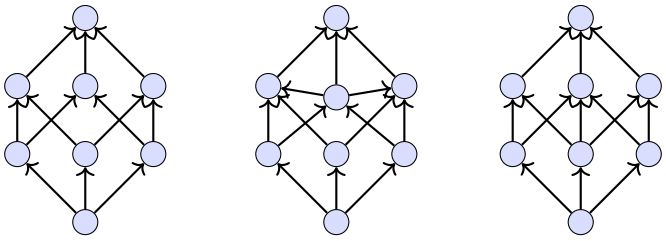


Figure 5.2: Three possible Hasse diagrams

Exercise 5.3.8. Suppose $(A,\sqsubseteq_A)$ and $(B,\sqsubseteq_B)$ are posets. If A and B are disjunct, then we define the relation $\sqsubseteq$ on $A \cup B$ as follows:

$$\begin{aligned} x \sqsubseteq y \text{ if} \quad & x, y \in A \text{ and } x \sqsubseteq_A y; \\ \text{or} \quad & x, y \in B \text{ and } x \sqsubseteq_B y; \\ \text{and if} \quad & x \in A \text{ and } y \in B. \end{aligned}$$

(a) Prove that $\sqsubseteq$ is an order on $A \cup B$.
(b) Give necessary and sufficient conditions such that $\sqsubseteq$ is a linear order on $A \cup B$.

Exercise 5.3.9. On $\mathbb{Z}$ we define $\sqsubseteq$ by $x \sqsubseteq y$ if and only if $x - y$ is odd and x is even, or, $x - y$ is even and $x \leq y$. Show that $\sqsubseteq$ is an order on $\mathbb{Z}$. Is this order linear?

Exercise 5.3.10. Find a well founded linear order on $\mathbb{N} \times \mathbb{N}$.

6. Recursion and Induction

6.1 Recursion

A *recursive definition* tells us how to build objects by using ones we have already built. Let us start with some examples of some common functions from $\mathbb{N}$ to $\mathbb{N}$ which can be defined recursively:

Example 6.1.1. The function $f(n) = n!$ can be defined recursively:

$$\begin{aligned} f(0) &:= 1; \\ \text{for } n > 0\text{: } f(n) &:= n \cdot f(n-1). \end{aligned}$$

Example 6.1.2. The sum $1+2+\cdots+n$ can also be written as $\sum_{i=1}^{n} i$. Here we make use of the summation symbol $\sum$, which, for any map f with domain $\mathbb{N}$, we recursively define by:

$$\begin{aligned} \textstyle\sum_{i=1}^{1} f(i) &:= f(1); \\ \text{for } n > 1\text{: } \textstyle\sum_{i=1}^{n} f(i) &:= [\textstyle\sum_{i=1}^{n-1} f(i)] + f(n); \end{aligned}$$

Similarly, $n!$ is often expressed as $\prod_{i=1}^{n} i$. Here we use the product symbol $\prod$ which is recursively defined by:

$$\begin{aligned} \textstyle\prod_{i=1}^{1} f(i) &:= f(1); \\ \text{for } n > 1\text{: } \textstyle\prod_{i=1}^{n} f(i) &:= [\textstyle\prod_{i=1}^{n-1} f(i)] \cdot f(n). \end{aligned}$$

Example 6.1.3 — Fibonacci sequence. The Italian mathematician Fibonacci (1170-1250) studied the population growth of rabbits. He considered the following model of growth.

Start with one pair of rabbits, one male and one female rabbit.

As soon as a pair of rabbits, male and female, is one months old, it starts producing new rabbits. It takes another month before the young rabbits, again a pair consisting of a male and a female rabbit, are born. Let $F(n)$ denote the number of pairs in month n. We have the following recursive definition for F. Here $n \in \mathbb{N}$:

$$\begin{aligned} F(1) &:= 1; \\ F(2) &:= 1; \\ F(n+2) &:= F(n+1) + F(n). \end{aligned}$$

Indeed, in month $n+2$ we still have the pairs of one month earlier, i.e., $F(n+1)$, but also the young pairs of those pairs which are at least one month old in month $n+1$, i.e., the number of pairs in month n.

Fibonacci ©Public Domain

Figure 6.1: Fibonacci (1170-1250)

In the examples above we see that for a recursively defined function f we need two ingredients:

- a *base* part, where we define the function value $f(n)$ for some small values of n like 0 or 1.
- a *recursive* part in which we explain how to compute the function in n with the help of the values for integers smaller than n.

Of course, we do not have to restrict our attention to functions with domain $\mathbb{N}$. Recursion can be used at several places.

Example 6.1.4. Let S be the subset of $\mathbb{Z}$ defined by:

$3 \in S$;

if $x, y \in S$ then also $-x$ and $x+y \in S$.

Then S consists of all the multiples of 3. Indeed, if $n = 3m$ for some $m \in \mathbb{N}$, then $n = (\dots(3+3)+3)+\cdots+3)+3$, and hence is in S. But then also $-3m \in S$. Thus S contains all multiples of 3.

On the other hand, if S contains only multiples of 3, then in the next step of the recursion, only multiples of 3 are added to S. So, since initially S contains only 3, S contains only multiples of 3.

Example 6.1.5. Suppose R is a relation on a set S. We define $\overline{R} \subseteq S \times S$ recursively by

$R \subseteq \overline{R}$

if (a,b) and (b,c) in $\overline{R}$ then also $(a,c) \in \overline{R}$.

Then $\overline{R}$ is the transitive closure of R. Indeed, $\overline{R}$ contains R and is transitive. Hence it contains the transitive closure of R. We only have to show that $\overline{R}$ is contained in the transitive closure of R. This will be shown 6.4.3.

Example 6.1.6. Suppose Σ is a set of symbols. By Σ^* we denote the set of all strings over Σ. The set Σ^* can be defined by the following:

λ (the empty string) is in Σ^*;

if $w \in \Sigma^*$ and $s \in \Sigma$, then $w.s$ is in Σ^*.

Here $.$ stands for concatenation of the strings. So, If $\Sigma = \{a,b,c\}$, then

$$\Sigma^* = \{\lambda, a, b, c, aa, ab, ac, ba, bb, bc, ca, cb, cc, aaa, \dots\}.$$

Example 6.1.7. A (finite, directed) *tree* is a (finite) digraph Γ such that:

- there is a unique vertex, called the *root* of the tree with indegree 0; all other vertices have indegree 1;
- for any vertex v there is a path from the root to v.

Notice that a tree has no undirected cycles! (Often a tree is also considered to be a connected undirected graph containing no cycles.)

A tree is called *binary* is every vertex has outdegree 0 or 2. Notice that the graph consisting of a single vertex is a binary tree.

Moreover, if $T_1 = (V_1, E_1)$ and $T_2 = (V_2, E_2)$ are binary trees, then we can make a new binary tree $\mathsf{Tree}(T_1, T_2)$ in the following way. As vertex set we take the vertices of T_1 and T_2 and add a new vertex r. This vertex r is the root of the new tree and is the tail of two new edges with head r_1 and r_2, the roots of T_1 and T_2, respectively. All other edges come from T_1 and T_2. So $\mathsf{Tree}(T_1, T_2) = (V_1 \cup V_2 \cup \{r\}, E_1 \cup E_2 \cup \{(r, r_1), (r, r_2)\})$.

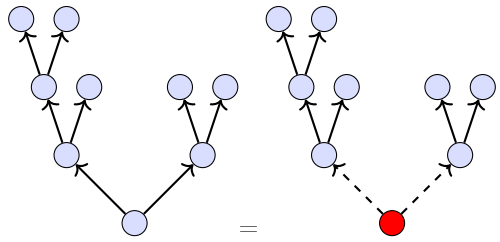


Figure 6.2: A tree composed out of two subtrees.

We can also give a recursive definition of the set of finite binary trees in the following way.

The set $\mathscr{T}$ of finite binary trees is defined by:

- the binary tree on a single vertex is in $\mathscr{T}$;
- if T_1 and T_2 are in $\mathscr{T}$, then $\mathsf{Tree}(T_1, T_2)$ is in $\mathscr{T}$.

Notice that a recursive definition of some operation or structure consists of:

- a definition of the basic structures or operations,
- a procedure to construct new basic structures or operations out of already constructed ones.

These two ingredients do not guarantee that a recursion is well defined. To avoid contradicting rules, we assume that if an object x is used (at some stage) in the construction of an object y, then y is not used in the construction of x.

This leads to an ordering $\sqsubseteq$ on the objects constructed. The basic objects are the minimal elements of the order; if $x_1, \ldots, x_n$ are objects used to create y then we say $x_i \sqsubset y$. The transitive and reflexive closure $\sqsubseteq$ of this relation is an order.

Indeed, if $x \sqsubseteq y$, then x is used in the construction of y but, unless $x = y$, the object y is not used for constructing x. As each object is constructed in finitely many steps, the order $\sqsubseteq$ only has descending chains of finite length. It is well founded.

Example 6.1.8. Consider the set $\mathscr{T}$ of finite directed binary trees as defined in Example 6.1.7. If $T_i = (V_i, E_i)$, $i = 1, 2$, are trees in $\mathscr{T}$, then we say $T_1 \sqsubseteq T_2$ if and only if $V_1 \subseteq V_2$ and E_1 is the set of all edges in E_2 with tail in V_1.

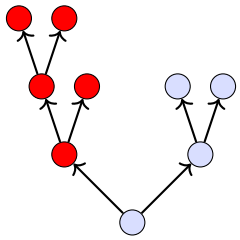


Figure 6.3: The red tree T_1 is part of the tree T, so $T_1 \sqsubseteq T$.

This relation is a well founded order on $\mathscr{T}$. (Prove this!) It is the transitive closure of the relation $\sqsubset$

defined in the above example.

6.2 Natural Induction

Principle 6.2.1 — Principle of Natural Induction. Suppose $P(n)$ is a predicate for $n \in \mathbb{Z}$. Let $b \in \mathbb{Z}$. If the following holds:

- $P(b)$ is true;
- for all $k \in \mathbb{Z}, k \geq b$ we have that $P(k)$ implies $P(k+1)$.

Then $P(n)$ is true for all $n \geq b$.

We give some examples:

Example 6.2.2. We claim that for all $n \in \mathbb{N}$ we have

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

We first check the claim for $n = 1$:

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

Now suppose that for some $k \in \mathbb{N}$ we do have

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

Then

$$\begin{array}{ll} \sum_{i=1}^{k+1} i & = (\sum_{i=1}^{k} i) + (k+1) \\ \text{(by assumption)} & = \frac{1}{2}k(k+1) + (k+1) \\ & = \frac{1}{2}(k+1)(k+2). \end{array}$$

Hence if the claim holds for some k in $\mathbb{N}$, then it also holds for $k+1$.
The principle of natural Induction implies now that for all $n \in \mathbb{N}$ we have

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

Warning. 6.2.3 A common mistake in a proof by induction is that the arguments for the induction step are given in the wrong order. Consider the following "proof" of the above example.

We prove by induction that for all $n \in \mathbb{N}$ we have

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

Basis $n = 1$:

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

Assume for $n = k$ we have $\sum_{i=1}^{n} i = \frac{1}{2}n(n+1)$.

Then for $n=k+1$:

$$\begin{aligned}
\sum_{i=1}^{n} i &= \tfrac{1}{2}n(n+1)\\
\sum_{i=1}^{k+1} i &= \tfrac{1}{2}(k+1)(k+2)\\
\sum_{i=1}^{k} i+(k+1) &= \tfrac{1}{2}(k+1)k+(k+1)\\
\sum_{i=1}^{k} i &= \tfrac{1}{2}(k+1)k
\end{aligned}$$

which is true.

The principle of natural induction implies now that for all $n \in \mathbb{N}$ we have

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

In this "proof" there are at least two things to notice. First, the connection between the various lines in the computation in red are not explained. Second, the computation starts with what we would like to proof and ends with what we know. The argument should go into the other direction!

Start with what you know (or assume) to be true, and work towards what you want to prove.

Example 6.2.4. For all $n \in \mathbb{N}$ and $x \in \mathbb{R}$, $x \neq 1$, we have

$$\sum_{i=1}^{n} x^i = \frac{x^{n+1}-x}{x-1}.$$

Here is a proof of this statement using natural induction. First consider the case $n = 1$. Then the left hand side of the above equation equals x. The right hand side equals $\frac{x^2-x}{x-1} = x$. So, for $n = 1$, equality holds.

Now assume that $\sum_{i=1}^{k} x^i = \frac{x^{k+1}-x}{x-1}$ for some $k \in \mathbb{N}$. Then $\sum_{i=1}^{k+1} x^i = [\sum_{i=1}^{k} x^i] + x^{k+1}$. By assumption this equals $\frac{x^{k+1}-x}{x-1} + x^{k+1} = \frac{x^{k+2}-x}{x-1}$.

The Principle of Natural Induction implies now that for all $n \in \mathbb{N}$ we have

$$\sum_{i=1}^{n} x^i = \frac{x^{n+1}-x}{x-1}.$$

Example 6.2.5. Let $a, b, c \in \mathbb{R}$. A *linear recurrence* is a recurrence relation of the form

$$\begin{aligned}
a_0 &:= a;\\
a_{n+1} &:= b \cdot a_n + c;
\end{aligned}$$

This is a generalization of the the recurrence relation as given in Example 6.2.4. For linear recurrence relations we can find a closed formula. Indeed,

$$a_n = b^n \cdot a + b^{n-1}c + b^{n-1} \cdot c + \cdots + b \cdot c + c = b^n \cdot a + \left(\frac{b^n - 1}{b-1}\right) \cdot c.$$

We give a proof by induction.

For $n = 1$ we indeed have $a_1 = b \cdot a + c = b^1 \cdot a + \left(\frac{b^1-1}{b-1}\right) \cdot c$.

Suppose that for some $k \in \mathbb{N}$ we do have the equality

$$a_k = b^k \cdot a + \left(\frac{b^k - 1}{b-1}\right) \cdot c.$$

Then

$$\begin{aligned}
a_{k+1} &= b \cdot a_k + c\\
&= b \cdot (b^k \cdot a + \left(\tfrac{b^k-1}{b-1}\right) \cdot c) + c\\
&= b^{k+1} \cdot a + \left(\tfrac{b^{k+1}-b}{b-1}\right) \cdot c + c\\
&= b^{k+1} \cdot a + \left(\tfrac{b^{k+1}-b+(b-1)}{b-1}\right) \cdot c\\
&= b^{k+1} \cdot a + \left(\tfrac{b^{k+1}-1}{b-1}\right) \cdot c.
\end{aligned}$$

By the principle of natural induction we now have proved that

$$a_n = b^n \cdot a + \left(\frac{b^n - 1}{b-1}\right) \cdot c.$$

for all $n \in \mathbb{N}$ with $n > 0$.

Example 6.2.6. Let S be a set with n elements, then $\mathscr{P}(S)$, the set of all subsets of S, has size 2^n. We give a proof by induction.

For $n = 0$, the set S is the empty set and S itself is the only subset of S. So indeed, in this case $\mathscr{P}(S)$ has size $2^0 = 1$.

Suppose for some $k \in \mathbb{N}$ all sets of size k have exactly 2^k distinct subsets. Then consider a set S of size $k+1$. Fix an element $s \in S$. Then all subsets of S not containing s are precisely the subsets of $S \setminus \{s\}$. Hence, there are 2^k such subsets of S. For each such subset T there is a unique subset $T \cup \{s\}$ of S containing s. As every subset T' of S containing s is obtained as $T' \setminus \{s\} \cup \{s\}$ there are also 2^k subsets containing s.

We conclude that $\mathscr{P}(S)$ contains $2^k + 2^k = 2^{k+1}$ elements.

Now the principle of natural induction implies that every set S of n elements admits exactly 2^n subsets.

Example 6.2.7 — Binomials. Let n, k be integers with $0 \leq k \leq n$. Then by

$$\binom{n}{k}$$

we denote the number of subsets of size k out of a set of n elements. It is called a *binomial* or *binomial coefficient*.

We do have the equality

$$\binom{n}{k} = \frac{n!}{k! \cdot (n-k)!}.$$

Indeed, we can order the elements of a set S of size n in $n!$ ways, and then take the first k elements to form a subset T of size k. Now any reordering of the elements in T and in $S \setminus T$, which can be done in $k! \cdot (n-k)!$ ways, will provide us with the same set T.

Suppose $k \leq n$, then the number of subsets of size $k+1$ of the set $\{1, \ldots, n+1\}$ equals the number of subsets of size k of $\{1, \ldots, n\}$ to which we add $n+1$, there are $\binom{n}{k}$ of them, added to the number of subsets $\{1, \ldots, n\}$ of size $k+1$, of which there are $\binom{n}{k+1}$.

This yields the following identity, known as Pascal's identity:

$$\binom{n}{k} + \binom{n}{k+1} = \binom{n+1}{k+1}.$$

An algebraic proof is also possible:

$$\begin{aligned}
\tbinom{n}{k} + \tbinom{n}{k+1} &= \tfrac{n!}{k!\cdot(n-k)!} + \tfrac{n!}{(k+1)!\cdot(n-k-1)!} \\
&= \tfrac{n!}{k!\cdot(n-k-1)!}\left(\tfrac{1}{n-k} + \tfrac{1}{k+1}\right) \\
&= \tfrac{n!}{k!\cdot(n-k-1)!} \cdot \tfrac{(k+1)+(n-k)}{(n-k)(k+1)} \\
&= \tfrac{n!}{k!\cdot(n-k-1)!} \cdot \tfrac{n+1}{(n-k)(k+1)} \\
&= \tfrac{(n+1)n!}{(k+1)k!\cdot(n-k)(n-k-1)!} \\
&= \tfrac{(n+1)!}{(k+1)!(n+1-(k+1))!} \\
&= \tbinom{n+1}{k+1}
\end{aligned}$$

We use this to prove the following identity, known as the *Binomium of Newton*:

For all x, y we have

$$(x+y)^n = \sum_{i=0}^{n} \binom{n}{i} x^i y^{n-i}.$$

$$
\begin{array}{ccccccccccccc}
 & & & & 1 & & 1 & & & & & & \\
 & & & 1 & & 2 & & 1 & & & & & \\
 & & 1 & & 3 & & 3 & & 1 & & & & \\
 & 1 & & 4 & & 6 & & 4 & & 1 & & & \\
1 & & 5 & & 10 & & 10 & & 5 & & 1 & & \\
 & 6 & & 15 & & 20 & & 15 & & 6 & & 1 & \\
 & & & & & \vdots & & & & & & &
\end{array}
$$

Figure 6.4: Triangle of Pascal: In the n-th row you find the values of $\binom{n}{k}$ with k running from 0 to n. The formula $\binom{n+1}{k} = \binom{n}{k} + \binom{n}{k+1}$ can be used to find the values in row $n+1$.

Our proof is by induction on n.
For $n = 1$ we have

$$(x+y)^1 = x+y = \binom{1}{0}x + \binom{1}{1}y.$$

Now suppose for $n = k$ we do have that

$$(x+y)^n = \sum_{i=0}^{n} \binom{n}{i} x^i y^{n-i}.$$

Then for $n = k+1$ we have

$$
\begin{array}{ll}
(x+y)^n & = (x+y)^{k+1} \\
 & = (x+y)\cdot(x+y)^k \\
\text{by assumption} & = (x+y)\cdot\left[\sum_{i=0}^{k}\binom{k}{i}x^i y^{k-i}\right] \\
 & = \displaystyle\sum_{i=0}^{k}\binom{k}{i}x^{i+1}y^{k-i} + \sum_{i=0}^{k}\binom{k}{i}x^i y^{k+1-i} \\
 & = \left[\displaystyle\sum_{i=0}^{k}\left(\binom{k}{i} + \binom{k}{i+1}\right)x^{i+1}y^{k-i}\right] + y^{k+1} \\
 & = \displaystyle\sum_{i=0}^{k+1}\binom{k+1}{i}x^k y^{k+1-i}
\end{array}
$$

Newton's Binomium also follows from the observation that when working out the product of n terms $x+y$ in

$$(x+y)\cdot(x+y)\cdots(x+y)$$

we find a term $x^k y^{n-k}$ when picking x from k different factors and y in the complementary set of factors. So, the numbers of terms $x^k y^{n-k}$ equals the number of subsets of size k in a set of size n.

Example 6.2.8. For $n \geq 3$ we have

$$\binom{n+2}{3} - \binom{n}{3} = n^2.$$

We prove this using induction on n.
The basis of induction is the case where $n = 3$. If $n = 3$, then

$$\binom{n+2}{3} - \binom{n}{3} = \frac{5\cdot 4\cdot 3}{3\cdot 2\cdot 1} - \frac{3\cdot 2\cdot 1}{3\cdot 2\cdot 1} = 10 - 1 = 3^2.$$

Now suppose for $n = k \geq 3$ we do have $\binom{n+2}{3} - \binom{n}{3} = n^2$. Then for $n = k+1$ we find

$$\begin{array}{ll}
\binom{n+2}{3} - \binom{n}{3} & = \binom{k+3}{3} - \binom{k+1}{3} \\
\text{(Pascal's identity)} & = \binom{k+2}{3} + \binom{k+2}{2} - \binom{k}{3} - \binom{k}{2} \\
& = \binom{k+2}{3} - \binom{k}{3} + \binom{k+2}{2} - \binom{k}{2} \\
\text{(Assumption)} & = k^2 + \binom{k+2}{2} - \binom{k}{2} \\
\text{(Pascal's identity)} & = k^2 + \binom{k+1}{2} + \binom{k+1}{1} - \binom{k}{2} \\
\text{(Pascal's identity)} & = k^2 + \binom{k}{2} + \binom{k}{1} + \binom{k+1}{1} - \binom{k}{2} \\
& = k^2 + \binom{k}{1} + \binom{k+1}{1} \\
& = k^2 + k + k + 1 \\
& = k^2 + 2k + 1 \\
& = (k+1)^2 \\
& = n^2.
\end{array}$$

So, by induction we have show for all $n \geq 3$ that

$$\binom{n+2}{3} - \binom{n}{3} = n^2.$$

As we have seen in the above examples, a proof by natural induction consists of 4 steps:

- A statement $P(n)$ for all $n \in \mathbb{N}$.
- A base b, for which $P(b)$ is true.
- A proof that for all $k \in \mathbb{N}$ (or $k \geq b$) we have: $P(k)$ implies $P(k+1)$.
- The conclusion that for all $n \geq b$ we have $P(n)$ is true.

6.3 Strong Induction and Minimal Counter Examples

In this section we discuss two variations on Natural Induction. The first is strong induction.

Principle 6.3.1 — Principle of Strong Induction. Suppose $P(n)$ is a predicate for $n \in \mathbb{Z}$. Let $b \in \mathbb{Z}$. If the following holds:

- $P(b)$ is true;
- for all $k \in \mathbb{Z}, k \geq b$ we have that $P(b), P(b+1), \ldots, P(k-1)$ and $P(k)$ together imply $P(k+1)$.

Then $P(n)$ is true for all $n \geq b$.

(Of course strong induction is just a variation of natural induction. Indeed, just replace the predicate $P(n)$ by the predicate $Q(n) := P(b) \wedge P(b+1) \wedge \cdots \wedge P(n)$.)

We give some examples.

Example 6.3.2. Consider the game of Nimm. In this game for two players a (positive) number of matches is placed on the table. The two players take turns removing one, two or three matches from the table. The player to remove the last match form the table loses.

The first player has a winning strategy if and only if the number of matches, n say, is not of the form $4m+1$, with $m \in \mathbb{N}$. Otherwise, the second player has a winning strategy.

We prove this statement with strong induction.

If $n = 1$, then the first player has to take the match from the table and loses.

Now suppose that the statement is correct for all values of n with $1 \leq n \leq k$ for some $k \in \mathbb{N}$. We will prove it to be true for $n = k+1$.

We divide the prove in two parts:

- $k+1 = 4m+1 > 1$ for some $m \in \mathbb{N}$.
  Since the first player can remove 1, 2 or 3 matches, the second player is faced with k, $k-1$ or $k-2$ matches. Since these numbers are not of the form $4l+1$, $l \in \mathbb{N}$, our induction hypothesis implies that there is a winning strategy for the second player.

Figure 6.5: Matches for Nimm

- $k+1 = 4m+i$ for some $m \in \mathbb{N}$ and $i = 2,3$ or 4.
  The first player can removes $i-1$ matches. Then the second player is facing $4m+1$ matches. By our induction hypothesis, there is a winning strategy for the first player.

Example 6.3.3. Suppose you have to divide an $n \times m$ chocolate bar into nm pieces. Then you will need to break it at least $nm-1$ times. This we can prove.

Figure 6.6: Break a bar of chocolade

If $nm = 1$, then we are dealing with a single piece of chocolate, and we don't have to do anything. So indeed, we need zero breaks.

Suppose, $nm > 1$ and for all $n' \times m'$ bars with $n'm' < nm$, we need at least $n'm'-1$ breaks to divided into $n'm'$ pieces. Then consider an $n \times m$ bar. Break it ones. Then one obtains two bars B_0 and B_1 of size $n_0 \times m_0$ and $n_1 \times m_1$, respectively, with $n_0m_0 + n_1m_1 = nm$. By our induction hypothesis, one has to break bar B_0 at least $n_0m_0 - 1$ times and bar B_0 at least $n_0m_0 - 1$ times. Hence in total we have to break the bar at least $1 + (n_0m_0 - 1) + (n_1m_1 - 1) = nm - 1$.

By the principle of strong induction we have shown that indeed one has to break an $n \times m$ chocolate bar at least $nm-1$ times to get nm pieces.

The second variation of natural induction that we discuss is the (non)-existence of a minimal counter example.

Principle 6.3.4 — Minimal Counter Example. Let $P(n)$ be a predicate for all $n \in \mathbb{Z}$. Let $b \in \mathbb{Z}$. If the statement that $P(n)$ is true for all $n \in \mathbb{Z}, n \geq b$, is *not true*, then there is a minimal counter example. That means, there is an $m \in \mathbb{Z}, m \geq b$ with

$P(m)$ false and

$P(n)$ true for all $n \in \mathbb{N}$ with $b \leq n < m$.

Example 6.3.5. A prime is a natural number $p > 2$ such that each divisor of p equals 1 or p. Every element $n \in \mathbb{N}$ with $n > 1$ is divisible by a prime.

Suppose m is a minimal counter example to this statement. Then, as $m|m$, we find that m cannot be prime. Hence, it admits a divisor $1 < m_1 < m$. As m is a minimal counter example to the statement, m_1 is divisible by some prime p. But by transitivity of the relation "divides", p also divides m. This contradicts m being the

minimal counter example. Hence we have proved the statement.

6.4 Structural Induction

In this final section we discuss another variation of induction, the so-called *structural induction*. If a structure of data types is defined recursively, then we can use this recursive definition to derive properties by induction.

In particular,

Principle 6.4.1 — Structural induction. If a structure of data types is defined recursively, then we can use this recursive definition to derive properties by induction.

In particular,

- if all basic elements of a recursively defined structure satisfy some property P,
- and if newly constructed elements satisfy P, assuming the elements used in the construction already satisfy P,

then all elements in the structure satisfy P.

We give some examples.

Example 6.4.2. In Example 6.1.7 we have given a recursive definition of the set $\mathscr{T}$ of finite binary trees.

$(*)$ In every binary tree T the number edges is one less than the number of vertices.

We prove this by induction:

The tree consisting of a single vertex has 1 vertex and 0 edges. Hence for this tree the statement is correct.

Now assume suppose a tree $T = (V,E)$ is obtained as $\mathsf{Tree}(T_1,T_2)$ where $T_1 = (V_1,E_1)$ and $T_2 = (V_2,E_2)$ are two binary trees satisfying $(*)$. Then the number of vertices in T equals $1+|V_1|+|V_2|$, and the number of edges equals $2+|E_1|+|E_2|$. Since $|V_1| = |E_i|+1$ we find that $|V| = |V_1|+|V_2|+1 = (|E_1|+1)+(|E_2|+1)+1 = |E|+1$. Hence T also satisfies $(*)$.

This proves that all finite binary trees satisfy $(*)$.

Example 6.4.3. Let R be a relation on a set S. In 6.1.5 we defined the relation $\overline{R}$. We will use structure induction to show that $\overline{R}$ is the transitive closure of R.

We already showed that $\overline{R}$ contains the transitive closure. So it remains to prove that $\overline{R}$ is contained in the closure.

Denote the transitive closure of R by TR. Our first step in the proof is to show that R is contained in TR. But this is by definition of TR. Next suppose $(a,b),(b,c)$ of $\overline{R}$ are also in TR, then the element (a,c) of $\overline{R}$ is also in TR as TR is transitive. Hence by structural induction, we have $\overline{R} \subseteq TR$ and hence we may conclude that $\overline{R} = TR$.

Although we will not go into the details, we want to mention that natural, strong and structural induction are actually particular cases of induction on a well founded order:

Principle 6.4.4 — The Principle of Induction on a well founded order. Let $(P,\sqsubseteq)$ be a well founded order. Suppose $Q(x)$ is a predicate for all $x \in P$ satisfying:

- $Q(b)$ is true for all minimal elements $b \in P$.
- If $x \in P$ and $Q(y)$ is true for all $y \in P$ with $y \sqsubseteq x$ but $y \neq x$, then $P(x)$ holds.

Then $Q(x)$ holds for all $x \in P$.

6.5 Exercises

Exercise 6.5.1. John wants to buy a new house. Therefore he needs \$200,000 from the bank. He can pay off this mortgage in 20 years, \$10,000 a year. Besides these \$10,000, John also has to pay 8% interest a year over the amount, he still has to pay to the bank.

What is the total amount John has to pay to the bank for this mortgage of $200.000?

Exercise 6.5.2. Suppose $f(n)$ is the number of strings of length n with symbols from the alphabet $\{a,b,c,d\}$ with an even number of a's.

(a) What is $f(0)$? And what $f(1)$?

(b) Show that f satisfies the recurrence

$$f(n+1) = 2 \cdot f(n) + 4^n.$$

Exercise 6.5.3. Suppose $f : \mathbb{N} \to \mathbb{Z}$ satisfies the recurrence relation

$$f(0) = 1 \text{ and } f(1) = 1$$

$$f(n+2) := 2f(n+1) - 4f(n).$$

(a) Show that for all $n \in \mathbb{N}$ we have $f(n+3) = -8f(n)$.

(b) Find a closed formula for $f(n)$ for all $n \in \mathbb{N}$ (No need to prove correctness.)

Exercise 6.5.4. Consider the following statement and its proof:

For all integers $n \geq 0$ we have $5n = 0$.

Proof. We prove this statement with strong induction.

Basis: for $n = 0$ we have $5n = 0$.

Step: Suppose for all $0 \leq k \leq n$ we have $5n = 0$. Then consider $5(n+1)$. Write $n+1 = i+j$ with $0 \leq i, j \leq n$. Then $5(n+1) = 5(i+j) = 5i + 5j = 0 + 0 = 0$ by assumption.

Hence by strong induction we have $5n = 0$ for all $n \geq 0$. □

Obviously something is wrong here. What is it?

Exercise 6.5.5. Let F be the Fibonacci sequence.

(a) Show that for all $n > 2$ we have

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

(b) Show that for all $n > 2$ we have

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

Exercise 6.5.6. Suppose f is defined on $\mathbb{N}$ by

$f(0) := 1$,

$f(n) = \frac{2n}{n+1} f(n-1)$ for all $n > 0$

Compute $f(1), f(2), \ldots, f(5)$. Can you find a closed formula for $f(n)$? Prove that your formula is correct for all $n \in \mathbb{N}$.

Exercise 6.5.7. Notice that $7 = 2 \cdot 2 + 3$ and $8 = 2 + 2 \cdot 3$. Every integer ≥ 7 can be written as $3a + 2b$ for some positive integers a, b.

Prove this by assuming that there is a minimal counterexample and obtain a contradiction.

Exercise 6.5.8. Let $n \in \mathbb{N}$. Prove that for all $m \in \mathbb{N}$ we have

$$\sum_{j=0}^{m} \binom{n+j}{n} = \binom{n+m+1}{n+1}.$$

Use induction on m.

Exercise 6.5.9. Prove that for all $n \geq 1$ we have

$$\sum_{i=0}^{n} \binom{n-i}{i} = F(n+1),$$

where $F(n+1)$ is the $(n+1)$-th Fibonacci number and $\binom{k}{j} = 0$ if $k < j$.

Exercise 6.5.10. Suppose f is defined on $\mathbb{N}$ by

$$\sum_{i=1}^{n} \frac{2i-1}{i^4 - 2i^3 + 3i^2 - 2i + 2}$$

Compute $f(1), f(2), \ldots, f(5)$. Can you find a closed formula for $f(n)$? Prove that your formula is correct for all $n \in \mathbb{N}$.

Exercise 6.5.11. Suppose f is defined on $\mathbb{N}$ by

$$\sum_{i=1}^{n} \frac{3i^2 - 3i + 1}{(i^3+1)(i^3 - 3i^2 + 3i)}$$

Compute $f(1), f(2), \ldots, f(5)$. Can you find a closed formula for $f(n)$? Prove that your formula is correct for all $n \in \mathbb{N}$.

Exercise 6.5.12. In a triangle in the plane, the sum of all the three angles equals $180°$. In a 4-gon, the sum of all the four angles equals $360°$. How about the sum of the angles in a convex n-gon with $n \geq 5$? (An n-gon is called convex, if any straight line between two vertices of the n-gon does not leave the interior of the n-gon.)

Exercise 6.5.13. Suppose you have an infinite collection of coins of 2 and 5 Euro cents.

Prove, using strong induction, that you can pay any amount of n Euro cents, where $n \in \mathbb{N}, n \geq 4$.

Give also a proof by assuming the existence of a minimal counter example and reaching a contradiction.

Exercise 6.5.14. Give a recursive definition of the set of all finite directed trees.

Use structural induction to prove that in all finite directed trees the number of edges is one less than the number of vertices.

Exercise 6.5.15. Consider the set $\mathscr{T}$ of binary trees as recursively defined in Example 6.1.7.

A *leaf* of a tree is a vertex with outdegree 0. Denote by l the number of leaves in a tree $T \in \mathscr{T}$. Then $l = (v+1)/2$ where v is the number of vertices. Prove this using structural induction.

Exercise 6.5.16. Let S be the subset of $\mathbb{Z}$ defined by

- $-12, 20 \in S$;
- if $x, y \in S$, then $x + y \in S$.

We use structural induction to show that $S = \{4k \mid k \in \mathbb{Z}\}$. The proof is divided into three parts.

(a) Show that 4 and -4 are in S.
(b) Prove, by structural induction, that $S \subseteq \{4k \mid k \in \mathbb{Z}\}$.
(c) Use (a) and structural induction to prove that $S \supseteq \{4k \mid k \in \mathbb{Z}\}$.

Exercise 6.5.17. In Example 6.1.7 we presented two definitions of binary trees:

- Definition by degrees: A finite, directed tree is a (finite) digraph such that:
  - there is a unique vertex, called the root of the tree with indegree 0; all other vertices have indegree 1 and outdegree 0 or 2;
  - for any vertex v there is a path from the root to v.
- A recursive definition:
  - the graph on a single vertex is a tree;
  - if T_1, T_k are trees, then $\mathsf{Tree}(T_1, T_2)$ is a tree.

(a) Use structural induction to show that a binary tree recursively defined does satisfy the conditions of the definition by degrees.

(b) Show that a binary tree defined by degrees, can be constructed recursively as in the second definition.
(c) Can you generalize the above to arbitrary trees which may not be binary?

7. Cardinalities

Let S be a set. To measure the size of a set, we can try to count the number of elements it contains. If S contains only finitely many elements, then that is easy. But also in case that S contains infinitely many elements, we can still measure its size.

Indeed, we can say that a set X has the same number of elements as a set Y, if and only if there is a bijection between X and Y.

For finite sets X and Y this is only possibile, if $|X| = |Y|$. But how about infinite sets?

To obtain an answer to this question, we study injective, surjective and bijective maps between (mainly) infinite sets.

7.1 Cardinality

Definition 7.1.1. Two sets A and B have the same *cardinality* if there exists a bijection from A to B.

Example 7.1.2. Two finite sets have the same cardinality if and only if they have the same number of elements.

Example 7.1.3. The sets $\mathbb{N}$ and $\mathbb{Z}$ have the same cardinality. Indeed, consider the map $f : \mathbb{N} \to \mathbb{Z}$ defined by $f(2n) = n$ and $f(2n+1) = -n$ where $n \in \mathbb{N}$. This map is clearly a bijection.

Theorem 7.1.4. Having the same cardinality is an equivalence relation.

Proof. We have to check that having the same cardinality is reflexive, symmetric and transitive.

Reflexivity. Let A be a set. Then the identity map $a \in A \mapsto a$ is a bijection from A to itself. So A has the same cardinality as A.

Symmetry. Suppose A has the same cardinality as B. Then there is a bijection $f : A \to B$. Now f has an inverse f^{-1}, which is a bijection from B to A. So B has the same cardinality as A.

Transitive. Suppose A has the same cardinality as B and B the same cardinality as C. So, there exist bijections $f : A \to B$ and $g : B \to C$. But then $g \circ f : A \to C$ is a bijection from A to C. So A has the same cardinality as C.

Georg Cantor

We conclude that having the same cardinality is an equivalence relation. □

7.2 Countable sets

Definition 7.2.1. A set is called *finite* if it is empty or has the same cardinality as the set $\mathbb{N}_n := \{1, 2, \ldots, n\}$ and *infinite* otherwise.

Definition 7.2.2. A set is called *countable* if it is finite or has the same cardinality as the set $\mathbb{N}$.
An infinite set that is not countable is called *uncountable*.

Theorem 7.2.3. Every infinite set contains an infinite countable subset.

Proof. Suppose A is an infinite set. Since A is infinite, we can start enumerating the elements of $a_1, a_2, \ldots$ such that all the elements are distinct. This yields a sequence of elements in A. The set of all the elements in this sequence form a countable subset of A. □

Theorem 7.2.4. Let A be a set. If there is a surjective map from $\mathbb{N}$ to A, then A is countable.

Proof. Let $f : \mathbb{N} \to A$ be a surjection. Then consider the sequence $f(1), f(2), \ldots$. Remove from this sequence (going from left to right) each element that you have seen before. The result is either a finite sequence, or an infinite sequence $f(n_1), f(n_2), \ldots$ of which all elements are distinct. In the latter case, consider the map $g : \mathbb{N} \to A$ with $g(i) = f(n_i)$. This map is a bijection, which proves A to be countable. □

Corollary 7.2.5. Let A be countable and $f : A \to B$ surjective, then B is countable.

Proof. Suppose A is a countable set and $f : A \to B$ a surjective map. If A is finite, then so is B. Thus assume that A has infinitely many elements. Since A is countable, there is a bijection $g : \mathbb{N} \to A$. But then $f \circ g$ is a surjection from $\mathbb{N}$ to B. Hence we can apply the previous result and find a bijection from $\mathbb{N}$ to B. This proves B to be countable. □

Theorem 7.2.6. Any subset of a countable set is countable.

Proof. Suppose A is an infinite subset of a countable set B. Let $f : \mathbb{N} \to B$ be bijective and fix an element $a \in A$. Now consider the map $g : \mathbb{N} \to A$ defined by $g(x) = f(x)$ if $f(x) \in A$ and $g(x) = a$ if $f(x) \in B \setminus A$. Then g is surjective, as f is surjective. Now Theorem 7.2.4 implies A to be countable. □

Proposition 7.2.7. $\mathbb{N} \times \mathbb{N}$ is countable.

Proof. Let $n \in \mathbb{N}$. Let m be maximal with $\sum_{i=0}^{m} i < n$. Now let $k = n - \sum_{i=0}^{m} i$. So, $1 \leq k \leq m+1$.
We define $f : \mathbb{N} \to \mathbb{N} \times \mathbb{N}$ in the following way:

$$f(n) = (k, m+2-k).$$

So, in a table this looks as follows:
The map f is a bijection. By construction, f is injective. Indeed, the m and k are uniquely defined by n.
So it only remains to prove surjectivity. Let $(k,l) \in \mathbb{N} \times \mathbb{N}$. Set $m = k+l-2$. Hence $(k,l) = (k, m+2-k)$ and $(k,l) = f(n)$ for n equal to $\sum_{i=0}^{m} i + k$. □

$f(1)=(1,1)$	$f(2)=(1,2)$	$f(4)=(1,3)$	$f(7)=(1,4)$	$\dots$
$f(3)=(2,1)$	$f(5)=(2,2)$	$f(8)=(2,3)$	$\dots$	
$f(6)=(3,1)$	$f(9)=(3,2)$	$\dots$		
$\vdots$	$\vdots$			

Theorem 7.2.8. Let A and B be countable sets. Then $A \times B$ is countable.

Proof. Suppose $f : \mathbb{N} \to A$ and $g : \mathbb{N} \to B$ are surjections. The map $h : \mathbb{N} \times \mathbb{N} \to A \times B$ defined by $h((i,j)) = (f(i), g(j))$ is surjective. So, since $\mathbb{N} \times \mathbb{N}$ is countable, also $A \times B$ is countable. □

Proposition 7.2.9. The sets $\mathbb{Z}$ and $\mathbb{Q}$ are countable.

Proof. The map $g : \{-1,1\} \times \mathbb{N} \to \mathbb{Z}$ given by $g(x,y) = xy$ is surjective. By Theorem 7.2.8 we find $\{-1,1\} \times \mathbb{N}$ to be countable, and hence also $\mathbb{Z}$.

Now let $f : \mathbb{Z} \times \mathbb{N} \to \mathbb{Q}$ be defined by $f(i,j) = \frac{i}{j}$ for $(i,j) \in : \mathbb{Z} \times \mathbb{N}$. This is clearly a surjective map.

By the previous result and Theorem 7.2.8 we find $\mathbb{Z} \times \mathbb{N}$ to be countable and hence also $\mathbb{Q}$. □

Theorem 7.2.10. Let $\mathscr{C}$ be a countable collection of countable sets. Then $\bigcup_{A \in \mathscr{C}} A$ is countable.

Proof. For each $A \in \mathscr{C}$ there exists a bijection $f_A : \mathbb{N} \to A$. Moreover, as $\mathscr{C}$ is countable, there exists also a bijection $g : \mathbb{N} \to \mathscr{C}$. We write $A_i = g(i)$.

Now consider the map $f : \mathbb{N} \times \mathbb{N} \to \bigcup_{A \in \mathscr{C}} A$ defined by $f(i,j) = f_{A_i}(j)$. This is a surjection. Thus $\bigcup_{A \in \mathscr{C}} A$ is countable. □

Example 7.2.11. Let S be the set of all finite subsets of $\mathbb{N}$. Then $S = \bigcup_{i \in \mathbb{N}} S_i$, where S_i is the set of subsets of size at most i of $\mathbb{N}$.

Now, by 7.2.8, $\mathbb{N}^i$ is countable. But the map $(a_1, \dots, a_i) \in \mathbb{N}^i \mapsto \{a_1, \dots, a_i\} \in S_i$ is clearly surjective. Thus S_i is also countable. Now Theorem 7.2.10 implies S to be countable.

Proposition 7.2.12. If A is infinite and B is finite then A and $A \cup B$ have the same cardinality.

Proof. Assume that A is infinite and, without loss of generality, that A and B are disjunct. Let A_0 be a countable subset of A. Then $A_0 \cup B$ is also countable. Then there exists a bijection $g : A_0 \cup B \to A_0$. Now define $f : A \cup B \to A$ by

$$f(x) = \begin{cases} g(x) & \text{if } x \in A_0 \cup B \\ x & \text{if } x \notin A_0 \cup B. \end{cases}$$

Then clearly f is a bijection between $A \cup B$ and A. □

7.3 Some uncountable sets

We have encountered various sets that are countable. In this section we concentrate on sets that are uncountable and derive a way to prove this.

Proposition 7.3.1. The set $\{0,1\}^{\mathbb{N}}$ is uncountable.

Proof. Let $F : \mathbb{N} \to \{0,1\}^{\mathbb{N}}$. By f_i we denote the function $F(i)$ from $\mathbb{N}$ to $\{0,1\}$.

We will show that F is not surjective by constructing a function $f \in \{0,1\}^{\mathbb{N}}$ which is different from all the functions f_i with $i \in \mathbb{N}$.

For each $i \in \mathbb{N}$ let

$$f(i) = 0 \text{ if } f_i(i) = 1 \text{ and}$$

$$f(i) = 1 \text{ if } f_i(i) = 0.$$

Clearly, for all $i \in \mathbb{N}$ we have $f(i) \neq f_i(i)$ and hence $f \neq f_i$. So, F is not surjective. This shows that there is no surjection from $\mathbb{N}$ to $\{0,1\}^{\mathbb{N}}$. In particular, $\{0,1\}^{\mathbb{N}}$ is not countable. □

Remark 7.3.2 — Cantor's diagonal argument. The main argument in the above proof is called *Cantor's diagonal argument*. Consider the following table.

$f_1(1)$	$f_1(2)$	$f_1(3)$	$\dots$
$f_2(1)$	$f_2(2)$	$f_2(3)$	$\dots$
$f_3(1)$	$f_3(2)$	$f_3(3)$	$\dots$
$\vdots$	$\vdots$	$\vdots$	

We have created a new function f which differs from all the f_i at the diagonal of this table, i.e. at position i. This argument can be applied in various situations.

If A is a set, then for each subset B of A we define the *characteristic function* $\chi_B : A \to \{0,1\}$ to be the function that takes the value 1 on all elements in B and the value 0 in all elements in $A \setminus B$.

Clearly, every element $f \in \{0,1\}^A$ is the characteristic function of the set $\{a \in A \mid f(a) = 1\}$. So, we find the map $B \in \mathscr{A} \mapsto \chi_B$ to be a bijection between from $\mathscr{P}(A)$ to $\{0,1\}^A$.

Corollary 7.3.3. The set $\mathscr{P}(\mathbb{N})$ has the same cardinality as $\{0,1\}^{\mathbb{N}}$ and hence is uncountable.

Proposition 7.3.4. The interval $[0,1)$ is uncountable.

Proof. Consider the map $f \in \{0,1\}^{\mathbb{N}} \mapsto \sum_{i=1}^{\infty} \frac{f(i)}{10^i} \in [0,1)$. This map is injective. So, if $[0,1)$ is countable, then so is $\{0,1\}^{\mathbb{N}}$, which contradicts the above Proposition 7.3.1.

This proves $[0,1)$ to be uncountable. □

We can also prove this proposition with Cantor's diagonal argument.

Proof. We provide a proof by contradiction.

So, assume that $[0,1)$ is countable and $f : \mathbb{N} \to [0,1)$ is a bijection. Then expand each $f(n)$ as a decimal number $0.a_{n,1}a_{n,2}a_{n,3}\dots$. (This may not be unique, but just take one.)

Now we apply Cantor's diagonal argument. For each $n \in \mathbb{N}$ let b_n be an integer between 0 and 9 with $b_n \equiv a_{n,n} + 5 \pmod{10}$ and consider $b = 0.b_1b_2b_3\dots$. Then $b \neq a_n$ for each $n \in \mathbb{N}$, and we find b not to be in the range of f. This contradicts f to be a bijection. We conclude that our assumption that $[0,1)$ is countable is wrong, and hence $[0,1)$ is uncountable. □

Corollary 7.3.5. $\mathbb{R}$ is uncountable.

Proof. As $\mathbb{R}$ contains the uncountable subset $[0,1)$, it is uncountable. □

Theorem 7.3.6. If A and B are sets with the same cardinality, then also $\mathscr{P}(A)$ and $\mathscr{P}(B)$ have the same cardinality.

Proof. Suppose A and B have the same cardinality. Let $f : A \to B$ be a bijection.
Consider the map $\hat{f} : \mathscr{P}(A) \to \mathscr{P}(B)$ given by $\hat{f}(S) = \{f(s) \mid s \in S\}$. This map is a bijection. □

Corollary 7.3.7. If A is an infinite set, then $\mathscr{P}(A)$ is uncountable.

Proof. If A is uncountable, then clearly $\mathscr{P}(A)$ is uncountable, as it contains the subset $\{\{a\} \mid a \in A\}$ of the same cardinality as A.
If A is countable, then $\mathscr{P}(A)$ is uncountable, as follows from 7.3.6 and 7.3.3. □

Cantor's diagonal argument can also be used to prove that the cardinality of a set is different (and hence smaller, see exercise 7.6.7) from that of its power set.

Theorem 7.3.8. Let X be a set, then $\mathscr{P}(X)$ does not have the same cardinality as X.

Proof. Suppose X and $\mathscr{P}(X)$ have the same cardinality and $f : X \to \mathbb{P}(X)$ is a bijection. Then consider the set

$$Y = \{x \in X \mid x \notin f(x)\}.$$

(Notice that the elements $(x, f(x))$ with $x \in f(x)$ can be considered to be the diagonal elements.)
As f is surjective, there is an element $y \in X$ with $f(y) = Y$.
Now, if $y \in Y$, then, by definition of Y, we find $y \notin f(y) = Y$ and we find a contradiction. So, we can assume that $y \notin Y$. But then again we find a contradiction as the definition of Y implies that $y \in Y$.
In all cases we obtain a contradiction. So, X and $\mathscr{P}(X)$ can not have the same cardinality. □

Remark 7.3.9. The above theorem shows us that we can get bigger and bigger sets in the following way:

$$\begin{aligned} X_1 &:= \mathbb{N} \\ \text{for } n > 1,\ X_n &:= \mathscr{P}(X_{n-1}). \end{aligned}$$

7.4 Cantor-Schröder-Bernstein Theorem

Suppose that A and B are sets and there are two maps $f : A \to B$ and $g : B \to A$ which are injective. Can we then conclude that A and B have the same cardinality?
The following result, first announced by Cantor, but eventually proven by Schröder and Bernstein, answers this question affirmatively.

Theorem 7.4.1 — Cantor-Schröder-Bernstein Theorem. Let A and B be sets and assume that there are two maps $f : A \to B$ and $g : B \to A$ which are injective. Then there exists a bijection $h : A \to B$.
In particular, A and B have the same cardinality.

The proof is divided into a few lemmas.
Let $A_0 = A$ and $B_0 = B$. Now, by recursion, define $B_{n+1} = f(A_n)$ and $A_{n+1} = A \setminus g(B \setminus B_{n+1})$.

Lemma 7.4.2. For all $n \in \mathbb{N}$ we have $A_{n+1} \subseteq A_n$ and $B_{n+1} \subseteq B_n$.

Proof. By induction, we prove that $B_{n+1} \subseteq B_n$ and $A_{n+1} \subseteq A_n$.

The base case where $n = 0$ is obvious. We do have $B_1 \subseteq B_0$ and $A_1 \subseteq A_0$.

Now assume that for $n = k$ we do have both $A_{n+1} \subseteq A_n$ and $B_{n+1} \subseteq B_n$. Then for $n = k+1$ we get $B_{n+1} = B_{k+2} = f(A_{k+1})$. As, by our assumption, we have $A_{k+1} \subseteq A_k$, we also find $f(A_{k+1}) \subseteq f(A_k) = B_{k+1} = B_n$. In particular,

$$B_{n+1} \subseteq B_n.$$

But then also

$$A_{n+1} = A \setminus g(B \setminus B_{n+1}) \subseteq A \setminus g(B \setminus B_n) = A_n.$$

So, by induction we have proven that for all $n \in \mathbb{N}$ we have $A_{n+1} \subseteq A_n$ and $B_{n+1} \subseteq B_n$.

□

Let $A_\infty = \bigcap_{n\in\mathbb{N}} A_n$ and $B_\infty = \bigcap_{n\in\mathbb{N}} B_n$.

Lemma 7.4.3. $f(A_\infty) = B_\infty$.

Proof. Let $a \in A_\infty$. Then $a \in A_n$ for all $n \in \mathbb{N}$. Hence $f(a) \in B_{n+1}$ for all $n \in \mathbb{N}$ and therefore in B_∞. So, $f(A_\infty)$ is contained in B_∞.

Now assume $b \in B_\infty$. Then $b \in B_n$ for all $n \in \mathbb{N}$. But then for $n > 0$ we find an element $a_{n-1} \in A_{n-1}$ with $f(a_{n-1}) = b$. As f is injective, we find $a_n = a_m$ for all $n, m > 0$. Let $a = a_1$. Then $a \in A_\infty$ and $f(a) = b$. So, the image of $f(A_\infty)$ contains B_∞.

We conclude that $f(A_\infty) = B_\infty$. □

Lemma 7.4.4. $g(B \setminus B_\infty) = A \setminus A_\infty$.

Proof. Suppose $b \in B \setminus B_\infty$. Then we can find an $n \in \mathbb{N}$ such that $b \notin B_{n+1}$. As g is injective, we also find $g(b) \notin A_{n+1}$ proving $g(b) \in A \setminus A_\infty$.

So, $g(B \setminus B_\infty)$ is contained in $A \setminus A_\infty$.

Now assume $a \in A \setminus A_\infty$. Then $a \notin A_{n+1}$ for some $n \in \mathbb{N}$. But that can only happen if $a = g(b)$ for some $b \in B \setminus B_{n+1}$. As g is injective, this b is unique and not in B_∞. So, $g(B \setminus B_\infty)$ contains A_∞.

We find $g(B \setminus B_\infty) = A \setminus A_\infty$. □

Let $f_\infty : A_\infty \to B_\infty$ be the restriction of f to A_∞ and $g_\infty : B \setminus B_\infty \to A \setminus A_\infty$ the restriction of g to $B \setminus B_\infty$. Then both f_∞ and g_∞ are injective as f and g are and surjective as follows from the above lemmas. In particular, f_∞ and g_∞ are bijections. We can combine them to obtain a bijection $h : A \to B$. Define $h : A \to B$ by

$$h(a) = \begin{cases} f_\infty(a) & \text{if } a \in A_\infty \\ g_\infty^{-1}(a) & \text{if } a \notin A_\infty. \end{cases}$$

Lemma 7.4.5. $h : A \to B$ is a bijection.

Proof. The function h is injective as both f and g_∞ are injective. Surjectivity follows immediately from the above lemmas. □

The Cantor-Schröder-Bernstein Theorem 7.4.1 follows from the lemma.

Corollary 7.4.6. Let A be a set and assume $B \subseteq A$ has the same cardinality as A. Then each subset C of A with $B \subseteq C \subseteq A$ has the same cardinality as A.

Proof. Assume $B \subseteq C \subseteq A$. Then clearly, the map $f : C \to A$ with $f(c) = c$ for all $c \in C$ is injective.

If B and A have the same cardinality, there is a bijective map $g : A \to B$. But this map can also be considered to be an injective map from A to C. So, 7.4.1 implies C and A to have the same cardinality. □

Proposition 7.4.7. The sets $\{0,1\}^{\mathbb{N}}$ and $[0,1)$ have the same cardinality.

Proof. We show that $A = \{0,1\}^{\mathbb{N}}$ and $B = [0,1)$ have the same cardinality. For this we construct injections from A into B and from B into A and then apply 7.4.1.

The map $\phi : A \to B$ given by $f \in \{0,1\}^{\mathbb{N}} \mapsto \sum_{i=1}^{\infty} \frac{f(i)}{10^i} \in [0,1)$ is injective.

We will also construct a map from B to A which is injective. So, let $x \in B = [0,1)$, then define $f_x \in \{0,1\}^{\mathbb{N}}$ as follows. First let $f_x(1) = 1$ if $x \geq \frac{1}{2}$ and 0 otherwise.

Now recursively define $f_x(n+1)$ by

$$f_x(n+1) = \begin{cases} 1 & \text{if } x - \sum_{k=1}^{n} \frac{f_x(k)}{2^k} \geq \frac{1}{2^{n+1}} \\ 0 & \text{otherwise} \end{cases}$$

Notice that for all $n \geq 1$ we have

$$0 \leq x - \sum_{k=1}^{n} \frac{f_x(k)}{2^k} < \frac{1}{2^n}.$$

We claim that the map ψ mapping $x \in [0,1)$ to the map f_x is injective.

Indeed, suppose $x < y \in [0,1)$ but $f_x = f_y$. Then let N be the smallest integer with $y - x \geq \frac{1}{2^N}$. So

$$\frac{1}{2^N} \leq y - x < \frac{1}{2^{N-1}},$$

and

$$2^N \leq y - x = (y - \sum_{k=1}^{N} \frac{f_y(k)}{2^k}) - (x - \sum_{k=1}^{N} \frac{f_x(k)}{2^k}) < \frac{1}{2^{N-1}}.$$

This implies that $y - \sum_{k=1}^{N} \frac{f_y(k)}{2^k} \geq \frac{1}{2^{N+1}}$ and $x - \sum_{k=1}^{N} \frac{f_x(k)}{2^k} < \frac{1}{2^{N+1}}$. But then $f_y(N+1) = 1$ and $f_x(N+1) = 0$ contradicting that $f_x = f_y$. □

Theorem 7.4.8. The sets $\mathbb{R}$, $\{0,1\}^{\mathbb{N}}$ and $\mathscr{P}(\mathbb{N})$ have the same cardinality.

Proof. Let $f : (0,1) \to \mathbb{R}$ be defined by

$$f(x) = \tan(\pi(x - 1/2)).$$

One easily checks that f is a bijection. So, $(0,1)$ and by 7.2.12 also $[0,1)$ has the same cardinality as $\mathbb{R}$. By 7.4.7 and 7.3.3 the sets $\mathbb{R}$, $\{0,1\}^{\mathbb{N}}$ and $\mathscr{P}(\mathbb{N})$ all have the same cardinality. □

Theorem 7.4.9. The sets $\mathbb{R}^n$, with $n > 0$, and $\mathbb{R}$ have the same cardinality.

Proof. We first prove that $\mathbb{R}^2$ and $\mathbb{R}$ have the same cardinality. But that is equivalent by showing that

$$\{0,1\}^{\mathbb{N}} \times \{0,1\}^{\mathbb{N}}$$

and

$$\{0,1\}^{\mathbb{N}}$$

have the same cardinality.

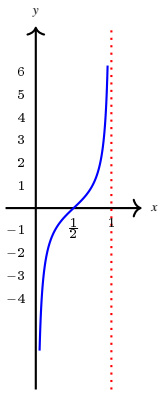


Figure 7.1: The graph of the function f of the proof of 7.4.8.

By 7.4.1 we only have to construct an injection from $\{0,1\}^{\mathbb{N}} \times \{0,1\}^{\mathbb{N}}$ to $\{0,1\}^{\mathbb{N}}$.
For $(f,g) \in \{0,1\}^{\mathbb{N}} \times \{0,1\}^{\mathbb{N}}$ define

$$F_{f,g} : \mathbb{N} \to \{0,1\}$$

by

$$F_{f,g}(n) = \begin{cases} f(\frac{n}{2}) & \text{if } n \text{ even} \\ g(\frac{n+1}{2}) & \text{if } n \text{ odd.} \end{cases}$$

Clearly we can recover f and g from $F_{f,g}$. So the map that maps (f,g) to $F_{f,g}$ is a wanted injection.
So, $\mathbb{R}^2$ has the same cardinality as $\mathbb{R}$.
As, for $n > 1$, we can identify $\mathbb{R}^n$ with $\mathbb{R}^{n-1} \times \mathbb{R}$, we can prove by induction that $\mathbb{R}^n$ has the same cardinality as $\mathbb{R} \times \mathbb{R}$ and hence as $\mathbb{R}$. □

Example 7.4.10. Let $\mathscr{L}$ be the set of straight lines in the plane $\mathbb{R}^2$. Then $\mathbb{R}$ and $\mathscr{L}$ have the same cardinality.
The map $f : \mathbb{R}^2 \setminus \{(0,0)\} \to \mathscr{L}$ with $f(a,b)$ being the line with equation $ax + by = 1$ is injective.
The map $g : \mathscr{L} \to \mathbb{R}^3$ which maps a line ℓ to a triple $(a,b,c) \in \mathbb{R}^3$ with $ax + by = c$ being an equation for ℓ is also injective. (You just take one such triple for each line.)
As $\mathbb{R}$, $\mathbb{R}^2 \setminus \{(0,0)\}$ and $\mathbb{R}^3$ have the same cardinality, there exist bijections $h_1 : \mathbb{R} \setminus \{(0,0)\} \to \mathbb{R}$, and $h_2 : \mathbb{R} \to \mathbb{R}$. But then $f \circ h_2^{-1}$ is an injection from $\mathbb{R}$ to $\mathscr{L}$, and $h_3 \circ g$ is an injection from $\mathscr{L}$ to $\mathbb{R}$.
By the Cantor-Schröder-Bernstein Theorem 7.4.1 we find $\mathscr{L}$ and $\mathbb{R}$ to have the same cardinality.

7.5 Additional Axioms of Set Theory

In the previous chapters and sections we developed some set theory, but we have been a bit sloppy. For example, to prove that every infinite set A contains a countable subset, see 7.2.3, we construct a series of distinct elements $a_1, a_2, \ldots$ leading to an infinite countable subset. The intuitive nature of the proof obscures the fact that it is not a trivial truth that one may choose elements $a_1, a_2, \ldots$ in this manner when the set A is infinite.

Of course we can do this any finite number of times. But can we also do it infinitely often?

To be able to do this, we need (a weak version of) the Axiom of Choice, which informally states that given any (and hence also any infinite) collection of sets, each with at least one element, it is possible to create a new set by choosing one element from each set in the collection.

Principle 7.5.1 — *Axiom of Choice*. Let $\mathscr{C}$ be a collection of nonempty sets. Then there exists a map

$$f : \mathscr{C} \to \bigcup_{A \in \mathscr{C}} A$$

with $f(A) \in A$.
The image of f is a subset of $\bigcup_{A\in\mathscr{C}} A$.
The function f is called a *choice function*.

The axiom of choice does not follow from basic Set Theory. So, it is an additional axiom.

The existence of a countable set follows from the latter axiom. We argue as follows.

Let A be an uncountable set and for each $n \in \mathbb{N}$ consider X_n to be the set all subsets of A of size n. Then $X_n \neq \emptyset$. By X we denote the set $\{X_n \mid n \in \mathbb{N}\}$ which is countable. Now by the Axiom of Choice there does exists a choice function $f : \mathbb{N} \to X$. Take the set $B = \bigcup_{x\in X} f(x)$. As B is a countable union of finite sets, it is countable. Moreover, B is clearly infinite, as it contains subsets of size n for each $n \in \mathbb{N}$.

There are many statements that are equivalent to the Axiom of Choice. For example:

Principle 7.5.2. The following statements are equivalent to the Axiom of Choice.

- For any two sets A and B there does exist a surjective map from A to B or from B to A.
- The cardinality of an infinite set A is equal to the cardinality of $A \times A$.
- Every vector space has a basis.
- For every surjective map $f : A \to B$ there is a map $g : B \to A$ with $f(g(b)) = b$ for all $b \in B$. (The map g is called a right inverse of f.)

Another problem occurs when we consider sets that contain them selves: Consider the set S of all sets that do not contain themselves as element. So, let U be the set of all sets and define

$$S = \{X \in U \mid X \notin X\}.$$

Now is $S \in S$ or not?

If $S \in S$, then by definition of S, we find $S \notin S$. If $S \notin S$, then by definition of S we have that $S \in S$. In both cases we obtain a contradiction. This example is know as *Russell's paradox*.

A more popular example of Russell's paradox is the following.

In a small town there is a barber. It is the unique person who shaves all those, and those only, who do not shave themselves. The question is, does the barber shave himself?

Any answer to this question results in a contradiction: The barber cannot shave himself, as he only shaves those who do not shave themselves. So, he does not shave himself. But the barber shaves all persons who do not shave themselves, so he should shave himself.

Russell's paradox was discovered by Bertrand Russell in 1901. It shocked the mathematical world. In the years after, many logicians started to investigate the foundations of set theory. Several new axiom systems have been proposed to avoid the problems caused by Russell's paradox. The most common axiom system is the Zermelo–Fraenkel system together with the Axiom of Choice. The axiom which is crucial for avoiding the problems caused by the paradox is the Axiom of Regularity.

Principle 7.5.3 — *Axiom of Regularity*. Let X be a nonempty set of sets. Then X contains an element Y with $X \cap Y = \emptyset$.

As a result of this axiom any set S cannot contain itself. Indeed, consider $X = \{S\}$ then there is a set Y in X with $X \cap Y = \emptyset$. As X only contains S, the set Y can only be S. So, $X \cap Y = \{S\} \cap S = \emptyset$. However, if $S \in S$, then $S \cap \{S\}$ would contain S. This contradiction shows $S \notin S$.

7.6 Exercises

Exercise 7.6.1. Prove that the following sets are countable.
(a) $\{x \in \mathbb{R} \mid x^2 \in \mathbb{Q}\}$.
(b) $\{x \in \mathbb{R} \mid \sin(x) \in \mathbb{Q}\}$.

Exercise 7.6.2. Let S be the set of all finite subsets of $\mathbb{N}$. Prove that S is countable.

Exercise 7.6.3. Let S be the subset

$$\{f \in \{0,1\}^{\mathbb{N}} \mid \exists m \in \mathbb{N} \forall n \geq m[f(n) = 0]\}$$

of $\{0,1\}^{\mathbb{N}}$.

Prove that S is countable.

Exercise 7.6.4. If A is an uncountable set and B is a countable subset of A, then $A \setminus B$ is uncountable. Give a proof.

Exercise 7.6.5. Prove that the set of all infinite integer sequences $(a_i)_{i \in \mathbb{N}}$, where $a_i \in \mathbb{N}$ for all i is uncountable.

Exercise 7.6.6. Let $\mathscr{C}$ be the set of all circles in the plane $\mathbb{R}^2$. Prove that $\mathscr{C}$ and $\mathbb{R}$ have the same cardinality.

Exercise 7.6.7. By $\mathscr{S}$ we denote a set of sets. The relation "having the same cardinality" is an equivalence relation on $\mathscr{S}$. The set of the equivalence classes is denoted by $\mathscr{C}$.

On $\mathscr{C}$ we define a relation $\sqsubseteq$ by the following rule: For $C, D \in \mathscr{C}$ we have $C \sqsubseteq D$ if and only if there are sets $X \in C$ and $Y \in D$ for which there exists an injective function $f : X \to Y$.
(a) Prove that $\sqsubseteq$ is well defined.
(b) Prove that $\sqsubseteq$ is a partial order on $\mathscr{C}$.

Exercise 7.6.8. Suppose $x < y$ are two real numbers, then the open interval (x, y) contains a rational number.

Use this to prove that a collection of pairwise disjunct open intervals is countable.

Exercise 7.6.9. Let $b \in \mathbb{R}$ and A be a subset of $\mathbb{R}^+$ with the property that for each finite subset $\{a_1, \ldots, a_n\}$ of A it holds that $a_1 + \cdots + a_n \leq b$.
(a) Show that for each $n \in \mathbb{N}$ it holds that $A_n := \{x \in A \mid x \geq \frac{1}{n}\}$ is finite.
(b) Prove that A is countable.

8. Integer Arithmetic

In this chapter we study properties of the set $\mathbb{Z}$ of integers. We mainly deal with its multiplicative structure and discuss notions such as the greatest common divisor ($\gcd$) and the least common multiple (lcm) of two (or more) integers.

8.1 Divisors and Multiples

Let $\mathbb{Z}$ denote the set of integers. We know how to add integers, how to subtract them and how to multiply them. Division is a bit harder.

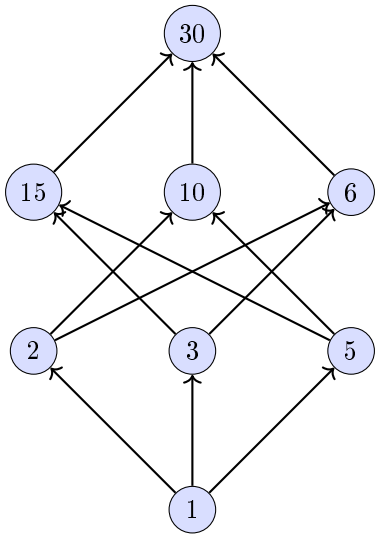


Figure 8.1: A schematic representation of all positive divisors of 30.

Euclid

Definition 8.1.1. Let $a \in \mathbb{Z}$ and $b \in \mathbb{Z}$.
- We call b a *divisor* of a, if there is an integer q such that $a = q \cdot b$.
- If b is a nonzero divisor of a then the (unique) integer q with $a = q \cdot b$ is called the *quotient* of a by b and denoted by $\frac{a}{b}$, a/b, or $\text{quot}(a,b)$.

If b is a divisor of a, we also say that b *divides* a, or a is a *multiple* of b, or a is *divisible* by b. We write this as $b|a$.

Example 8.1.2. If $a = 13$ and $b = 5$ then b does not divide a. Indeed, if there were an integer q such that $a = q \cdot b$, then q should be between 2 and 3, so $q = 2$ or $q = 3$. But neither value of q works. For instance, the former choice gives remainder 3 as $a = 2 \cdot b + 3$.

However, if $a = 15$ and $b = 5$ then b does divide a, as $a = 3 \cdot b$. So, in the latter case, the quotient of a by b equals 3.

Example 8.1.3. For all integers n we find $n-1$ to be a divisor of $n^2 - 1$.

Indeed, $n^2 - 1 = (n+1) \cdot (n-1)$.

More generally, for all $m \geq 2$ we have $n^m - 1 = (n-1) \cdot \left(n^{m-1} + n^{m-2} + \cdots + 1\right)$. So, $n-1$ divides $n^m - 1$.

Example 8.1.4. The *even* integers are simply the integers divisible by 2, such as 2, 6, and -10. Any even integer can be written in the form $2 \cdot m$ for some integer m.

The integers which are not divisible by 2, like 1 and -7, are usually called *odd*.

The following observations are straightforward, but very useful.

Lemma 8.1.5. Suppose that a, b and c are integers.
(a) If a divides b, and b divides c, then a divides c.
(b) If a divides b and c, then a divides $x \cdot b + y \cdot c$ for all integers x and y.
(c) If b is nonzero and if a divides b, then $|a| \leq |b|$.

Proof.

Part (a).

Suppose a divides b, and b divides c. Then there exist integers u and v such that $b = u \cdot a$ and $c = v \cdot b$. Consequently, $c = v \cdot (u \cdot a)$. Hence, $c = (v \cdot u) \cdot a$, and so a divides c.

Part (b).

Suppose that a divides b and c. Then there exist integers u and v such that $b = u \cdot a$ and $c = v \cdot a$. So, for all integers x and y, we have $x \cdot b + y \cdot c = x \cdot u \cdot a + y \cdot v \cdot a$. But this equals $(x \cdot u + y \cdot v) \cdot a$. Hence, $x \cdot b + y \cdot c$ is a multiple of a for all integers x and y.

Part (c).

Since a divides b, there exists an integer q such that $q \cdot a = b$. As b is nonzero, q must be nonzero. From this equality we get $|q| \cdot |a| = |b|$. Since $|q| \geq 1$, we conclude that $|a| \leq |b|$.

□

Clearly, division is not always possible within the integers. Indeed, suppose you need to fit rods of length $b = 4$ one after the other in a box of length $a = 23$. Then you can fit 5 rods in the box, and there will be an open space of length 3. This is an example of *division with remainder*.

Here is a precise statement about division with remainder.

Theorem 8.1.6 — Division with Remainder. If $a \in \mathbb{Z}$ and $b \in \mathbb{Z} \setminus \{0\}$, then there are unique integers q and r such that $a = q \cdot b + r$, $|r| < |b|$, and $b \cdot r \geq 0$.

Proof. In the case where both a and b are positive, the proof is roughly as follows. Find the greatest multiple $q\cdot b$ of b that is less than or equal to a; this can be accomplished by starting with $q=0$ and increasing q by 1 until $a-(q+1)\cdot b<0$. Then $r=a-q\cdot b$.

A proof follows that proceeds by induction on $|a|$.

The theorem holds if $|a|=0$.

Suppose $|a|=0$. Then $a=0$. Clearly, $q=0$ and $r=0$ is a solution. To show that this solution is unique, suppose that q and r represent a solution. Then $r=(-q)\cdot b$. If $q\neq 0$, then $|q|\geq 1$, so $|r|\geq|b|$, which contradicts the requirement $|r|<|b|$. Hence $q=0$. It immediately follows that also $r=0$. This establishes uniqueness of the solution.

Existence of q and r for non negative a and b.

Suppose that a and b are non negative. If $a<b$, then we set $q=0$ and $r=a$. If $a\geq b$, then $0\leq a-b<|a|$, so the induction hypothesis implies that there exist integers q' and r' (with $0\leq r'<b$) such that $a-b=q'\cdot b+r'$. This rewrites to $a=(q'+1)\cdot b+r'$. Now $q=q'+1$ and $r=r'$ satisfy the requirements of the theorem.

Existence of q and r for negative a and positive b.

If $a<0$, then $-a>0$, so by the above assertion there are q' and r' with $-a=q'\cdot b+r'$ and $0\leq r'<b$. But then $a=(-q'-1)\cdot b+(b-r')$ with $0\leq b-r'\leq b$. If $r'=0$ then $q=-q'$ and $r=0$, and if $r'>0$, then $q=-q'-1$ and $r=b-r'$ satisfy the requirements of the theorem.

Existence of q and r for negative b.

If b is negative, then applying one of the two previous assertions to $-a$ and $-b$ yields q' and r' with $-a=q'\cdot(-b)+r'$, where r' satisfies $0\leq r'<-b$. If we take $q=-q'$ and $r=-r'$ then $a=q\cdot b+r$ and $b<r\leq 0$ as required. We have shown the existence of both q and r.

Uniqueness of q and r for nonzero a.

Suppose that $a=q\cdot b+r$ and $a=q'\cdot b+r'$ with both $|r|$ and $|r'|$ less than $|b|$ and satisfying $b\cdot r\geq 0$ and $b\cdot r'\geq 0$.

Suppose moreover that $r\geq r'$. This restriction is not essential as the roles of r and r' can be interchanged. By subtracting the two equalities we find $0\leq r-r'=(q'-q)\cdot b$. Now, since b is nonzero, r and r' have the same sign. But then, as both r and r' are in absolute value less than $|b|$, we find that $0\leq r-r'<|b|$. It follows that the integral multiple $(q'-q)\cdot b$ of b satisfies $0\leq(q'-q)\cdot b<|b|$. This can only happen if $q'-q=0$. In other words, $q=q'$. But then it also follows that $r=r'$. □

Example 8.1.7. If $a=23$ and $b=7$, then division of a by b yields $23=3\cdot 7+2$. So, the quotient of $a=23$ by $b=7$ equals 3 and the remainder is 2.

If $a=-23$ and $b=7$, the quotient and remainder are $q=-4$ and $r=5$, respectively.

Finally, if $a=-23$ and $b=-7$, the quotient and remainder are $q=3$ and $r=-2$, respectively.

Example 8.1.8. For all integers n greater than 2 the remainder of n^2+1 divided by $n+1$ is 2. This follows immediately from the equality $n^2+1=(n+1)\cdot(n-1)+2$.

What is the remainder when n is less than or equal to 2?

Example 8.1.9. An odd integer leaves remainder 1 or -1 upon division by 2, since these are the only two nonzero integers whose absolute value is less than 2. Any odd integer can therefore be written in the form $2\cdot m+1$ or $2\cdot m-1$ for some integer m. In particular, adding or subtracting 1 from an odd integer gives an even integer. Likewise, adding or subtracting 1 from an even integer produces an odd integer.

Remark 8.1.10. The definitions of quotient and remainder as given here are used in many programming languages and computer algebra packages, see for example Mathematica or Python. However, sometimes slightly different definitions are used. For example, in Java the remainder r of a divided by b is defined by the property that $a=q\cdot b+r$ for some integer q where $|r|<|b|$ and $a\cdot r\geq 0$.

The integer q of the theorem is called the *quotient* of a divided by b. It is denoted by $\text{quot}(a,b)$. The integer r is called the *remainder* of a divided by b and will be denoted by $\text{rem}(a,b)$.

The Division with Remainder Theorem 8.1.6 states that there exist a quotient q and a remainder r, but it does not tell you how to find those two integers. A standard and well-known algorithm is of course *long division*. We describe (a variation of) this algorithm for finding q and r.

Algorithm 8.1.11 — Division and Remainder.

- Input: an integer a and a nonzero integer b.
- Output: the quotient q and remainder r of a upon division by b as a list $[q,r]$.

```
DivisionRemainder := procedure(a, b)
local variables
    | q := 0 , r, x
while (q+1)·|b| ≤ |a| do
    | x := q , q := x+1
r := |a| − q·|b|
if (a ≥ 0) ∧ (b > 0)
    | then
    |     | return
    |     |     | [q, r]
    | else
    |     | if (a ≥ 0) ∧ (b < 0)
    |     |     | then
    |     |     |     | return
    |     |     |     |     | [−q−1, b+r]
    |     |     | else
    |     |     |     | if (a < 0) ∧ (b > 0)
    |     |     |     |     | then
    |     |     |     |     |     | return
    |     |     |     |     |     |     | [−q−1, b−r]
    |     |     |     |     | else
    |     |     |     |     |     | return
    |     |     |     |     |     |     | [q, −r]
```

Proof.

Correctness.

By construction we have $a = q\cdot b + r$. Moreover, as $|q|\cdot|b| \le |a| < (|q|+1)\cdot|b|$ we find $|r| < |b|$. This proves correctness.

Termination.

Since b is nonzero, the while loop will end. Thus the algorithm terminates.

□

For a better understanding of the relations between two or more integers, it is useful to consider the divisors and multiples they have in common.

Definition 8.1.12. Let a and b be integers.

- An integer d is a *common divisor* of a and b if $d|a$ and $d|b$.
- If a and b are not both zero, the largest common divisor of a and b exists (see below) and is called *the greatest common divisor* of a and b.
  We denote the greatest common divisor (gcd) of a and b by $\gcd(a,b)$.
- If the greatest common divisor of a and b equals 1, then a and b are called *relatively prime*.

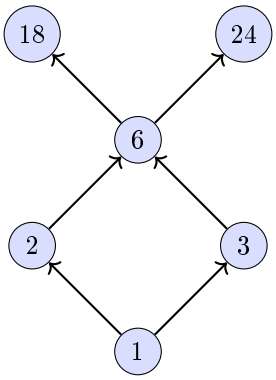


Figure 8.2: Positive common divisors of 18 and 24.

Example 8.1.13. The positive divisors of $a = 24$ are 1, 2, 3, 4, 6, 8, 12, and 24. Those of $b = 15$ are 1, 3, 5, and 15. Hence, the common divisors of a and b are 1 and 3 and their negatives. So the greatest common divisor equals 3.

Example 8.1.14. The positive common divisors of $a = 24$ and $b = 16$ are 1, 2, 3, 4, and 8. Hence, the greatest common divisor of a and b equals 8.

Example 8.1.15. Suppose that $n > 1$ is an integer. Then any common divisor of $n+1$ and $n-1$ is also a divisor of $n+1-(n-1) = 2$. Hence $\gcd(n+1, n-1) = 2$ if n is odd, and $\gcd(n+1, n-1) = 1$ if n is even.

Remark 8.1.16. If b divides a, then so does $-b$. For, if $a = q \cdot b$, then $a = (-q) \cdot (-b)$. In particular, any nonzero integer has positive divisors, so $\gcd(a,b) > 0$ if a or b is nonzero.

Since the divisors of a coincide with those of $|a|$, we have $\gcd(a,b) = \gcd(|a|, |b|)$.

If a and b are not both 0, their greatest common divisor exists. To see this, first note that the set of common divisors of a and b is certainly bounded above by the largest of $|a|$ and $|b|$ by Properties of Divisors 8.1.5. Since the set is nonempty (1 is in it), it must have a largest element.

For the sake of completeness, we define the greatest common divisor of 0 and 0 to be 0.

The greatest common divisor of more than two integers is defined analogously.

Just like studying common divisors of two integers, we can also consider common multiples of two (or more) integers.

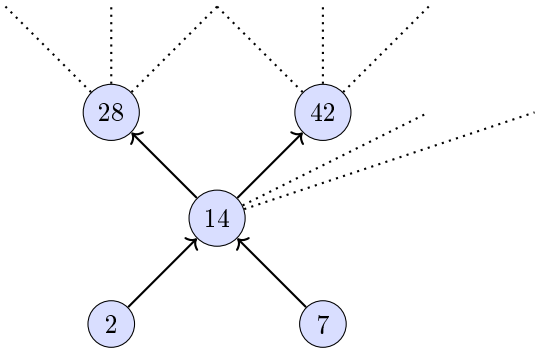


Figure 8.3: Some positive common multiples of 2 and 7.

Definition 8.1.17. Let a and b be nonzero integers.
- The integer c is a *common multiple* of a and b if c is a multiple of a and of b (that is, $a|c$ and $b|c$).
- The smallest positive common multiple of a and b is called the *least common multiple* of a and b.

We denote the least common multiple (lcm) of a and b by $\operatorname{lcm}(a,b)$.

Example 8.1.18. The first 5 positive multiples of $a = 13$ are 13, 26, 39, 52, and 65.
The first 13 multiples of $b = 5$ are 5, 10, 15, 20, 25, 30, 35, 40, 45, 50, 55, 60, and 65.
So, the only positive common multiple of $a = 13$ and $b = 5$ less than or equal to $a \cdot b$ is 65.
In particular, $\operatorname{lcm}(13,5) = 65$.

For any two nonzero integers a and b there exists a positive common multiple, namely $|a \cdot b|$. As a consequence, the least common multiple of a and b is well defined.

Of course, the least common multiple of more than two integers can be defined in a similar way.

The least common multiple and the greatest common divisor of two integers are closely related.

Theorem 8.1.19 — Relation between ggd and lcm. Let a and b be positive integers. Then $a \cdot b = \gcd(a,b) \cdot \operatorname{lcm}(a,b)$.

Proof. Our strategy is to apply division with remainder to $a \cdot b$ and $\operatorname{lcm}(a,b)$, and relate the quotient to $\gcd(a,b)$. Let q be the quotient and let r be the remainder of this division.

First we investigate the remainder r. We rewrite $a \cdot b = q \cdot \operatorname{lcm}(a,b) + r$ as $r = a \cdot b - q \cdot \operatorname{lcm}(a,b)$

Since both $a \cdot b$ and $\operatorname{lcm}(a,b)$ are divisible by a and b, we infer that the remainder r is also divisible by a and b. In other words, r is a common multiple of a and b. But $0 \leq r < \operatorname{lcm}(a,b)$ by the Division with Remainder Theorem 8.1.6, so $r = 0$. Consequently, $a \cdot b = q \cdot \operatorname{lcm}(a,b)$.

Next, we claim that q divides a and b. To see this, first let u be such that $\operatorname{lcm}(a,b) = u \cdot b$. Multiplying both sides by q gives $a \cdot b = q \cdot u \cdot b$. As b is nonzero, this equality can be simplified to $a = q \cdot u$, which proves the claim that q divides a. The proof that q divides b is entirely similar.

So q is a common divisor of a and b. In particular, q is less than or equal to $\gcd(a,b)$.

Finally, we show that q is also greater than or equal to $\gcd(a,b)$.

Since $\gcd(a,b)$ divides both a and b, $(a \cdot b)/\gcd(a,b)$ is also a common multiple of a and b. As $(a \cdot b)/q$ is the least common multiple of a and b, we conclude that q is greater than or equal to $\gcd(a,b)$. Hence q equals $\gcd(a,b)$, which proves the theorem as $a \cdot b = q \cdot \operatorname{lcm}(a,b)$.

□

The above theorem enables us to compute the lcm of two integers from the gcd and vice versa.

Example 8.1.20. For $a = 24$ and $b = 15$, we find $\gcd(a,b) = 3$, $\operatorname{lcm}(a,b) = 120$ and $a \cdot b = 360$. We see that $3 \cdot 120 = 360$.

Example 8.1.21. Suppose that $n > 1$ is an integer. Then, as we have seen in Example 8.1.15, $\gcd(n+1, n-1) = 2$ if n is odd, and $\gcd(n+1, n-1) = 1$ if n is even. So, $\operatorname{lcm}(n+1, n-1) = \frac{(n+1)\cdot(n-1)}{2}$ if n is odd, and $\operatorname{lcm}(n+1, n-1) = (n+1) \cdot (n-1)$ if n is even.

8.2 Euclid's algorithm

The greatest common divisor of two integers a and b can be determined by Euclid's Algorithm, one of the most important algorithms we will encounter. It is based on the observation that, if $a = q \cdot b + r$, then $\gcd(a,b)$ is equal to $\gcd(b,r)$, see Properties of Divisors 8.1.5, where $q = \operatorname{quot}(a,b)$ and $r = \operatorname{rem}(a,b)$.

For simplicity, we will assume the arguments of $\gcd$ to be positive. This does not really restrict us when we bear in mind that the arguments of $\gcd$ can be replaced by their absolutes in view of .

Figure 8.4: Euclid of Alexandria (about 325 BC-265 BC).

Algorithm 8.2.1 — Euclid's Algorithm.

- Input: two positive integers a and b.
- Output: the gcd of a and b.

GCD $:=$ **procedure**(a,b)
local variables
  c
while $b > 0$ **do**
  $c := a$, $a := b$, $b := \text{rem}(c,b)$
return
  a

Proof. We use three properties of the greatest common divisor of non negative integers that follow from Properties of Divisors 8.1.5:

$$\gcd(a,b) = \gcd(b,a)$$

$$\gcd(a,b) = \gcd(a,b-k\cdot a)$$

(for every integer k), and

$$\gcd(a,0) = a$$

Correctness.

If a' and b' denote the values of a and b, respectively, at the end of the body of the while loop, then $a' = b'$ and $b' = a - q\cdot b$, where q is the quotient of division with remainder of a by b. By the first two of the three properties, the greatest common divisor is an invariant, that is, $\gcd(a',b') = \gcd(a,b)$. As a consequence, the value of $\gcd(a',b')$ remains unaffected upon changing the arguments. At the end of the while loop, $b' = 0$, so the third property gives that the output a is equal to the initial value of $\gcd(a',b')$.

Termination.

The variable b decreases with each step. (By a step we mean a percursion of the full body of the while loop.) After at most b steps we arrive at the point where b equals 0. Then the algorithm ends.

□

Remark 8.2.2. The while loop in Euclid's Algorithm can be described rather conveniently in matrix form. Let q be the quotient of division of a by b. Then the vector $(a,b)^T$ is replaced by $(b,a-q\cdot b)^T$. We can also write this as the product of the matrix M and the vector $(a,b)^T$, where $M = \begin{pmatrix} 0 & 1 \\ 1 & -q \end{pmatrix}$

Example 8.2.3. Euclid's Algorithm computes the greatest common divisor of two positive integers. In this example, you can see all the steps of the algorithm.

We compute the greatest common divisor of $a = 123$ and $b = 13$. In each step of the algorithm we replace (simultaneously) a by b, and b by the remainder of a divided by b. The algorithm starts with $a = 123$ and $b = 13$.

Each row of the following table represents a step in the algorithm.

Step n	a	b
0	123	13
1	13	6
2	6	1
3	1	0

Since the value of the second parameter has become 0, the algorithm stops, and we can conclude that the greatest common divisor of $a = 123$ and $b = 13$ equals 1.

Example 8.2.4. In this example, we compute the greatest common divisor of $a = 56$ and $b = 36$. In the following table you find the values of a and b in each step of Euclid's Algorithm.

Step n	a	b
0	56	36
1	36	20
2	20	16
3	16	4
4	4	0

Since the value of the second parameter has become 0, the algorithm stops. We conclude that the greatest common divisor of $a = 56$ and $b = 36$ equals 4.

There is also an extended version of Euclid's Algorithm 8.2.1, which determines, apart from $\gcd(a,b)$, integers x and y such that $a\cdot x + b\cdot y = \gcd(a,b)$. We say that $\gcd(a,b)$ can be expressed as an *integral linear combination* of a and b. To find such an integral linear combination for $\gcd(a,b)$, we record at each step of Euclid's Algorithm 8.2.1 how to express the intermediate results in the input integers.

Algorithm 8.2.5 — Extended Euclidean Algorithm.

- Input: positive integers a and b.
- Output: list of integers $[g,x,y]$ with $g = \gcd(a,b)$, and $g = x\cdot a + y\cdot b$.

ExtendedGCD := **procedure**(a,b)
local variables
  $a_1,\ b_1$
  $u := 0\ ,\ v := 1\ ,\ x := 1\ ,\ y := 0$
  $u_1,\ v_1,\ x_1,\ y_1$
while $b > 0$ **do**
  $a_1 := a\ ,\ b_1 := b$
  $u_1 := u\ ,\ v_1 := v\ ,\ x_1 := x\ ,\ y_1 := y$
  $a := b_1\ ,\ b := \mathrm{rem}(a_1,b_1)$
  $x := u_1\ ,\ y := v_1$
  $u := x_1 - \mathrm{quot}(a_1,b_1)\cdot u_1\ ,\ y := y_1 - \mathrm{quot}(a_1,b_1)\cdot v_1$
return
  $[a,x,y]$

Proof.

Correctness.

Find the gcd of a and b using Euclid's Algorithm 8.2.1. In each step of the while-loop of the algorithm the two input values are changed into two new values. These values can be defined recursively by $a_0 = a$ and $b_0 = b$ and for $n \geq 1$ by $a_{n+1} = b_n$ and $b_{n+1} = a_n - \mathrm{quot}(a_n,b_n)\cdot b_n$.

We prove by induction on n that every a_n and b_n can be written as a linear combination of a and b with integer coefficients.

For $n = 0$ this is trivial.

Suppose for some n we have $a_n = x\cdot a + y\cdot b$ and $b_n = u\cdot a + v\cdot b$ for certain integers x, y, u, and v. Then after the next step we obtain $a_{n+1} = b_n$ which equals $u\cdot a + v\cdot b$. Thus also a_{n+1} is a linear combination of a and b with integer coefficients.

Furthermore we have $b_{n+1} = a_n - q\cdot b_n$. So, $b_{n+1} = x\cdot a + y\cdot b - q\cdot(u\cdot a + v\cdot b) = (x - q\cdot u)\cdot a + (y - q\cdot v)\cdot b$, where $q = \mathrm{quot}(a_n,b_n)$. In particular, also b_{n+1} is a linear combination of a and b with integer coefficients.

By induction we have proven for all n that a_n and b_n can be written as a linear combination of a and b with integer coefficients.

Since Euclid's algorithm will eventually return the gcd of a and b as a_n for some n, the extended Euclidean algorithm will output integers x and y with $\gcd(a,b) = x\cdot a + y\cdot b$.

Termination.

As Euclid's Algorithm 8.2.1 terminates, so does the extended Euclidean algorithm.

□

Remark 8.2.6. Integers x and y satisfying $x\cdot a + y\cdot b = \gcd(a,b)$ are not unique, since, for any integer t, we have $(x + t\cdot b)\cdot a + (y - t\cdot a)\cdot b = \gcd(a,b)$.

Remark 8.2.7. In terms of matrices, the algorithm can be written somewhat more succinctly. The idea is that in each step the values of the variables are such that the matrix $M = \begin{pmatrix} x & y \\ u & v \end{pmatrix}$ applied to the column vector $\begin{pmatrix} a \\ b \end{pmatrix}$ (the input values) gives the updated values of a and b.

At the end, we obtain $\begin{pmatrix} \gcd(a,b) \\ 0 \end{pmatrix} = M\cdot\begin{pmatrix} a \\ b \end{pmatrix}$, with the appropriate matrix M. Comparing the first and second entries on both sides of this equality gives $\gcd(a,b) = x\cdot a + y\cdot b$ and $0 = u\cdot a + v\cdot b$, where x, y, u, and v are the suitably updated entries of the matrix M.

Example 8.2.8. The extended Euclidean algorithm computes the greatest common divisor of two positive integers and expresses it as an integral linear combination of the input. In this example, you can see all the steps of the algorithm.

We compute the greatest common divisor of $a = 123$ and $b = 13$ following the extended Euclidean algorithm.

Each row of the following table represents a step in the algorithm.

Step n	a	b	x	y	u	v
0	123	13	1	0	0	1
0	13	6	0	1	1	-9
0	6	1	1	-9	-2	19
0	1	0	-2	19	13	-123

We conclude that the greatest common divisor of $a = 123$ and $b = 13$ equals 1. From the same table we infer that 1 can be written as $1 = (-2) \cdot 123 + 19 \cdot 13$.

The Extended Euclidean Algorithm 8.2.5 provides us with the following characterization of the gcd.

Theorem 8.2.9 — Characterization of the gcd. The following three statements concerning the positive integers a, b, and d are equivalent.

(a) $\gcd(a,b) = d$.

(b) The integer d is a positive common divisor of a and b such that any common divisor of a and b is a divisor of d.

(c) d is the least positive integer that can be expressed as $x \cdot a + y \cdot b$ with integers x and y.

Proof.

The second statement is equivalent to the first.

To show that the first assertion implies the second, let $d = \gcd(a,b)$. Then d is a common divisor of a and b. By the Extended Euclidean Algorithm 8.2.5 we have $d = x \cdot a + y \cdot b$ for some integers x and y. If c is any common divisor of a and b, then it also divides $x \cdot a + y \cdot b = d$, see Properties of Divisors 8.1.5. This proves that the first assertion implies the second.

As for the other way around, suppose that d is as in the second statement. Since $\gcd(a,b)$ is a common divisor of a and b it must divide d. On the other hand d cannot be greater than $\gcd(a,b)$. Hence d and $\gcd(a,b)$ must be equal. This proves that the second statement implies the first.

The third statement is equivalent to the first.

Let $d = \gcd(a,b)$ and let e be the least positive integer that can be expressed as $x \cdot a + y \cdot b$ with integers x and y. We show that $d = e$. Since d is a common divisor of a and b the equality $e = x \cdot a + y \cdot b$ implies that d divides e (see Properties of Divisors 8.1.5). So $d \leq e$. Moreover, as a result of the Extended Euclidean Algorithm 8.2.5, d itself can also be written as an integral linear combination of a and b. So $d \geq e$ by the defining property of e. Hence e must be equal to d. This proves the equivalence.

Conclusion.

Since both the second and the third statement of the theorem are equivalent to the first, all three statements are equivalent. This finishes the proof of the theorem.

□

These different characterizations of the gcd, in particular the possibility to express the gcd of two integers a and b as an integral linear combination of a and b, will turn out to be very useful in various applications.

The following corollary to the Characterization of the gcd 8.2.9 deserves to be stated separately.

Corollary 8.2.10 — Characterization of Relatively Prime Numbers. Integers a and b are relatively prime if and only if there exist integers x and y such that $x \cdot a + y \cdot b = 1$.

Proof. Apply the previous Characterization of the gcd 8.2.9 with $d = 1$.

□

Example 8.2.11. For all natural numbers m, n, and k with $m < n$, the integers k^m and $k^n - 1$ are relatively prime. For, $k^{n-m} \cdot k^m - 1 \cdot (k^n - 1) = 1$.

Example 8.2.12. Suppose that n is a positive integer. Then the greatest common divisor of $n^2 + n + 1$ and n^2 equals 1. Indeed, this follows from the equality $n \cdot n^2 - (n-1) \cdot \left(n^2 + n + 1\right) = 1$

A first application of the Characterization of the gcd 8.2.9 is the following useful result for deducing divisibility of one integer by another.

Proposition 8.2.13. Let a, b, and c be integers. If a and b are relatively prime, then $a|b \cdot c$ implies $a|c$.

Proof. Since the gcd of a and b equals 1, Characterization of Relatively Prime Numbers 8.2.10 implies that there exist integers x and y such that $x \cdot a + y \cdot b = 1$. Multiplying both sides of this equation by c yields that $x \cdot a \cdot c + y \cdot b \cdot c = c$. Since $a|x \cdot a \cdot c$ and $a|b \cdot c$ (and hence also $a|y \cdot b \cdot c$) we conclude that $a|\left((x \cdot a \cdot c) + (y \cdot b \cdot c)\right) = c$, which proves the proposition.

□

Example 8.2.14. The above proposition is a generalization of the following well known statement: The product of two integers is even if and only if at least one of the two integers is even.

8.3 Linear Diophantine equations

Let a, b, and c be integers. A linear equation in the unknowns x and y is an equation of the form $x \cdot a + y \cdot b = c$. If the unknowns x and y are integers, such equations are known as *linear Diophantine equations*.

We will use the Extended Euclidean Algorithm 8.2.5 to derive an algorithm for finding all integer pairs x, y that satisfy the linear Diophantine equation $x \cdot a + y \cdot b = c$, for given integers a, b, and c.

If we interpret the equation over $\mathbb{Q}$ or $\mathbb{R}$ and if we assume that b is not equal to 0, then the solutions are all of the form $(x, y) = (x, (c - x \cdot a)/b)$. However, not all of these solutions are integral, and we have to find out which ones are.

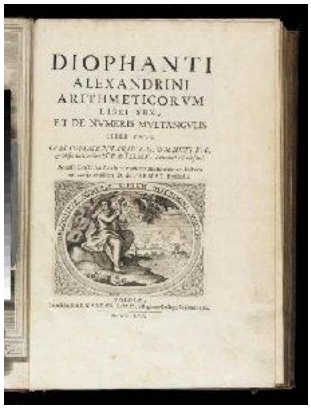


Figure 8.5: Diophantus' book on Arithmetic. Diophantus' work inspired Fermat to write in the margin of this book his famous last theorem: for $n > 2$ there are no nonzero integers x, y and z, such that $x^n + y^n = z^n$.

We first discuss a special case, the *homogeneous equation*, i.e., the case where c equals 0.

Lemma 8.3.1. If $x\cdot a+y\cdot b=0$ and $\gcd(a,b)=1$, then there exists an integer n such that $x=-n\cdot b$ and $y=n\cdot a$.

Proof. Suppose that $x\cdot a+y\cdot b=0$ and that $\gcd(a,b)=1$. From $x\cdot a=-b\cdot y$ it follows that $a|b\cdot y$. Since $\gcd(a,b)=1$, we find $a|y$, see . 8.2.13 This means that there exists an integer n such that $a\cdot n=y$. Substitution of y in the original equation gives $x=-n\cdot b$. This proves the lemma.

□

From Lemma on Diophantine Equation Solving 8.3.1 we conclude the following.

Lemma 8.3.2 — Homogeneous Diophantine Equation Solving. Suppose that a and b are integers which are not both equal to 0. Then the integer solutions to the equation $x\cdot a+y\cdot b=0$ are given by $x=\frac{-n\cdot b}{d}$ and $y=\frac{n\cdot a}{d}$, where $d=\gcd(a,b)$ and $n\in\mathbb{Z}$.

Proof. First we note that the integers $\frac{a}{d}$ and $\frac{b}{d}$ are relatively prime: Use the Extended Euclidean Algorithm 8.2.5 to find a relation of the form $u\cdot a+v\cdot b=d$, divide both sides by d, and, finally, apply the Characterization of Relatively Prime Numbers 8.2.10.

Next, we turn to the equation $x\cdot a+y\cdot b=0$. After dividing both sides of the equation $x\cdot a+y\cdot b=0$ by d, we arrive at the setting of Lemma on Diophantine Equation Solving 8.3.1. Our equation then reads $x\cdot\frac{a}{d}+y\cdot\frac{b}{d}=0$, where $\gcd\left(\frac{a}{d},\frac{b}{d}\right)=1$. Lemma on Diophantine Equation Solving 8.3.1 now shows that there exists an integer n such that $x=-n\cdot\frac{b}{d}$ and $y=n\cdot\frac{a}{d}$, as required.

□

Example 8.3.3. To find the integral solutions to the equation $24\cdot x+15\cdot y=0$ we first compute the gcd of 24 and 15. Using for example the Euclid's Algorithm 8.2.1 as in Example 8.2.3, we find $\gcd(24,15)=3$. By Homogeneous Diophantine Equation Solving 8.3.2, $x=\frac{15\cdot n}{3}=5\cdot n$ and $y=-(\frac{24\cdot n}{3})=(-8)\cdot n$ with $n\in\mathbb{Z}$.

We are now ready to solve general linear Diophantine equations of the form $x\cdot a+y\cdot b=c$. We do this in the form of an algorithm.

Algorithm 8.3.4 — Linear Diophantine Equation Solving Algorithm.

- Input: integers a, b, and c, with a and b not both equal to 0 .
- Output: set of all integer solutions (x,y) to the Diophantine equation $x\cdot a+y\cdot b=c$.

SolveDiophantine := **procedure**(a,b,c)
local variables
  $e:=\text{Extgcd}(a,b)$
  $g:=e[1]$
  $x_0:=e[2]$
  $y_0:=e[3]$
if $g|c$
  then
    return
      $\left\{\left(\frac{x_0\cdot c-n\cdot b}{g},\frac{y_0\cdot c+n\cdot a}{g}\right)\middle| n\in\mathbb{Z}\right\}$
  else
    return
      $\varnothing$

Proof.

Termination.

As there are no loops in the algorithm, this is obvious....provided we interpret the returned output set as finite data (instead of returning elements of the set one by one).

Correctness.

By definition of the extended gcd algorithm, the value of the variable g is equal to $\gcd(a,b)$.

If there are solutions to the equation $x\cdot a+y\cdot b=c$, then g divides c. Indeed, for all integer solutions x and y, the integer g divides $x\cdot a+y\cdot b$, which is equal to c.

So, suppose that g divides c. If $x_0\cdot a+y_0\cdot b=g$, then $\frac{c}{g}\cdot x_0\cdot a+\frac{c}{g}\cdot y_0\cdot b=c$. So $x_1=\frac{c}{g}\cdot x_0$ and $y_1=\frac{c}{g}\cdot y_0$ form a solution to the equation.

If (x_2,y_2) is another solution to the equation $a\cdot x+y\cdot b=c$, then the differences x_2-x_1 and y_2-y_1 form a solution to the so-called homogeneous equation $a\cdot x+y\cdot b=0$. Hence all solutions of $a\cdot x+y\cdot b=c$, if there are any, are of the form (x_1,y_1) plus a single solution to the homogeneous equation $a\cdot x+y\cdot b=0$.

From Homogeneous Diophantine Equation Solving 8.3.2 we conclude that every solution is of the form $x=\frac{x_0\cdot c-n\cdot b}{g}$ and $y=\frac{y_0\cdot c-n\cdot a}{g}$, which proves correctness of the algorithm.

□

Note the structure of the solutions in the Linear Diophantine Equation Solving Algorithm 8.3.4:

$$\left(\frac{x_0\cdot c}{\gcd(a,b)},\frac{y_0\cdot c}{\gcd(a,b)}\right)$$

is one particular solution to the equation $x\cdot a+y\cdot b=c$, and all other solutions are obtained by adding all solutions (x',y') of the homogeneous equation $x'\cdot a+y'\cdot b=0$ to it.

Example 8.3.5. Let a, b, and c be integers. We determine the integral solutions to the equation $24\cdot x+15\cdot y=63$

Following the Linear Diophantine Equation Solving Algorithm 8.3.4, we use the Extended Euclidean Algorithm 8.2.5 to compute the gcd of 24 and 15 and express it as a linear combination of these numbers. We find $\gcd(24,15)=3=2\cdot 24-3\cdot 15$. As 3 divides 63, there are solutions.

By the Linear Diophantine Equation Solving Algorithm 8.3.4 the general solution to the equation $24\cdot x+15\cdot y=63$ is now $x=\frac{2\cdot 63-n\cdot 15}{3}$ and $y=\frac{(-3)\cdot 63+n\cdot 24}{3}$, where n runs through $\mathbb{Z}$.

This solution simplifies to $x=42-5\cdot n$ and $y=-63+8\cdot n$, with n running through $\mathbb{Z}$, the sum of a particular solution and any solution of the homogeneous equation.

Of course, the particular solution $x=42$ and $y=-63$ could have been found by multiplying both sides of the equation $3=2\cdot 24-3\cdot 15$ by 21.

8.4 Prime numbers

In this section we discuss prime numbers, the building blocks for the multiplicative structure of the integers. We start with a definition of primes.

Definition 8.4.1. A *prime* is an integer p greater than 1 that has no positive divisors other than 1 and p itself.

Example 8.4.2. The integer 17 is prime.

The integer 51 is not prime, since it is divisible by 3.

Example 8.4.3. Suppose that n is a positive integer such that 2^n-1 is prime. Then n itself is prime.

Indeed, if n is the product of two integers a and b (both at least 2), then $2^n-1=(2^a)^b-1$, which is divisible by 2^a-1.

The smallest prime number is 2 (and not 1). The first five primes are $2,3,5,7$, and 11, but there are many more.

Theorem 8.4.4 — Euclid's Theorem. There are infinitely many primes.

Proof. Suppose that there are only finitely many primes, say $p_1, \ldots, p_n$, and no others. We will derive a contradiction by showing that there must exist at least one other prime, distinct from all the p_i.

Consider the integer $m = 1 + \prod_{i=1}^{n} p_i$ Then $m > 1$. Moreover, for each $i \in \{1, \ldots, n\}$, the integer m is clearly not divisible by p_i. Hence, the smallest divisor p of m greater than 1 is distinct from $p_1, \ldots, p_n$.

We claim that p is prime. Indeed, any positive divisor d of p is also a divisor of m. So, since p is the smallest divisor of m greater than 1, we find d to be equal to either 1 or p, which proves our claim. So, we have found a prime p distinct from all the primes $p_1, \ldots, p_n$. This contradicts the assumption that $p_1, \ldots, p_n$ are the only primes.

□

Example 8.4.5. The primes less than or equal to 1013 are given in the table below.

2	3	5	7	11	13	17	19	23	29
31	37	41	43	47	53	59	61	67	71
73	79	83	89	97	101	103	107	109	113
127	131	137	139	149	151	157	163	167	173
179	181	191	193	197	199	211	223	227	229
233	239	241	251	257	263	269	271	277	281
283	293	307	311	313	317	331	337	347	349
353	359	367	373	379	383	389	397	401	409
419	421	431	433	439	443	449	457	461	463
467	479	487	491	499	503	509	521	523	541
547	557	563	569	571	577	587	593	599	601
607	613	617	619	631	641	643	647	653	659
661	673	677	683	691	701	709	719	727	733
739	743	751	757	761	769	773	787	797	809
811	821	823	827	829	839	853	857	859	863
877	881	883	887	907	911	919	929	937	941
947	953	967	971	977	983	991	997	1009	1013

Table 8.1: The primes less than or equal to 1013.

Example 8.4.6. Although there are infinitely many prime numbers, see Euclid's Theorem 8.4.4, the gaps between two consecutive prime numbers can be arbitrarily large.

For example, none of the hundred consecutive integers between $101! + 2$ and $101! + 101$ is prime. A nontrivial divisor (i.e., a divisor greater than 1 and less than the number itself) of $101! + n$, where $n \in \{2, \ldots, 101\}$, is n.

Example 8.4.7. Suppose that L is a finite list of primes, for example $[2, 3, 5, 7, 11, 13, 17]$. Put $m = 1 + \prod_{i \in L} i$. According to the proof of the theorem, a new prime occurs among the divisors of m, which equals 510511.

The smallest nontrivial positive divisor of 510511 equals 19, a prime not in L.

Remark 8.4.8. Although there are infinitely many prime numbers, we actually know only a finite number of them. The largest known prime (April 2023) is $2^{82,589,933} - 1$. In its decimal representation this number is 24,862,048 digits long. It was found in 2018 by Patrick Laroche, a member of a collaborative effort to find primes known as GIMPS. The GIMPS program searches for so-called Mersenne primes.

Mersenne primes are primes of the form $2^n - 1$. The prime number $2^{30402457} - 1$ is the 43rd known Mersenne prime.

Prime numbers of the form $2^n - 1$ are called Mersenne primes, since they were studied first by Marin Mersenne (1588-1648).

By Example , 8.4.3 the integer $2^n - 1$ can be prime only when n itself is a prime.

Figure 8.6: Marin Mersenne (1588-1648).

A few examples of Mersenne primes are $3 = 2^2 - 1$, $7 = 2^3 - 1$, $31 = 2^5 - 1$ and $127 = 2^7 - 1$. Mersenne found that $2^{11} - 1$ is not a prime. Can you find its prime divisors?

Eratosthenes' sieve is an algorithm for making the list of all primes less than or equal to some integer n.

Figure 8.7: Eratosthenes (about 276 BC-194 BC).

If M is a list of integers and m is an integer, we shall write $M \cup [m]$ for the list obtained by appending m to M.

Algorithm 8.4.9 — Eratosthenes' Sieve.

- Input: a positive integer n.
- Output: the list of primes less than or equal to n.

Sieve := **procedure**(n)
local variables
  $L := \{2, \ldots, n\}$
  $M :=$ list2.nil
  m
while $L \neq$ list2.nil **do**
  $m := L[1]$, $L := L \backslash m \cdot \{1, \ldots, n\}$, $M := M \cup [m]$
return
  M

Proof.

Termination.

At each step (that is, percursion of the body of the while loop), the length of the list L strictly decreases, so the algorithm will stop after running the while loop at most the length of L times.

Correctness.

By construction, the output list M consists of all numbers in $\{2,\ldots,n\}$ that are no multiple of a strictly smaller number. These are precisely the primes less than or equal to n.

□

Example 8.4.10. We will make a list of all the primes in the interval from 2 to $n = 20$. We use Eratosthenes' Sieve 8.4.9. We start with the complete list of integers from 2 to $n = 20$. See the first row of the table below. Next, in each consecutive row, we remove the proper multiples of the first element for which this has not yet been done.

2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
2	3		5		7		9		11		13		15		17		19	
	3		5		7				11		13				17		19	

Table 8.2: Eratosthenes' sieve

We have removed multiples of 2, 3 and 5, respectively.

The numbers in the last row of the table are all prime. They form the set of all primes less than or equal to 20.

Remark 8.4.11. The number of runs of the while loop in Eratosthenes' Sieve 8.4.9 equals the number of primes in the interval $\{1,\ldots,n\}$. In each run, one has to check less than n integers. So the algorithm takes certainly less than n^2 operations. However, the memory use for the algorithm is quite big, as the whole range of numbers from 2 to n has to be in memory at the start of the algorithm.

Remark 8.4.12. Eratosthenes' Sieve 8.4.9 can also be used as a prime test. However, to avoid problems of big memory use as indicated in Remark on the Running time of Eratosthenes' sieve 8.4.11, one can apply the following straightforward algorithm for verifying if the integer n is prime. Let an integer variable m run from 2 up to $\sqrt{n}$ and check whether n is divisible by m. If for some m we find that it divides n, then we stop and decide that n is composite, otherwise we decide that n is prime.

Using Eratosthenes' sieve we can find all the primes in the interval $\{1,\ldots,n\}$. The number of such primes can be approximated as follows.

Theorem 8.4.13 — Prime Number Theorem. Let $\text{primes}(n)$ be the number of primes in the interval $\{1,\ldots,n\}$. Then we have $\lim_{n\to\infty^-}\left(\frac{\text{primes}(n)}{\frac{n}{\ln(n)}}\right) = 1$

The Prime Number Theorem is often stated as $\text{primes}(n) \approx \frac{n}{\ln(n)}$ when n tends to infinity. The Prime Number Theorem was proved by Hadamard and de la Vallee Poussin in 1896.

Figure 8.8: Jacques Hadamard (1865-1963).

Example 8.4.14. To find a large prime, for example a 100-digit number, we can use a random technique. Indeed, if we pick a 100-digit number at random, then by the Prime Number Theorem 8.4.13, the probability of having picked a prime is roughly $\frac{1}{\ln(10^{100})}$. Hence we expect to find a prime after at most $\ln(10^{100}) < 300$ picks.

Using a fast prime test (which does exist!), this can be easily done by a computer.

Example 8.4.15 — Secure internet traffic. The software company 'Frames' has finally produced a good operating system. The company wants to produce DVDs with this operating system at plants in the US, Europe, and Australia. All plants have a master copy of the operating system, but before starting the production, they first want to make sure that all these copies are the same.

For security reasons, the company does not want to compare the systems bit by bit over the internet. Indeed, competing companies could get secret information or hackers could corrupt it. So, the president of 'Frames' has asked the mathematics department to come up with a quick and very secure way of checking. The mathematicians' response is the following.

The procedure. All plants have high quality equipment at their disposal. First a random prime number p is chosen in the interval between 1 and some integer a which can be represented in the binary system with n bits. So a is approximately equal to 2^n. Next, each plant transforms the bit-string of the operating system, which has approximately length b say, into a number x, and then computes the remainder $r = \text{rem}(x, p)$. Finally the three plants compare the remainders thus obtained. This can be done easily, as these remainders are just numbers between 0 and p. If they all find the same remainder, they decide that their copies are the same.

The security. Why does this test yield a secure way of checking whether all three copies of the operating system are the same? Suppose that one plant's system is a bit-string representing the number x, while another plant's system represents the number y. If the bit-strings have length (approximately) b, then these numbers x and y have size at most 2^b. Of course, $x = y$ implies $\text{rem}(x, p) = \text{rem}(y, p)$. This means that the conclusion $x \neq y$ is justified if $\text{rem}(x, p) \neq \text{rem}(y, p)$. So suppose that $\text{rem}(x, p) = \text{rem}(y, p)$. How large is the probability of an error? How large is the probability that $x \neq y$?

In this case $x - y$ must be a nonzero multiple of p. So the probability P of a wrong conclusion is at most the quotient of the number of prime divisors of $x - y$ by the number of primes less than 2^n.

First we analyze the numerator of this quotient. If k is the number of primes that divide the number $z = x - y$, then $z \geq 2^k$. But that implies that k is at most b.

Now the denominator. According to the Prime Number Theorem the number of primes less than 2^n is approximately $2^n / \ln(2^n)$. So, a good estimate for the denominator is $2^n / n$.

Combining the above, we find that P, the probability of declaring x and y to be the same while they are not, is at most $\frac{b \cdot n}{2^n}$.

A concrete example. Suppose that the operating system fits on a single DVD of 5 Gigabyte. Then the number b of bits on the DVD equals $5 \cdot 2^{10} \cdot 2^{10} \cdot 2^{10} \cdot 2^3$. So, if we pick the prime p at random between 1 and 2^{200}, then the probability of declaring x and y to be the same while they are not, is less than $\frac{5 \cdot 2^{33} \cdot 200}{2^{200}}$, which is less than 2^{-153}.

In a similar way one can analyze the probability of declaring x and y to be not the same, while they are equal.

The next theorem gives a characterization of primes.

Theorem 8.4.16 — Prime Characterization. Let $p > 1$. Then p is a prime if and only if, for all integers b and c, the condition $p | b \cdot c$ implies that $p | b$ or $p | c$.

Proof.

If.

Proof. Suppose that p is prime. Assume that $p | b \cdot c$ for some integers b and c. If $p | b$ we are done. If p is not a divisor of b, then p and b have no common divisors greater than 1 and we can apply Result on the divisor of a product 8.2.13 to find that p divides c.

□

Only if.

Proof. If p is not prime, then $p = b \cdot c$ for two integers b and c that are greater than 1 and smaller than p. Then p divides the product $b \cdot c$, but divides neither b nor c (as b and c are smaller than p). We conclude that if, for all integers b and c the condition $p|b \cdot c$ implies that $p|b$ or $p|c$, then p is a prime.

□

□

Example 8.4.17. Suppose $a = b \cdot c$, where b and c are integers. The following fact is well known. If a is even, then so is at least one of b or c. It is one implication in the special case $p = 2$ of the theorem.

Prime Characterization 8.4.16 has the following useful corollary.

Corollary 8.4.18. If p is a prime and $b_1, \ldots, b_s$ are integers such that $p|\prod_{i=1}^{s} b_i$, then there is an index $i \in \{1, \ldots, s\}$ such that $p|b_i$.

Proof. Let p be a prime and $b_1, \ldots, b_s$ integers providing a counterexample to the corollary with s minimal. Hence $p|\prod_{i=1}^{s} b_i$, but p does not divide b_i for each index i.

Since p does not divides b_s, the Prime Characterization 8.4.16 implies that p divides $\prod_{i=1}^{s-1} b_i$. By the minimality of s, the integers $b_1, \ldots, b_{s-1}$ do not provide a counterexample to the statement of the corollary. Thus, there is an index i less than s such that p divides b_i. This contradicts our assumptions. Hence, no counterexamples exist and we have proven the corollary.

□

Example 8.4.19. Let p be a prime, then p does not divide a product of integers, none of which is divisible by p. For example, if i is a positive integer less than p, then p does not divide $p - i! \cdot i!$.

8.5 Factorization

The prime numbers are the building blocks for the multiplicative decomposition of integers. We will now see how integers are built up out of primes.

Theorem 8.5.1 — Unique Factorization. Every positive integer $a > 1$ can be written as the product of finitely many primes: $a = \prod_{i=1}^{s} p_i$ where s is a positive integer and each p_i is a prime. Up to the order of the factors, this factorization is unique.

Proof. The proof is divided into two steps. Each step is proved by induction on a.

Every integer a is a product of primes.

The case $a = 2$ is trivial. So suppose that a is at least 3 and that all positive integers less than a can be expressed as a product of primes. If a itself is a prime, then we are done. If a is not a prime, then it has a divisor b such that $1 < b$ and $b < a$. According to the induction hypothesis, both b and a/b can be written as a product of primes. Explicitly, $b = \prod_{i=1}^{t} p_i$ and $\frac{a}{b} = \prod_{i=1}^{r} q_i$ where t and r are positive integers and all p_i and q_i are primes. But then, as $a = b \cdot (a/b)$, we can write a as the product $a = \prod_{i=1}^{t} p_i \cdot \prod_{i=1}^{r} q_i$. Hence, a is a product of primes.

The factorization of an integer a is unique (up to order).

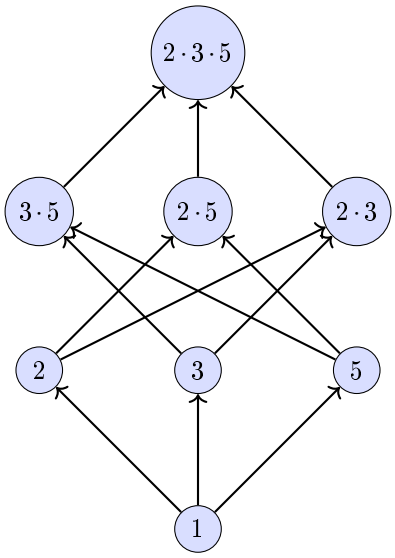


Figure 8.9: Building integers from their prime divisors.

Again the case $a = 2$ is easy. Suppose that $a > 2$, and also suppose that uniqueness of the factorization into primes has been proven for the integers less than a.

If $a = \prod_{i=1}^{t} p_i$ and $a = \prod_{i=1}^{r} q_i$ are two ways of expressing a as a product of primes, then it follows that p_1 divides a. But then p_1 also divides $\prod_{i=1}^{r} q_i$.

Using 8.4.18 we conclude that there exists an index i in the set $\{1, ..., r\}$ such that $p_1 | q_i$. But then, as p_1 and q_i are prime, we have $p_1 = q_i$. Without loss of generality we can assume i to be 1, so $p_1 = q_1$.

Now apply the induction hypothesis to the integer a/p_1 with the two expressions as products of primes $\frac{a}{p_1} = \prod_{i=2}^{t} p_i$ and $\frac{a}{p_1} = \prod_{i=2}^{r} q_i$.

These factorizations of a/p_1 are the same (up to the order of the factors) and therefore the two factorization of a are also the same.

□

Example 8.5.2. Factoring a number into its prime factors is hard! Up to now (2023), the best factorization algorithms can factor numbers consisting of about 200 digits. Factorization of much larger numbers is exceptional. For example, there are numbers with more than 250 digits that have been factorized. One of the more famous examples is the number called RSA-129. In a newspaper article of April, 1994, the following factorization record by A.K. Lenstra, et al. was announced. RSA-129:

$$
\begin{gathered}
114381625757888867669235779976146612010218296721242362562561842 9 \\
357069352457338978305971235639587050589890751475992900268795435 41 \\
= \\
349052951084765094914784961990389813341776463849338784399082057 7 \\
\times \\
327691329932667095499619881908344614131776429679929425397982885 33
\end{gathered}
$$

It is not difficult to check that the product of these two factors is indeed the large number: any computer system that can work with these large numbers will confirm it. But it is very hard (indeed many thought it to be unfeasible) to find the factors given the product.

As an indication of how difficult this is, you should try to calculate how many years it would cost to find the above factorization using the obvious algorithm of trying all integers less than the number to be factored.

You may assume that the multiplication of two numbers of 130 digits takes about $1/100000$-th of a second. There remains the problem of checking that these two numbers are prime. By means of Eratosthenes' Sieve , 8.4.9 this would take a very long time. However there exist primality tests that can check if a 200 digit number is prime in a reasonable amount of time. In 2002, Agrawal, Kayal, and Saxena came up with an algorithm that, for input a prime number p, gives a proof of primality in time a polynomial function of the input length, the logarithm of p.

Example 8.5.3. The prime factorizations of the integers between 2 and 20 are

2	2^1
3	3^1
4	2^2
5	5^1
6	$2^1 \cdot 3^1$
7	7^1
8	2^3
9	3^2
10	$2^1 \cdot 5^1$
11	11^1
12	$2^2 \cdot 3^1$
13	13^1
14	$2^1 \cdot 7^1$
15	$3^1 \cdot 5^1$
16	2^4
17	17^1
18	$2^1 \cdot 3^2$
19	19^1
20	$2^2 \cdot 5^1$

Remark 8.5.4. If a is a square, then $\mathrm{ord}_p(a)$ is even for each prime p. Using this observation it is not difficult to prove that the square root of 2 is not *rational*, i.e., it is not in $\mathbb{Q}$. This means that there are no integers a and b with $b \neq 0$ such that $\left(\frac{a}{b}\right)^2 = 2$. For, if such a and b exist, then $2 \cdot b^2 = a^2$ and so $\mathrm{ord}_2(2 \cdot b^2) = \mathrm{ord}_2(a^2)$. But $\mathrm{ord}_2(2 \cdot b^2)$ is odd and $\mathrm{ord}_2(a^2)$ is even, a contradiction. Therefore, the assumption that a and b with $\left(\frac{a}{b}\right)^2 = 2$ exist is false.

The same method implies that any n-th root of a prime number is not rational. Indeed, suppose q is a prime and n is at least 2. If a and b are two integers with $\frac{a}{b} = q^{1/n}$, then $\left(\frac{a}{b}\right)^n = q$. So $q \cdot b^n = a^n$ and hence $\mathrm{ord}_q(q \cdot b^n) = \mathrm{ord}_q(a^n)$. But $\mathrm{ord}_q(q \cdot b^n)$ equals $1 + n \cdot \mathrm{ord}_q(b)$, a multiple of n plus 1, while $\mathrm{ord}_q(a^n)$ equals $n \cdot \mathrm{ord}_q(a)$, a multiple of n. This is a contradiction.

Remark 8.5.5. There also exist arithmetic systems in which uniqueness of factorizations is not guaranteed. For example, in the system R of numbers of the form $a + b \cdot \sqrt{-5}$ with $a, b \in \mathbb{Z}$ we can express 6 in two essentially different ways: $6 = 3 \cdot 2 = \left(1 + \sqrt{-5}\right) \cdot \left(1 - \sqrt{-5}\right)$. The system R is an example of a ring, an algebraic structure with properties similar to those of $\mathbb{Z}$, $\mathbb{Q}$, or $\mathbb{R}$.

For a non-zero integer a, we denote the number of times that the prime p occurs in its factorization by $\mathrm{ord}_p(a)$. So $\mathrm{ord}_p(a)$ is the maximum of all integers n for which a is divisible by p^n.

The factorization into primes of a can be written as

$$a = \prod_{p \in \mathbb{P}} p^{\mathrm{ord}_p(a)}$$

Here the product is taken over the set $\mathbb{P}$ of all primes. Note however, that only a finite number of factors is distinct from 1.

By definition, a product that has the empty set as index set (the empty product) is 1. With this convention the equality also holds for $a = 1$.

Here is an explicit description of the gcd and lcm of two integers in terms of their prime factorizations.

Theorem 8.5.6. If a and b are positive integers, then

$$\gcd(a,b) = \prod_{p\in\mathbb{P}} p^{min\left(\mathrm{ord}_p(a),\mathrm{ord}_p(b)\right)}$$

and

$$\mathrm{lcm}(a,b) = \prod_{p\in\mathbb{P}} p^{max\left(\mathrm{ord}_p(a),\mathrm{ord}_p(b)\right)}$$

In particular we have

$$a\cdot b = \gcd(a,b)\cdot \mathrm{lcm}(a,b)$$

Proof. We prove the first equality: For each prime p we certainly have: $min(\mathrm{ord}_p(a),\mathrm{ord}_p(b)) \leq \mathrm{ord}_p(a)$ and $min(\mathrm{ord}_p(a),\mathrm{ord}_p(b)) \leq \mathrm{ord}_p(b)$. Hence the right-hand side of the equality $\gcd(a,b) = \prod_{p\in\mathbb{P}} p^{min\left(\mathrm{ord}_p(a),\mathrm{ord}_p(b)\right)}$ is a common divisor of a and b. In particular, by the Characterization of the gcd , 8.2.9 we find that the right-hand side divides $\gcd(a,b)$.

On the other hand, if for some prime p we have $\mathrm{ord}_p(\gcd(a,b)) = m$, then p^m divides both a and b. Therefore, $m \leq \mathrm{ord}_p(a)$ and $m \leq \mathrm{ord}_p(b)$.

Hence the left-hand side of the equation $\gcd(a,b) = \prod_{p\in\mathbb{P}} p^{min\left(\mathrm{ord}_p(a),\mathrm{ord}_p(b)\right)}$ is a divisor of the right-hand side.

Combining the above the equality follows.

The proof of the second equality is left to the reader.

The third statement is a direct consequence of the first two, when you take into account that, for any two integers, their sum is equal to the sum of their maximum and their minimum. In Relation between ggd and lcma 8.1.19nother proof of this statement is given.

□

Example 8.5.7. Suppose that a is a positive integer and that p^n divides a for some prime number p and positive integer n. Choose n maximal with this property, so $n = \mathrm{ord}_p(a)$. Then the binomial coefficient $\begin{pmatrix} a \\ p^n \end{pmatrix}$ is not divisible by p.

Indeed, the binomial coefficient $\begin{pmatrix} a \\ p^n \end{pmatrix}$ can be written as the quotient of $\prod_{i=0}^{p^n-1}(a-i)$ by $(p^n)!$.

Now for all positive integers b with $b \leq p^n$ we find that $\mathrm{ord}_p(b)$ equals $\mathrm{ord}_p(a-b)$. So every factor p in the numerator is canceled by a factor p in the denominator.

Example 8.5.8. Given the integers a and b we can express them as a product of primes. Indeed, we can factor $a = 345$ and $b = 246$ as $a = 3\cdot 5\cdot 23$ and $b = 2\cdot 3\cdot 41$

Moreover, $\gcd(a,b) = 3$ and $\mathrm{lcm}(a,b) = 2\cdot 3\cdot 5\cdot 23\cdot 41$

Each of the factors in the above products is prime. You can check this with the Prime test of Eratothenes. 8.4.12

The prime factorization is very well suited for studying the multiplicative structure of the integers. However, it is not so convenient to study the additive structure.

8.6 The b-ary number system

We commonly represent integers in the *decimal system*. But there are also other systems, like the *binary system* which is heavily used in computer science. The decimal and binary system are two examples in a

series.

Definition 8.6.1 — b-ary representation. Let $b > 1$ be an integer. A b-ary representation, or representation with respect to base b, of an integer $a \geq 0$ is a sequence of numbers $a_0, \ldots, a_k$ with $0 \leq a_i < b$ (the *digits*), such that $a = \sum_{i=0}^{k} a_i \cdot b^i$

We write $a = [a_k, \ldots, a_0]_b$. We speak of the *b-ary number system*.

Remark 8.6.2. Besides the binary system, the octal (base 8) and hexadecimal (base 16) systems are often used in computer science.

In base 8 we use the digits 0 to 7, but in base 16 we need more digits. Apart from the digits 0 to 9, it is customary to use the symbols A, B, C, D, E, F to represent the decimal numbers 10, 11, 12, 13, 14, and 15, respectively.

Thus, the integer 123 is represented as $[7\mathrm{B}]_{16}$.

In the b-ary number system, every positive number can be written in precisely one way.

Theorem 8.6.3. Let $b > 1$ be an integer. Every integer $a \geq 0$ has a b-ary representation. Furthermore, this representation is unique if $a > 0$ and if we require that $a_k \neq 0$ for the 'most significant' (i.e., left most) digit in $a = [a_k, \ldots, a_0]_b$.

Proof. The proof consists of two parts. In both we proceed by induction on a.

Existence: the number a has a b-ary representation.

For $a = 0$, a b-ary representation is $[0]_b$. Now suppose that $a > 0$ and that the existence assertion is true for all non-negative integers less than a. Let r be the remainder of division of a by b. Then $0 \leq r$ and $r < b$. Moreover, $b | a - r$. Since $\frac{a-r}{b} < a$, we can apply the induction hypothesis. We find that there are digits $a_0, \ldots, a_k$ satisfying $\frac{a-r}{b} = \sum_{i=0}^{k} a_i \cdot b^i$ Rewriting this expression as $a = r + \sum_{i=0}^{k} a_i \cdot b^{i+1}$ we find that $a = [a_k, \ldots, a_0, r]_b$.

Uniqueness of the representation.

Suppose that $a = [a_k, \ldots, a_0]_b$ and also $a = [c_l, \ldots, c_0]_b$ are both b-ary representations of a. By the assumption on the most significant digit we have $a_k \neq 0$ and $c_l \neq 0$. According to the first representation, the remainder when a is divided by b is equal to a_0 and, according to the second, it equals c_0. Hence $a_0 = c_0$. If $a < b$, then $a = a_0$ and we are finished. Otherwise, we apply the induction hypothesis to the number $\frac{a-a_0}{b}$, which is smaller than a. It has representations $[c_l, \ldots, c_1]_b$ and $[a_k, \ldots, a_1]_b$ in the b-ary number system. So, by the induction hypothesis, $k = l$ and $a_i = c_i$ for all $i \in \{1, \ldots, k\}$. As we already proved $a_0 = c_0$, this establishes that the two representations are the same.

□

Example 8.6.4. The proof of Theorem on b-ary Representation 8.6.3 provides an algorithm for computing the b-ary representation of the integer a (which is given in the decimal system). Suppose $a = 1238$ and $b = 7$. The last symbol in the string representing a equals $\mathrm{rem}(a, b)$, while the string before the last symbol is the representation of $\mathrm{quot}(a, b)$.

We begin with the empty string. At each step of the algorithm we insert the remainder $\mathrm{rem}(a, b)$ at the beginning of the string and replace a by $\mathrm{quot}(a, b)$.

The algorithm starts with $a = 1238$ and stops when a is equal to 0.

Each row of the following table represents a step in the algorithm.

The algorithm has finished! The b-ary representation, where $b = 7$, of $a = 1238$ equals $[3416]_7$.

8.7 Exercises

Exercise 8.7.1. Determine the remainder of a divided by b for each of the following pairs a, b.

n	$a_n = \text{quot}(a_{n-1}, b)$	$\text{rem}(a_{n-1}, b)$
1	176	6
2	25	1
3	3	4
4	0	3

Table 8.3: b-ary representation

(a) 480, 175;
(b) 5621, 192;
(c) 983675, 105120.

Exercise 8.7.2. Suppose that a and b are nonzero integers. Prove that if a divides b and b divides a, then $a = b$ or $a = -b$.

Exercise 8.7.3. Show that if a divides b and c divides d, then $a \cdot c$ divides $b \cdot d$.

Exercise 8.7.4. Use induction to prove that 10 divides $3^{4 \cdot n} - 1$ for all positive integers n.

Exercise 8.7.5. Use induction to prove that, if a and b are integers, $a - b$ divides $a^n - b^n$ for every positive integer n.

Exercise 8.7.6. Determine the $\gcd$ and lcm of a and b for each of the following pairs a, b.
(a) 48, 15;
(b) 21, 19;
(c) 75, 105.

Exercise 8.7.7. Suppose that a and b are nonzero relatively prime integers and suppose that c is a divisor of a. Prove that c and b are relatively prime.

Exercise 8.7.8. Show that the following three properties hold for the greatest common divisor. Here, a, b and k are integers.
(a) $\gcd(a,b) = \gcd(b,a)$
(b) $\gcd(a,b) = \gcd(a, b - k \cdot a)$
(c) $\gcd(a,0) = |a|$

Exercise 8.7.9. For any positive integer n divide $10^{3 \cdot n}$ by $10^n - 1$ and find the remainder.

Exercise 8.7.10. If n is a positive integer, determine the possibilities for the greatest common divisor of n and $n^2 + 3$, and also provide examples.

Exercise 8.7.11. Three cogwheels with 24, 15, and 16 cogs, respectively, touch as shown.

What is the smallest positive number of times you have to turn the left-hand cogwheel (with 24 cogs) before the right-hand cogwheel (with 16 cogs) is back in its original position? What is the smallest positive number of times you have to turn the left-hand cogwheel before all three wheels are back in their original position?

Exercise 8.7.12. Prove that the square of an odd integer is again odd, where 'odd' means 'not divisible by 2' or, equivalently, 'having remainder 1 upon division by 2'. Show that the remainder of division by 4 of the square of an odd integer is 1. Does the last statement hold if we replace 4 by 8? And by 16?

Exercise 8.7.13. Suppose that a, b, and c are integers. If c divides a and b, it also divides $\text{rem}(a,b)$. Prove this.

Exercise 8.7.14. If c is a common multiple of the integers a and b, then c is a multiple of $\text{lcm}(a,b)$. Prove this.

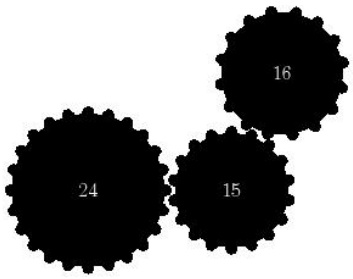


Figure 8.10: Three cogs.

Exercise 8.7.15. Determine the $\gcd$ of each of the following pairs of numbers, and write this gcd as a linear combination of the given numbers:
(a) 480, 175;
(b) 5621, 192;
(c) 983675, 105120.

Exercise 8.7.16. Show that, for all positive integers x and y, and non negative z, we have $\gcd(z\cdot x, z\cdot y) = z\cdot\gcd(x,y)$

Exercise 8.7.17. Suppose that d is the nonzero gcd of a and b. Prove that a/d and b/d are relatively prime.

Exercise 8.7.18. Let a, b, and c be integers. Show that $\gcd(a,b,c) = \gcd(\gcd(a,b),c)$

Exercise 8.7.19. Let a, b and c be integers. Prove that there are integers x, y, and z such that $\gcd(a,b,c) = x\cdot a + y\cdot b + z\cdot c$

Exercise 8.7.20. Let a be a rational number such that both $18\cdot a$ and $25\cdot a$ are integers. Show that a itself is an integer.

Exercise 8.7.21. Let a, b, and c be nonzero integers.
Determine the set of all integers that can be expressed in the form $x\cdot a + y\cdot b + z\cdot c$ with x, y, and z integers.

Exercise 8.7.22. Determine the $\gcd$ of each of the following pairs of numbers, and write each gcd as a linear combination of the given numbers:
(a) 5672, 234;
(b) 5311, 121;
(c) 32125, 1012.

Exercise 8.7.23. Suppose a is a rational number such that $45\cdot a$ and $36\cdot a$ are integers. Is a necessarily an integer? And what if $20\cdot a$ is also known to be an integer?

Exercise 8.7.24. Find all integer solutions x and y to the following Diophantine equations.
(a) $22\cdot x + 32\cdot y = 12$
(b) $12\cdot x + 25\cdot y = 11$
(c) $24\cdot x + 36\cdot y = 18$

Exercise 8.7.25. In how many ways can you pay 50 eurocents using only 5 euro cent and 20 euro cent coins? Can you do it with exactly 7 coins?

Exercise 8.7.26. Find all integers x, y, and z that satisfy the two equations $x + y + 3\cdot z = 19$ and $x + 2\cdot y + 5\cdot z = 29$ simultaneously. Also, determine all solutions with x, y, and z positive.

Exercise 8.7.27. Determine all primes of the form $n^2 - 4$, where n is an integer.

Exercise 8.7.28. Determine all primes p and q satisfying $p \cdot q = 4 \cdot p + 7 \cdot q$.

Exercise 8.7.29. Prove that there exist infinitely many primes of the form $4 \cdot n + 3$, where n is a positive integer.

Exercise 8.7.30. Let $p > 1$ be an integer. Prove that p is a prime if and only if for every integer a either $\gcd(p,a) = 1$ or $\gcd(p,a) = p$.

Exercise 8.7.31. Let p be a prime and let a be a positive multiple of p. Show that there exists a positive integer n such that a/p^n is an integer and $\gcd(p, a/p^n) = 1$.

Exercise 8.7.32. Determine all primes less than 100.

Exercise 8.7.33. Determine all primes of the form $n^3 + 1$, with n an integer.

Exercise 8.7.34. Which of the following integers is prime: 187, 287, 387, 487, or 587?

Exercise 8.7.35. Let n be an integer greater than 1, and let p be the smallest divisor of n greater than 1. Prove that p is prime.

Exercise 8.7.36. Determine the prime factorization of the integers 111, 143, 724, and 1011.

Exercise 8.7.37. Prove that the cube root of 17 is not rational.

Exercise 8.7.38. Prove that 5 is the only prime p such that $3 \cdot p + 1$ is a square.

Exercise 8.7.39. The musical pitch of each note corresponds to its frequency, which is expressed in Hertz. If you double the frequency, you find a note an octave higher. If you change the frequency by a factor $3/2$, you obtain a note which is a so-called fifth higher. Starting from a given note, you can construct notes which are one, two, etc., octaves higher. Similarly, you can construct notes which are one, two, etc., fifths higher. Show that these two series of notes have no note in common, except the note you started with.

Exercise 8.7.40. Suppose that a and b are coprime positive integers and that the positive integer n is a multiple of both a and b. Show that n is a multiple of $a \cdot b$.

Exercise 8.7.41. Determine $\gcd\left(2^3 \cdot 3^5 \cdot 7^2, 2^4 \cdot 5 \cdot 5 \cdot 11\right)$ and $\operatorname{lcm}\left(2^3 \cdot 3^5 \cdot 7^2, 2^4 \cdot 5 \cdot 5 \cdot 11\right)$.

Exercise 8.7.42. Determine $\gcd\left(4^3 \cdot 6^5 \cdot 7^2, 8^4 \cdot 10^5 \cdot 11\right)$.

Exercise 8.7.43. Determine $\gcd\left(2^4 \cdot 3^2 \cdot 5 \cdot 7^6 \cdot 11, 2^2 \cdot 3^2 \cdot 5^3 \cdot 11\right)$.

Exercise 8.7.44. How many different positive divisor does 1000 have? And how many $10.000.000$?

Exercise 8.7.45. What are the gcd and lcm of the following integers:
(a) $2^3 \cdot 5^7 \cdot 11$ and $2^2 \cdot 3^4 \cdot 5^2 \cdot 11^4$;
(b) $2^1 \cdot 3^3 \cdot 5^2$ and $2^2 \cdot 3^4 \cdot 5 \cdot 11$;
(c) $3^2 \cdot 4^5 \cdot 7^2$ and $2^3 \cdot 3^2 \cdot 6^5 \cdot 7^2$.

Exercise 8.7.46. Prove the following identity: $\gcd\left(a^2, b^2\right) = (\gcd(a,b))^2$.

Exercise 8.7.47. Compute the 7-ary representation of the following integers given in their decimal representation: 12373, 32147, and 7231.

Exercise 8.7.48. Write an algorithm that converts numbers given in the decimal system to the binary system and vice versa.

Exercise 8.7.49. Compute the 3-ary representation of the following integers given in their decimal representation: 12373, 32147, and 7231.

Exercise 8.7.50. Which b-ary system would you use to weigh all possible weights between 1 and 40 with just four standard weights on a balance?

Exercise 8.7.51. The decimal representation of an integer n is $[\text{abcabc}]_{10}$, where a, b and c are elements from $\{0, \ldots, 9\}$.

Prove that 7, 11, and 13 are divisors of n.

Exercise 8.7.52. The integers 1222, 124211, 2113 and 4121 are given in their decimal representation.

Give the representation in base 2, 4, and 8, respectively.

9. Modular arithmetic

It frequently happens that we prefer to ignore multiples of a given number when we do calculations. Just think of the days in the week or the hours in a day; in the first case we ignore multiples of seven, in the second case multiples of 12 or 24. In this chapter we will describe this "arithmetic modulo n". As an application we will describe the RSA cryptosystem.

9.1 Arithmetic modulo n

Clock arithmetic is an example of arithmetic modulo an integer, which is 24 in this case. Suppose that the time is 15:00 hours. If 20 hours pass by, then it will be 11:00 hours. In terms of modular arithmetic, we say that 15 + 20 equals 11 modulo 24. Here, modulo means "up to a multiple of". On the other hand, if 83 hours elapse, then it will be 2 o'clock in the morning. In modular arithmetic, 15 + 83 equals 2 modulo 24. We look at the time of day as a quantity determined up to a multiple of 24.

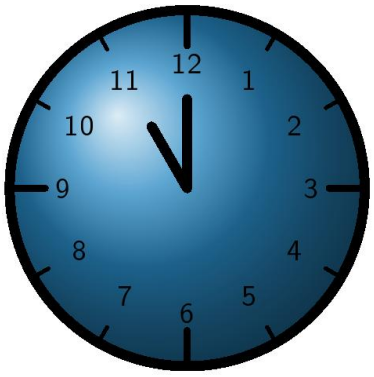


Figure 9.1: Clock arithmetic

Pierre de Fermat

We will analyze arithmetic modulo an integer.

Definition 9.1.1. Let n be an integer. On the set $\mathbb{Z}$ of integers we define the relation *congruence modulo n* as follows: a and b are *congruent modulo n* if and only if $n|a-b$.

We write $a \equiv b \pmod{n}$ to denote that a and b are congruent modulo n. If a and b are congruent modulo n, we also say that a is congruent to b modulo n, or that a is equal to b modulo n.

Example 9.1.2. If $a = 342$, $b = 241$, and $n = 17$, then a is not congruent to b modulo n. Indeed $a - b = 101$ is not divisible by $n = 17$.

However, if $a = 342$, $b = 240$, and $n = 17$, then a is congruent to b modulo n. Indeed, $a - b = 102$ is divisible by $n = 17$.

Proposition 9.1.3. Let n be an integer. The relation congruence modulo n is reflexive, symmetric, and transitive; in particular, it is an equivalence relation.

For nonzero n, there are exactly n distinct equivalence classes:

$$n\cdot\mathbb{Z}, 1+n\cdot\mathbb{Z}, \ldots, n-1+n\cdot\mathbb{Z}$$

The set of equivalence classes of $\mathbb{Z}$ modulo n is denoted by $\mathbb{Z}/n\mathbb{Z}$.

Proof. We need to verify that the relation is reflexive, symmetric, and transitive. This implies congruence modulo n to be an equivalence relation. The other statements of the proposition follow easily.

The relation is reflexive.

Let a be an integer. Then $a \equiv a \pmod{n}$ as n divides $a - a = 0$.

The relation is symmetric.

Suppose that a and b are integers with $a \equiv b \pmod{n}$. Then n divides $a - b$, and hence also $b - a$. Thus $b \equiv a \pmod{n}$.

The relation is transitive.

If a, b, and c are integers with $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$, then n divides both $a - b$ and $b - c$. But then n is also a divisor of $a - b + b - c = a - c$ and so $a \equiv c \pmod{n}$.

□

Example 9.1.4. As congruence modulo n is an equivalence relation, its equivalence classes partition the set $\mathbb{Z}$ of all integers.

For example, the relation modulo 2 partitions the integers into two classes, the even numbers and the odd numbers.

Remark 9.1.5. In the Definition of quot and rem 8.1, the notation $\mathrm{rem}(a,n)$ for the remainder r of the division of a by n is introduced. Observe that r is congruent to a modulo n. The remainder r is a natural representative of the set of all elements congruent to a modulo n.

If n equals 0, then a is only congruent to itself modulo n.

Congruence modulo n is the same relation as congruence modulo $-n$. So, when studying congruence modulo n, we may take n to be non-negative without loss of generality.

The set $k + n\cdot\mathbb{Z}$ consists of all integers of the form $k + n\cdot m$ where m is an integer. It is the equivalence class of congruence modulo n containing the integer k and will also be denoted by $k \pmod{n}$.

The integer k is a representative of this equivalence class. If no confusion arises, we will also denote the class $k \pmod{n}$ by k itself.

Let n be an integer. Consider $\mathbb{Z}/n\mathbb{Z}$, the set of equivalence classes of $\mathbb{Z}$ modulo n. Addition and multiplication with these classes can be defined in the following way.

Theorem 9.1.6 — Addition and Multiplication. On $\mathbb{Z}/n\mathbb{Z}$ we define two so-called binary operations, an *addition* and a *multiplication*, by:

- Addition: $x \pmod n + y \pmod n = x + y \pmod n$.
- Multiplication: $x \pmod n \cdot y \pmod n = x \cdot y \pmod n$.

Both operations are well defined.

Proof. We have to verify that the definitions of addition and multiplication are consistent. That is, if $x \equiv x' \pmod n$ and $y \equiv y' \pmod n$, then $x+y \equiv x'+y' \pmod n$ and $x \cdot y \equiv x' \cdot y' \pmod n$. For then, the outcome of an addition or multiplication is independent of the chosen representatives. Well, $x \equiv x' \pmod n$ means that there exists an integer a such that $x - x' = n \cdot a$. Similarly, $y \equiv y' \pmod n$ means that there exists an integer b such that $y - y' = n \cdot b$.

Addition.

The above implies $(x+y) - (x'+y') = x - x' + y - y' = n \cdot a + n \cdot b = n \cdot (a+b)$. Hence $x+y \equiv x'+y' \pmod n$.

Multiplication.

By the above we find $x \cdot y - x' \cdot y' = x \cdot (y - y') + (x - x') \cdot y' = n \cdot b \cdot x + n \cdot a \cdot y' = n \cdot (b \cdot x + a \cdot y')$. Hence $x \cdot y \equiv x' \cdot y' \pmod n$.

□

Example 9.1.7 — Tables for modular addition and multiplication. Here is the addition table for $\mathbb{Z}/17\mathbb{Z}$.

+	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
0	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	0
2	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	0	1
3	3	4	5	6	7	8	9	10	11	12	13	14	15	16	0	1	2
4	4	5	6	7	8	9	10	11	12	13	14	15	16	0	1	2	3
5	5	6	7	8	9	10	11	12	13	14	15	16	0	1	2	3	4
6	6	7	8	9	10	11	12	13	14	15	16	0	1	2	3	4	5
7	7	8	9	10	11	12	13	14	15	16	0	1	2	3	4	5	6
8	8	9	10	11	12	13	14	15	16	0	1	2	3	4	5	6	7
9	9	10	11	12	13	14	15	16	0	1	2	3	4	5	6	7	8
10	10	11	12	13	14	15	16	0	1	2	3	4	5	6	7	8	9
11	11	12	13	14	15	16	0	1	2	3	4	5	6	7	8	9	10
12	12	13	14	15	16	0	1	2	3	4	5	6	7	8	9	10	11
13	13	14	15	16	0	1	2	3	4	5	6	7	8	9	10	11	12
14	14	15	16	0	1	2	3	4	5	6	7	8	9	10	11	12	13
15	15	16	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
16	16	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15

Table 9.1: Addition table for $\mathbb{Z}/17\mathbb{Z}$.

Below is the multiplication table for $\mathbb{Z}/17\mathbb{Z}$.

In computations modulo n the following properties of the two operations addition and multiplication are often tacitly used. They look quite straightforward and are easy to use in practice. But since we have

·	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
2	0	2	4	6	8	10	12	14	16	1	3	5	7	9	11	13	15
3	0	3	6	9	12	15	1	4	7	10	13	16	2	5	8	11	14
4	0	4	8	12	16	3	7	11	15	2	6	10	14	1	5	9	13
5	0	5	10	15	3	8	13	1	6	11	16	4	9	14	2	7	12
6	0	6	12	1	7	13	2	8	14	3	9	15	4	10	16	5	11
7	0	7	14	4	11	1	8	15	5	12	2	9	16	6	13	3	10
8	0	8	16	7	15	6	14	5	13	4	12	3	11	2	10	1	9
9	0	9	1	10	2	11	3	12	4	13	5	14	6	15	7	16	8
10	0	10	3	13	6	16	9	2	12	5	15	8	1	11	4	14	7
11	0	11	5	16	10	4	15	9	3	14	8	2	13	7	1	12	6
12	0	12	7	2	14	9	4	16	11	6	1	13	8	3	15	10	5
13	0	13	9	5	1	14	10	6	2	15	11	7	3	16	12	8	4
14	0	14	11	8	5	2	16	13	10	7	4	1	15	12	9	6	3
15	0	15	13	11	9	7	5	3	1	16	14	12	10	8	6	4	2
16	0	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1

Table 9.2: Multiplication table for $\mathbb{Z}/17\mathbb{Z}$.

constructed a new arithmetical structure, they actually do require proofs. Here is a list of the properties we mean.

Proposition 9.1.8 — Properties of Modular Arithmetic. Let n be an integer bigger than 1. For all integers a, b, and c, we have the following equalities.

- Commutativity of addition:

$$a \pmod n + b \pmod n = b \pmod n + a \pmod n.$$

- Commutativity of multiplication:

$$a \pmod n \cdot b \pmod n = b \pmod n \cdot a \pmod n.$$

- Associativity of addition:

$$\Big(a \pmod n + b \pmod n\Big) + c \pmod n = a \pmod n + \Big(b \pmod n) + c \pmod n\Big).$$

- Associativity of multiplication:

$$\Big(a \pmod n \cdot b \pmod n\Big) \cdot c \pmod n = a \pmod n \cdot \Big(b \pmod n \cdot c \pmod n\Big).$$

- Distributivity of multiplication over addition:

$$a \pmod n \cdot \Big(b \pmod n + c \pmod n\Big) = a \pmod n \cdot b \pmod n + a \pmod n \cdot c \pmod n.$$

Proof. The laws hold for integers. For instance, in the case of commutativity, we have $a+b=b+a$. Now apply the Modular Addition and Multiplication Theorem 9.1.6 to both sides. The commutativity for $\mathbb{Z}/n\mathbb{Z}$ follows. The proofs of the other equalities are similar.

□

Example 9.1.9 — Solving equations. Calculations modulo an integer can sometimes be used to show that an equation has no integer solutions. By working in $\mathbb{Z}/4\mathbb{Z}$, for example, we can show that 1203 cannot be written as a sum of two (integer) squares. For, in $\mathbb{Z}/4\mathbb{Z}$, the set of squares is $\{0,1\}$. This is easily verified by squaring each of the four elements of $\mathbb{Z}/4\mathbb{Z}$. Indeed,

$$\begin{aligned}(0 \pmod 4)^2 &= 0 \pmod 4,\\ (1 \pmod 4)^2 &= 1 \pmod 4,\\ (2 \pmod 4)^2 &= 0 \pmod 4,\\ (3 \pmod 4)^2 &= 1 \pmod 4.\end{aligned}$$

Now if m and n are integral, then $m^2+n^2 \pmod 4 = m^2 \pmod 4 + n^2 \pmod 4$, and, by the above, this sum can only take the values $0 \pmod 4$, $1 \pmod 4$, or $2 \pmod 4$. So m^2+n^2 is not equal to 3 plus a multiple of 4. In particular, 1203 cannot be written as the sum of two squares.

Example 9.1.10 — The nine test. Suppose that $a = [a_k, \ldots, a_0]_{10}$ is the usual decimal representation of a. The well-known nine test

$$9|a \Leftrightarrow 9|a_k + \cdots + a_0$$

is based on modular arithmetic. In order to see this, we work modulo 9.

Since

$$10 \equiv 1 \pmod 9,$$

we find

$$10^n \equiv 1^n \equiv 1 \pmod 9$$

for all non negative integers n. As $[a_k, \ldots, a_0]_{10} = a_k \cdot 10^k + \cdots + a_0 \cdot 10^0$ reduction modulo 9 implies that $a \equiv a_k + \cdots + a_0 \pmod 9$. Thus $9|a$ if and only if $9|a_k + \cdots + a_0$.

Example 9.1.11 — Trigonometric arguments. When playing with a calculator, you may have noticed that $\sin(10^a)$ gives the same value for all values of a bigger than 2, at least when the argument expresses the number of degrees of an angle. The explanation is that 10^a is the same number modulo 360 for each of these values of a. Check this!

Example 9.1.12 — Calculating with powers. Modular arithmetic can greatly reduce the amount of work when computing divisibility properties of expressions involving powers. By way of example, we show that 10^9+1 is divisible by 19. Working modulo 19 we start with $10^2 \equiv 5 \pmod{19}$. Squaring this equation, we find $10^4 \equiv 6 \pmod{19}$. Similarly we get $10^8 \equiv -2 \pmod{19}$ and $10^9 \equiv -1 \pmod{19}$. But then we deduce that $10^9+1 \equiv 0 \pmod{19}$, which implies that $19|10^9+1$.

9.2 Invertible elements and zero divisors

Consider $\mathbb{Z}/n\mathbb{Z}$. A *neutral* element for the addition is $0 \pmod n$. Indeed, $a \pmod n + 0 = a \pmod n$ and $0 + a \pmod n = a \pmod n$. The *opposite* of $a \pmod n \in \mathbb{Z}/n\mathbb{Z}$ is $-a \pmod n$, the unique element b such that $a \pmod n + b \pmod n = 0$.

A *neutral* element for the multiplication is $1 \pmod n$, as $a \pmod n \cdot 1 \pmod n = a \pmod n$ and $1 \pmod n \cdot a \pmod n = a \pmod n$.

The set $\mathbb{Z}/n\mathbb{Z}$ together with addition and multiplication is an example of a quotient ring, an algebraic structure to be discussed in the theory of rings and fields.

In $\mathbb{Z}/n\mathbb{Z}$ we can add, multiply, and subtract. But how about division? Does every nonzero element have an inverse?

Definition 9.2.1. An element $a \in \mathbb{Z}/n\mathbb{Z}$ is called *invertible* if there is an element b, called *inverse* of a, such that $a \cdot b = 1$.

If a is invertible, its inverse (which is unique, as follows from Uniqueness of the Inverse 9.2.3) will be

denoted by a^{-1}.

The set of all invertible elements in $\mathbb{Z}/n\mathbb{Z}$ will be denoted by $\mathbb{Z}/n\mathbb{Z}^{\times}$. This set is also called the *multiplicative group* of $\mathbb{Z}/n\mathbb{Z}$.

Example 9.2.2. In $\mathbb{Z}/18\mathbb{Z}$ the element $5 \pmod{18}$ is invertible. Indeed, since $2\cdot 18 - 7\cdot 5 = 1$, the inverse of $5 \pmod{18}$ is $7 \pmod{18}$. The element $6 \pmod{18}$ is not invertible, since any multiple of 6 is either congruent to 0, 6, or 12 modulo 18.

Proposition 9.2.3 — Uniqueness of the Inverse. Let $n > 1$. If an element $a \in \mathbb{Z}/n\mathbb{Z}$ is invertible, then its inverse is unique.

Proof. Suppose $a \pmod{n}$ is invertible with inverses $b \pmod{n}$ and $c \pmod{n}$. Then

$$a \pmod{n} \cdot b \pmod{n} = a \pmod{n} \cdot c \pmod{n} = 1$$

and hence

$$\begin{aligned} b \pmod{n} &= b \pmod{n} \cdot \Big(a \pmod{n} \cdot c \pmod{n}\Big) \\ &= \Big(a \pmod{n} \cdot b \pmod{n}\Big) \cdot c \pmod{n} \\ &= 1 \pmod{n} \cdot c \pmod{n} \\ &= c \pmod{n}. \end{aligned}$$

So, the inverse of $a \pmod{n}$ is unique. □

An integer a will be called *invertible modulo n* if its class $a \pmod{n}$ is invertible.

In $\mathbb{Z}$ division is not always possible. Some nonzero elements do have an inverse, others don't. The following theorem tells us precisely which elements of $\mathbb{Z}/n\mathbb{Z}$ have an inverse.

Theorem 9.2.4 — Characterization of Modular Invertibility. Let $n > 1$ and $a \in \mathbb{Z}$.

(a) The class $a \pmod{n}$ in $\mathbb{Z}/n\mathbb{Z}$ has a multiplicative inverse if and only if $\gcd(a,n) = 1$.
(b) If a and n are relatively prime, then the inverse of $a \pmod{n}$ is the class $\text{Extgcd}(a,n)_2 \pmod{n}$.
(c) In $\mathbb{Z}/n\mathbb{Z}$, every class distinct from 0 has an inverse if and only if n is prime.

Proof. The second and third statement of the theorem are straightforward consequences of the first and its proof. So, we only prove the first. There are two parts to the proof.

If.

If $\gcd(a,n) = 1$, then, from the Extended Euclidean Algorithm 8.2.5, it follows that there are integers x and y such that $a\cdot x + n\cdot y = 1$. In $\mathbb{Z}/n\mathbb{Z}$ this translates to $a \pmod{n}\cdot x \pmod{n} + 0 = 1$. In particular, $x \pmod{n}$ is the inverse of $a \pmod{n}$.

Notice that x indeed coincides with $\text{Extgcd}(a,n)_2$ modulo n, which proves the second statement.

Only if.

If $a \pmod{n}$ has an inverse $b \pmod{n}$ in $\mathbb{Z}/n\mathbb{Z}$, then there exists an integer x with $a\cdot b + x\cdot n = 1$. So, by the Characterization of the gcd 8.2.9, we find $\gcd(a,n) = 1$.

□

Example 9.2.5. The invertible elements in $\mathbb{Z}/2^n\mathbb{Z}$ are the classes $x \pmod{2}^n$ for which x is an odd integer.

Indeed, the gcd of x and 2^n equals 1 if and only if x is odd.

An arithmetical system such as $\mathbb{Z}/p\mathbb{Z}$ with p prime, in which every element not equal to 0 has a multiplicative inverse, is called a *field*, just like $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$.

Suppose that n and a are integers with $n > 1$ and $\gcd(a,n) = 1$. The Characterization of Modular Invertibility 9.2.4 not only gives the existence of the inverse of $a \pmod n$ in $\mathbb{Z}/n\mathbb{Z}$, but also a way to compute this inverse.

Algorithm 9.2.6 — Modular Inverse.
- Input: integers $n > 1$ and a.
- Output: the inverse of the class $a \pmod n$ of a in $\mathbb{Z}/n\mathbb{Z}$ if it exists, and 0 otherwise.

```
Inverse := procedure(a, n)
local variables
    | E := Extgcd(a, n)
if E_1 = 1
    | then
    |     | return
    |     |     | E_2 (mod n)
    | else
    |     | return
    |     |     | 0
```

Proof.

Termination.
By the absence of loops this is obvious.

Correctness.

Obvious by part (b) of the Characterization of Modular Invertibility 9.2.4.

□

Example 9.2.7. Consider $a = 24$ and $n = 35$. Then a and n are relative prime. So $a \pmod n$ has an inverse. To find the inverse of $a \pmod n$, we apply the Extended Euclidean Algorithm. This gives the following expression of 1 as a linear combination of a and n:

$$1 = 35 \cdot 11 - 24 \cdot 16$$

We deduce that the inverse of $a \pmod n$ equals $-16 \pmod n$.

Besides invertible elements in $\mathbb{Z}/n\mathbb{Z}$, which can be viewed as divisors of 1, see Definition of inverse 9.2.1, one can also consider the divisors of 0.

Definition 9.2.8. An element $a \in \mathbb{Z}/n\mathbb{Z}$ not equal to 0 is called a *zero divisor* if there is a nonzero element b such that $a \cdot b = 0$.

Example 9.2.9. The zero divisors in $\mathbb{Z}/24\mathbb{Z}$ are those elements for which one finds a 0 in the corresponding row (or column) of the multiplication table. These are the elements $2 \pmod{24}$, $4 \pmod{24}$, $6 \pmod{24}$, $8 \pmod{24}$, $9 \pmod{24}$, $10 \pmod{24}$, $12 \pmod{24}$, $14 \pmod{24}$, $15 \pmod{24}$, $16 \pmod{24}$, $18 \pmod{24}$, $20 \pmod{24}$, $21 \pmod{24}$, and $22 \pmod{24}$.

The following theorem tells us which elements of $\mathbb{Z}/n\mathbb{Z}$ are zero divisors. They turn out to be those nonzero elements which are not invertible. Hence a nonzero element in $\mathbb{Z}/n\mathbb{Z}$ is either invertible or a zero divisor.

Theorem 9.2.10 — Zero Divisor Characterization. Let $n > 1$ and $a \in \mathbb{Z}$.
(a) The class $a \pmod n$ in $\mathbb{Z}/n\mathbb{Z}$ is a zero divisor if and only if $\gcd(a,n) > 1$ and $a \pmod n$ is nonzero.
(b) The residue ring $\mathbb{Z}/n\mathbb{Z}$ has no zero divisors if and only if n is prime.

·	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
1	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
2	2	4	6	8	10	12	14	16	18	20	22	0	2	4	6	8	10	12	14	16	18	20	22
3	3	6	9	12	15	18	21	0	3	6	9	12	15	18	21	0	3	6	9	12	15	18	21
4	4	8	12	16	20	0	4	8	12	16	20	0	4	8	12	16	20	0	4	8	12	16	20
5	5	10	15	20	1	6	11	16	21	2	7	12	17	22	3	8	13	18	23	4	9	14	19
6	6	12	18	0	6	12	18	0	6	12	18	0	6	12	18	0	6	12	18	0	6	12	18
7	7	14	21	4	11	18	1	8	15	22	5	12	19	2	9	16	23	6	13	20	3	10	17
8	8	16	0	8	16	0	8	16	0	8	16	0	8	16	0	8	16	0	8	16	0	8	16
9	9	18	3	12	21	6	15	0	9	18	3	12	21	6	15	0	9	18	3	12	21	6	15
10	10	20	6	16	2	12	22	8	18	4	14	0	10	20	6	16	2	12	22	8	18	4	14
11	11	22	9	20	7	18	5	16	3	14	1	12	23	10	21	8	19	6	17	4	15	2	13
12	12	0	12	0	12	0	12	0	12	0	12	0	12	0	12	0	12	0	12	0	12	0	12
13	13	2	15	4	17	6	19	8	21	10	23	12	1	14	3	16	5	18	7	20	9	22	11
14	14	4	18	8	22	12	2	16	6	20	10	0	14	4	18	8	22	12	2	16	6	20	10
15	15	6	21	12	3	18	9	0	15	6	21	12	3	18	9	0	15	6	21	12	3	18	9
16	16	8	0	16	8	0	16	8	0	16	8	0	16	8	0	16	8	0	16	8	0	16	8
17	17	10	3	20	13	6	23	16	9	2	19	12	5	22	15	8	1	18	11	4	21	14	7
18	18	12	6	0	18	12	6	0	18	12	6	0	18	12	6	0	18	12	6	0	18	12	6
19	19	14	9	4	23	18	13	8	3	22	17	12	7	2	21	16	11	6	1	20	15	10	5
20	20	16	12	8	4	0	20	16	12	8	4	0	20	16	12	8	4	0	20	16	12	8	4
21	21	18	15	12	9	6	3	0	21	18	15	12	9	6	3	0	21	18	15	12	9	6	3
22	22	20	18	16	14	12	10	8	6	4	2	0	22	20	18	16	14	12	10	8	6	4	2
23	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1

Table 9.3: The multiplication table modulo 24

Proof. The second statement of the theorem is a straightforward consequence of the first. So, we only prove the first. There are two parts to the proof.

If.

Suppose that $\gcd(a,n) > 1$, and set $b = n/\gcd(a,n)$. Then the class $b \pmod n$ of b is nonzero, but $a \cdot b$ is a multiple of n and so $a \cdot b \pmod n = 0$. This translates to $a \pmod n \cdot b \pmod n = 0$ in $\mathbb{Z}/n\mathbb{Z}$. In particular, $a \pmod n$ is a zero divisor.

Only if.

If $a \pmod n$ is a zero divisor, then it is nonzero and there is a nonzero element $b \pmod n$ in $\mathbb{Z}/n\mathbb{Z}$ with $a \pmod n \cdot b \pmod n = 0$. So, for the representative b_0 of $b \pmod n$ in $\{1,\ldots,n-1\}$, we find that $a \cdot b_0$ is a common multiple of a and n. In particular, $\operatorname{lcm}(a,n) < a \cdot b_0$, which is certainly less than $a \cdot n$. Now the Relation between ggd and lcm 8.1.19 implies that $\gcd(a,n) > 1$.

□

Example 9.2.11. Below you find the multiplication table of $\mathbb{Z}/17\mathbb{Z} \setminus \{0\}$. As you can see, it contains no entry with a 0, which implies that $\mathbb{Z}/17\mathbb{Z}$ has no zero divisors. Moreover, as each row and column contains a 1, each nonzero element of $\mathbb{Z}/17\mathbb{Z}$ is invertible.

·	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
2	2	4	6	8	10	12	14	16	1	3	5	7	9	11	13	15
3	3	6	9	12	15	1	4	7	10	13	16	2	5	8	11	14
4	4	8	12	16	3	7	11	15	2	6	10	14	1	5	9	13
5	5	10	15	3	8	13	1	6	11	16	4	9	14	2	7	12
6	6	12	1	7	13	2	8	14	3	9	15	4	10	16	5	11
7	7	14	4	11	1	8	15	5	12	2	9	16	6	13	3	10
8	8	16	7	15	6	14	5	13	4	12	3	11	2	10	1	9
9	9	1	10	2	11	3	12	4	13	5	14	6	15	7	16	8
10	10	3	13	6	16	9	2	12	5	15	8	1	11	4	14	7
11	11	5	16	10	4	15	9	3	14	8	2	13	7	1	12	6
12	12	7	2	14	9	4	16	11	6	1	13	8	3	15	10	5
13	13	9	5	1	14	10	6	2	15	11	7	3	16	12	8	4
14	14	11	8	5	2	16	13	10	7	4	1	15	12	9	6	3
15	15	13	11	9	7	5	3	1	16	14	12	10	8	6	4	2
16	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1

Table 9.4: Multiplication table for $\mathbb{Z}/17\mathbb{Z}$.

Since an element $a \pmod n$ of $\mathbb{Z}/n\mathbb{Z}$ is either 0, a zero divisor, or invertible, the Modular Inverse Algorithm 9.2.6 for computing inverses in $\mathbb{Z}/n\mathbb{Z}$ also provides us with a way to check whether an arbitrary

element of $\mathbb{Z}/n\mathbb{Z}$ is a zero divisor.

Let n be an integer. Inside $\mathbb{Z}/n\mathbb{Z}$, we can distinguish the set of invertible elements and the set of zero divisors. The set of invertible elements is closed under multiplication, the set of zero divisors together with 0 is even closed under multiplication by arbitrary elements.

Lemma 9.2.12. Let n be an integer with $n > 1$.

(a) If a and b are elements in $\mathbb{Z}/n\mathbb{Z}^\times$, then their product $a \cdot b$ is invertible and therefore also in $\mathbb{Z}/n\mathbb{Z}^\times$. The inverse of $a \cdot b$ is given by $b^{-1} \cdot a^{-1}$.

(b) If a is a zero divisor in $\mathbb{Z}/n\mathbb{Z}$ and b an arbitrary element, then $a \cdot b$ is either 0 or a zero divisor.

Proof. Assume that a and b are elements in $\mathbb{Z}/n\mathbb{Z}^\times$. As $(a \cdot b) \cdot (b^{-1} \cdot a^{-1}) = a \cdot a^{-1} = 1$ the inverse of $a \cdot b$ is $b^{-1} \cdot a^{-1}$. This establishes the first assertion.

If a is a zero divisor in $\mathbb{Z}/n\mathbb{Z}$, then there is a nonzero element c with $a \cdot c$ equal to 0. But then $a \cdot b \cdot c$ is also equal to 0. So $a \cdot b$ is 0 or a zero divisor.

□

Example 9.2.13. The zero divisors in $\mathbb{Z}/6\mathbb{Z}$ are those elements for which 0 occurs in the corresponding row (or column) of the multiplication table. The invertible elements are the elements for which 1 occurs in the corresponding row (or column).

·	1	2	3	4	5
1	1	2	3	4	5
2	2	4	0	2	4
3	3	0	3	0	3
4	4	2	0	4	2
5	5	4	3	2	1

Table 9.5: Multiplication table modulo 6.

So, the zero divisors are the classes of 2, 3, and 4, while the invertible elements are the classes of 1 and 5. Notice that $5^2 \pmod{n} = 1 \pmod{n}$. So indeed, the set of invertible elements is closed under multiplication.

9.3 Linear congruences

In addition to the linear equation

$$a \cdot x = b$$

with integer coefficients a and b in the single unknown x, we study, for positive integers n, the related equation

$$a \cdot x \equiv b \pmod{n}$$

in the unknown x. Such equation is called a *linear congruence*. It is closely related to the equation

$$a \cdot x = b$$

where a and b are elements of $\mathbb{Z}/n\mathbb{Z}$ and the unknown x is also in $\mathbb{Z}/n\mathbb{Z}$.

Solving such a linear congruence or the related equation in $\mathbb{Z}/n\mathbb{Z}$ is based on solving

$$a \cdot x + n \cdot y = b$$

in the unknown x and y; see Linear Diophantine Equation Solving Algorithm 8.3.4. The results of Linear Diophantine Equation Solving Algorithm 8.3.4 can easily be translated to the present situation. As a result we obtain the following algorithm for solving linear congruences.

Algorithm 9.3.1 — Linear Congruence.

- Input: integers a, b, and a positive integer n
- Output: the set of all classes x modulo n satisfying the equation $a \cdot x \equiv b \pmod{n}$

SolveLinCong $:=$ **procedure**(a,b,n)
local variables
  $E := \text{Extgcd}(a,n)$
  $g := E_1$
  $z := E_2$
if $g \mid b$
  then
    return
      $\left\{ z \cdot \frac{b}{g} + k \cdot \frac{n}{g} \pmod{n} \;\middle|\; k \in \mathbb{Z}/n\mathbb{Z} \right\}$
  else
    return
      $\varnothing$

Proof.

Termination.
Obvious in the absence of loops.

Correctness.

For each integer solution x to the linear congruence $a \cdot x \equiv b \pmod{n}$, there is an integer y such that the pair x, y is a solution to the linear Diophantine equation $a \cdot x + n \cdot z = b$, and vice versa. So, the correctness of the algorithm follows from the correctness of Linear Diophantine Equation Solving Algorithm 8.3.4 for solving linear Diophantine equations.

□

Remark 9.3.2. In the terminology of the Linear Congruence Algorithm 9.3.1, the solutions of the related equation $a \cdot x = b$ over $\mathbb{Z}/n\mathbb{Z}$ are the elements of the set

$$\left\{ z \cdot \frac{b}{g} + k \cdot \frac{n}{g} \pmod{n} \;\middle|\; k \in \mathbb{Z}/n\mathbb{Z} \right\}$$

Observe that there are exactly g distinct solutions.

Example 9.3.3. In order to find all solutions to the congruence $24 \cdot x \equiv 12 \pmod{15}$ we first compute the gcd of 24 and 15. Using the Extended Euclidean Algorithm 8.2.5 we find

$$\gcd(24,15) = 3 = 2 \cdot 24 - 3 \cdot 15$$

Now 3 divides 12, so the solution set is

$$\{(2 \cdot 12 + k \cdot 15)/3 \mid k \in \mathbb{Z}\}$$

Instead of using the algorithm, we can also use the expression of the gcd as a linear combination of 24 and 15 to argue what the solution is. To this end, multiply both sides of the equality $3 = 2 \cdot 24 - 3 \cdot 15$ by 4. This gives $12 = 8 \cdot 24 - 12 \cdot 15$.

So, a solution of the congruence is $x = 8 \pmod{15}$. Other solutions can be found by adding multiples of $15/3 \pmod{15}$ to this particular solution.

So, the complete set of solutions for x consists of the classes $3 \pmod{15}$, $8 \pmod{15}$, and $13 \pmod{15}$.

We extend the study of a single congruence to a method for solving special systems of congruences.

Theorem 9.3.4 — Chinese Remainder Theorem. Suppose that n_1, ..., n_k are pairwise coprime integers. Then for all integers a_1, ..., a_k the system of linear congruences

$$x \equiv a_i \pmod{n_i}$$

with $i \in \{1, \ldots, k\}$ has a solution.

Indeed, the integer

$$x = \sum_{i=1}^{k} a_i \cdot y_i \cdot \frac{n}{n_i}$$

where

$$n = \prod_{i=1}^{k} n_i$$

and for each i we have

$$y_i = \text{Extgcd}\left(\frac{n}{n_i}, n_i\right)_3$$

satisfies all congruences.

Any two solutions to the system of congruences are congruent modulo the product $\prod_{i=1}^{k} n_i$.

Proof. The proof consists of two parts.

Existence of a solution.

Let n be equal to $\prod_{i=1}^{k} n_i$. Then, by the assumption that all the n_i are coprime we find that for each i the greatest common divisor of n_i and $\frac{n}{n_i}$ equals 1. Thus by the Extended Euclidean Algorithm 8.2.5 we can find x_i and y_i with $x_i \cdot n_i + y_i \cdot \frac{n}{n_i} = 1$. Since $x_i \cdot n_i + y_i \cdot \frac{n}{n_i} = 1$, we find that $a_i \cdot y_i \cdot \frac{n}{n_i}$ is equal to a_i if we compute modulo n_i, and equal to 0 if we compute modulo n_j where $n_i \neq n_j$. This clearly implies that $x = \sum_{i=1}^{k} (a_i \cdot y_i \cdot \frac{n}{n_i})$ satisfies $x \equiv a_i \pmod{n_i}$ for all i. So we have found that x is a solution. This solution is not unique. Indeed, for any integer a, the integer $x + a \cdot n$ is also a solution.

Uniqueness modulo n.

Suppose that, besides x, also y is a solution to the system of congruences. Then for each i we find that the integer n_i divides the difference $x - y$. By the observation that, if two coprime integers divide an integer, then so does their product, this implies that $x - y$ is a common multiple of all the n_i, and thus a multiple of the least common multiple of the n_i, which equals n. This proves that up to multiples of n there is only one solution. □

Example 9.3.5. Suppose that a, b, m, and n are integers. We indicate how to find the common integral solutions x to the linear congruences $x \equiv a \pmod{m}$ and $x \equiv b \pmod{n}$.

Consider the case where $a = 13$, $b = 5$, $m = 14$, and $n = 17$.

Of course, adding multiples of $m \cdot n = 238$ to any solution will provide other solutions. Therefore we can restrict our attention to solutions in the interval $\{0, \ldots, 237\}$.

The positive integers x in $\{0, \ldots, 237\}$ satisfying $x \equiv 13 \pmod{14}$ are

$$13, 27, 41, 55, 69, 83, 97, 111, 125, 139, 153, 167, 181, 195, 209, 223, 237$$

The positive integers x in $\{0, \ldots, 237\}$ satisfying $x \equiv 5 \pmod{17}$ are

$$5, 22, 39, 56, 73, 90, 107, 124, 141, 158, 175, 192, 209, 226$$

So, modulo 238, the unique common solution to both congruences is 209.

Here is another way of making the last statement of Chinese Remainder Theorem 9.3.4: If x is a solution, then the set of all solutions is the set $x \pmod{\prod_{i=1}^{k} n_i}$.

The Chinese Remainder Theorem 9.3.4 can be turned into an algorithm to solve systems of linear congruences.

Algorithm 9.3.6 — Chinese Remainder Algorithm.

- Input: distinct and pairwise coprime integers n_1, ..., n_k, as well as integers a_1, ..., a_k.
- Output: a common solution x to the congruences $x \equiv a_i \pmod{n_i}$.

ChineseRemainder := **procedure**$(n_1,\ldots,n_k,a_1,\ldots,a_k)$
local variables
  i
  $y_1,\ldots,y_k$
  $n := \prod_{i=1}^{k} n_i$
for $i := 1$ **while** $i \leq k$ **with step** $i := i+1$ **do**
  $y_i := \text{Extgcd}\left(\frac{n}{n_i}, n_i\right)_3$
return
  $\sum_{i=1}^{k} a_i \cdot y_i \cdot \frac{n}{n_i}$

Proof.

Termination.
Obvious.

Correctness.

This follows immediately from the Chinese Remainder Theorem 9.3.4.

□

9.4 The Theorems of Fermat and Euler

Let p be a prime. Consider $\mathbb{Z}/p\mathbb{Z}$, the set of equivalence classes of $\mathbb{Z}$ modulo p. In $\mathbb{Z}/p\mathbb{Z}$ we can add, subtract, multiply, and divide by elements which are not 0. Moreover, it contains no zero divisors. So $\mathbb{Z}/p\mathbb{Z}$ has very nice properties. These are used in the proof of the following important result.

Figure 9.2: Pierre de Fermat (1601-1665).

Theorem 9.4.1 — Fermat's Little Theorem. Let p be a prime. For every integer a we have

$$a^p \equiv a \pmod{p}$$

In particular, if a is not in $0 \pmod{p}$ then

$$a^{p-1} \equiv 1 \pmod{p}$$

Equivalently, for all elements a in $\mathbb{Z}/p\mathbb{Z}$ we have

$$a^p = a$$

For nonzero elements a we have

$$a^{p-1} = 1$$

Proof. Although the statements on integers and on classes are easily seen to be equivalent, we present a proof for each of these. Let p be a prime.

For every integer a we have $a^p \equiv a \pmod{p}$.

For non negative a we give a proof by induction on a.

For a equal to 0 the statement is trivial. Now assume that, for some $a \geq 0$, we have $a^p \equiv a \pmod{p}$. By Newton's Binomium, we find that $(a+1)^p$ equals $\sum_{i=0}^{p} \binom{p}{i} \cdot a^i$. Recall that the binomial coefficient is determined by $\binom{p}{i} = \frac{p!}{(p-i)!\cdot i!}$. Thus, for i not equal to 0 or p, the numerator of this fraction is divisible by the prime p, whereas the denominator is not. We conclude that, for i not equal to 0 or p, the binomial coefficient $\binom{p}{i}$ is divisible by p.

As a result we find that $(a+1)^p \equiv a^p + 1 \pmod{p}$. Now, from the hypothesis $a^p \equiv a \pmod{p}$ we conclude that

$$(a+1)^p \equiv a+1 \pmod{p}$$

This proves the theorem for all non negative a.

If a is negative, then, by the above, $(-a)^p \equiv -a \pmod{p}$. If p is odd, we immediately deduce $a^p \equiv a \pmod{p}$. If p is even, then it is 2 and the above implies that $a^p \equiv -a \pmod{p}$. But as $-a \equiv a \pmod{2}$, we again find that $a^p \equiv a \pmod{p}$. This proves the assertion for all integers a.

For all elements a in $\mathbb{Z}/p\mathbb{Z}$ we have $a^p = a$.

For a equal to 0 the statements are trivial. Thus assume that a is nonzero. Consider the set $\mathbb{Z}/p\mathbb{Z}^\times$ of nonzero (and hence invertible) elements of $\mathbb{Z}/p\mathbb{Z}$.

Consider the map

$$M_a \colon \mathbb{Z}/p\mathbb{Z}^\times \to \mathbb{Z}/p\mathbb{Z}^\times, b \longmapsto a \cdot b$$

that is, multiplication by a. As $\mathbb{Z}/p\mathbb{Z}$ contains no zero divisors, see Characterization of Modular Invertibility 9.2.4, the map is well defined. Moreover, this map is bijective. Indeed, its inverse is $M_{a^{-1}}$, multiplication by a^{-1}. As a result we see that the product of all elements in $\mathbb{Z}/p\mathbb{Z}^\times$ is not only equal to $\prod_{z \in \mathbb{Z}/p\mathbb{Z}^\times} z$, but also to $\prod_{z \in \mathbb{Z}/p\mathbb{Z}^\times} (M_a(z))$. The products are taken over the same set. The order in which the elements are multiplied might differ, but that does not affect the result. The latter product equals

$$\prod_{z \in \mathbb{Z}/p\mathbb{Z}^\times} ((a \cdot z)) = a^{p-1} \cdot \prod_{z \in \mathbb{Z}/p\mathbb{Z}^\times} z$$

By Characterization of Modular Invertibility 9.2.4 the product $\prod_{z\in\mathbb{Z}/p\mathbb{Z}^\times} z$ is nonzero and hence invertible, see Invertibility of Products 9.2.12. Therefore, $a^{p-1}=1$. Multiplying both sides of the equation by a proves the assertion.

The other statements in Fermat's Little Theorem 9.4.1 follow easily from the above assertions.

□

Example 9.4.2. As 7 is prime, Fermat's Little Theorem 9.4.1 implies that $2^6 \equiv 1 \pmod 7$. Indeed, $2^6 = 64 = 9\cdot 7+1$.

Example 9.4.3. The integer $1234^{1234}-2$ is divisible by 7.

Indeed, if we compute modulo 7, then we find $1234 \equiv 2 \pmod 7$. Moreover, by Fermat's Little Theorem 9.4.1 we have $2^6 \equiv 1 \pmod 7$, so

$$1234^{1234} \equiv 2^{1234} \equiv 2^{6\cdot 205+4} \equiv 2^4 \equiv 2 \pmod 7.$$

Remark 9.4.4. Pierre de Fermat (1601-1665) was a French magistrate who was very interested in mathematics. He is especially known for the statement that there are no nonzero integers x,y,z with $x^n+y^n=z^n$ when n is an integer greater than 2. For $n=2$ there are lots of solutions.

Fermat wrote this statement in the margin of a book and claimed to have proved it; see also Diophantus' book on Arithmetic 8.3. Although many mathematicians have tried to prove this statement, it took more than 300 years before a rigorous proof was found. In 1994, Andrew Wiles finally came up with a proof, that uses very deep and advanced mathematics. Whether Fermat really proved the statement remains unclear.

Fermat's Little Theorem 9.4.1 states that the multiplicative group $\mathbb{Z}/p\mathbb{Z}^\times$, where p is a prime, contains precisely $p-1$ elements. For arbitrary positive n, the number of elements in the multiplicative group $\mathbb{Z}/n\mathbb{Z}^\times$ is given by the so-called *Euler totient function*.

Definition 9.4.5 — Euler totient function. The Euler totient function $\Phi\colon \mathbb{N}\to\mathbb{N}$ is defined by

$$\Phi(n) = \left|\mathbb{Z}/n\mathbb{Z}^\times\right|$$

for all $n\in\mathbb{N}$ with $n>1$, and by $\Phi(1)=1$.

Example 9.4.6. Below the values of the Euler totient function are listed for all positive integers up to 20.

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
$\Phi(n)$	1	1	2	2	4	2	6	4	6	4	10	3	12	6	8	8	16	6	18	8

Table 9.6: Euler totient function

Theorem 9.4.7 — Euler Totient. The Euler totient function 9.4.5 satisfies the following properties.

(a) Suppose that n and m are positive integers. If $\gcd(n,m)=1$, then

$$\Phi(n\cdot m) = \Phi(n)\cdot\Phi(m)$$

(b) If p is a prime and n a positive integer, then

$$\Phi(p^n) = p^n - p^{n-1}$$

(c) If a is a positive integer with distinct prime divisors $p_1,\dots,p_s$ and prime factorization $a=\prod_{i=1}^{s}(p_i)^{n_i}$ then

$$\Phi(a) = \prod_{i=1}^{s} \left((p_i)^{n_i} - (p_i)^{n_i - 1} \right)$$

(d) The Euler Totient function satisfies the following recursion:

$$\Phi(1) = 1$$

and

$$\Phi(n) = n - \sum_{d \in \{d \in \mathbb{N} | d | n\}} \Phi(d).$$

Proof.

Part (a).

Suppose that n and m are two positive integers which are coprime. If a and b are two integers congruent modulo $n \cdot m$, then they are also congruent modulo n and modulo m.

Moreover, if an integer a is relatively prime to $n \cdot m$, then clearly a is also relatively prime to both n and m. Consequently, the map $F : \mathbb{Z}/n \cdot m\mathbb{Z}^\times \to \mathbb{Z}/n\mathbb{Z}^\times \times \mathbb{Z}/m\mathbb{Z}^\times$ defined by $F(a \pmod{n \cdot m}) = (a \pmod{n}, a \pmod{m})$ is well defined.

The Chinese Remainder Theorem 9.3.4 implies that for each pair $(b \pmod{n}, c \pmod{m})$ in $\mathbb{Z}/n\mathbb{Z}^\times \times \mathbb{Z}/m\mathbb{Z}^\times$ there is one and only one class $a \pmod{n \cdot m}$ of $\mathbb{Z}/n \cdot m\mathbb{Z}^\times$ which is mapped onto the pair $(b \pmod{n}, c \pmod{m})$ by F. This proves that F is a bijection. So $\mathbb{Z}/n \cdot m\mathbb{Z}^\times$ and $\mathbb{Z}/n\mathbb{Z}^\times \times \mathbb{Z}/m\mathbb{Z}^\times$ have the same number of elements. This proves that $\Phi(n \cdot m) = \Phi(n) \cdot \Phi(m)$.

Part (b).

Suppose that p is a prime and n a positive integer. The integers a which are not relatively prime to p^n are exactly the multiples of p. As there are p^{n-1} multiples of p in $\{1, \ldots, p^n\}$, we find $\Phi(p^n) = p^n - p^{n-1}$.

Part (c).

Part (c) is a direct consequence of the two other statements.

Part (d).

The first part is obvious, so we concentrate on proving the second Part.

The set $\{1, \ldots, n\}$ is the disjoint union of the sets $V(n,d) = \{m \in \{1, \ldots, n\} \mid \gcd(m,n) = d\}$ where d runs through the set of positive divisors of n (in which case also $\frac{n}{d}$ runs through the set of positive divisors of n).

For multiples m, n of d, we have $\gcd(m,n) = d$ if and only if $\gcd\left(\frac{m}{d}, \frac{n}{d}\right) = 1$. The set $V(n,d)$ therefore also equals $d \cdot V\left(\frac{n}{d}, 1\right)$.

But $|V(m,1)| = \Phi(m)$, so $V(n,d)$ contains precisely $\Phi(\frac{n}{d})$ elements. Consequently, $n = \sum_{d \in \{d \in \mathbb{N} | d | n\}} \left(\Phi(\frac{n}{d})\right) = \sum_{d \in \{d \in \mathbb{N} | d | n\}} (\Phi(d))$.

Taking apart the summand $\Phi(n)$ (occurring for $d = n$), and bringing the remaining summation to the other side, we find the required formula.

□

Example 9.4.8. By the Euler Totient Theorem 9.4.7 we find:

$$\Phi(100) = \Phi(2^2 \cdot 5^2) = \Phi(2^2) \cdot \Phi(5^2) = \left(2^2 - 2\right) \cdot \left(5^2 - 5\right) = 40.$$

Example 9.4.9. The number of invertible elements in $\mathbb{Z}/6\mathbb{Z}$ can be computed with the formula of Part (4) of the theorem:

$$\Phi(6) = 6 - \Phi(1) - \Phi(2) - \Phi(3) = 6 - 1 - 1 - 2 = 2.$$

Let n be a prime. Then $\Phi(n) = n - 1$. So, by Fermat's Little Theorem 9.4.1 we have $(a \pmod{n})^{\Phi(n)} = 1 \pmod{n}$ for all integers a that are not a multiple of n.

This statement can be generalized to arbitrary n.

Figure 9.3: Leonard Euler.

Theorem 9.4.10 — Euler's Theorem. Suppose n is an integer with $n \geq 2$. Let a be an element of $\mathbb{Z}/n\mathbb{Z}^\times$. Then $a^{\Phi(n)} = 1$.

Proof. The proof of the theorem almost literally follows the second proof of Fermat's Little Theorem 9.4.1.

Suppose a in $\mathbb{Z}/n\mathbb{Z}^\times$. Consider the map

$$M_a \colon \mathbb{Z}/n\mathbb{Z}^\times \to \mathbb{Z}/n\mathbb{Z}^\times, z \longmapsto a \cdot z$$

In other words, M_a is multiplication by a. By the Invertibility of Products 9.2.12, this map is well defined. Moreover, the map is bijective. Indeed, its inverse is given by $M_{a^{-1}}$, multiplication by a^{-1}. As a result we see that the product of all elements in $\mathbb{Z}/n\mathbb{Z}^\times$ equals not only $\prod_{z \in \mathbb{Z}/n\mathbb{Z}^\times} z$ but also $\prod_{z \in \mathbb{Z}/n\mathbb{Z}^\times} (M_a(z))$. The products are over the same set of elements. They are just taken in different order, but that does not influence the result. In other words, the products are equal. But the latter product equals $\prod_{z \in \mathbb{Z}/n\mathbb{Z}^\times} (a \cdot z) = a^{\Phi(p)} \cdot \prod_{z \in \mathbb{Z}/n\mathbb{Z}^\times} z$. By Invertibility of Products 9.2.12 the product $\prod_{z \in \mathbb{Z}/n\mathbb{Z}^\times} z$ is invertible, so, multiplying both sides of the above equation by its inverse, we find $a^{\Phi(n)} = 1$. This proves the theorem.

□

Example 9.4.11. The set $\mathbb{Z}/15\mathbb{Z}^\times$ contains 8 elements, one of them being $7 \pmod{15}$. For this element we have $7^8 \equiv 49^4 \equiv 4^4 \equiv 1^2 \equiv 1 \pmod{15}$.

This in accordance with Euler's Theorem 9.4.10.

Let n be an integer. The *order* of an element a in $\mathbb{Z}/n\mathbb{Z}^\times$ is the smallest positive integer m such that $a^m = 1$. By Euler's Theorem 9.4.10 the order of a exists and is at most $\Phi(n)$. More precise statements on the order of elements in $\mathbb{Z}/n\mathbb{Z}^\times$ can be found in the following result.

Theorem 9.4.12 — Orders. Let n be an integer greater than 1.

(a) If $a \in \mathbb{Z}/n\mathbb{Z}$ satisfies $a^m = 1$ for some positive integer m, then a is invertible and its order divides m.
(b) For all elements a in $\mathbb{Z}/n\mathbb{Z}^\times$ the order of a is a divisor of $\Phi(n)$.
(c) If $\mathbb{Z}/n\mathbb{Z}$ contains an element a of order $n-1$, then n is prime.

Proof.

Part (a).

Suppose $a \in \mathbb{Z}/n\mathbb{Z}$ satisfies $a^m = 1$ for some integer m. Then, since $a \cdot a^{m-1} = 1$, the element a is invertible with inverse a^{m-1}.

Let k be the order of a, and set $q = \operatorname{quot}(m,k)$ and $r = \operatorname{rem}(m,k)$. Then $(a \pmod n)^r$ equals $(a \pmod n))^{m-q\cdot k} = (a \pmod n))^m \cdot \left((a \pmod n))^k\right)^{-q}$, which is equal to 1. By the definition of order, the above implies that r is equal to 0, which proves the first part of the theorem.

Part (b).

The second part follows immediately from the first statement of the theorem and Euler's Theorem 9.4.10.

Part (c).

As for the last statement, $\Phi(n) = n-1$ if and only if all integers between 0 and $n-1$ have greatest common divisor 1 with n. This implies that n is prime.

□

Example 9.4.13. The element $7 \pmod{15}$ of $\mathbb{Z}/15\mathbb{Z}$ satisfies $7^4 \equiv 49^2 \equiv 4^2 \equiv 1 \pmod{15}$
Hence its order divides 8, which is the order of $\mathbb{Z}/15\mathbb{Z}^\times$.

Remark 9.4.14. Fermat's Little Theorem 9.4.1 and the Theorem on orders 9.4.12 form a basis for various prime tests. Suppose, for example, that given some large integer n one wants to decide whether n is prime. Choosing a random integer a one can check whether $a^{n-1} \equiv 1 \pmod n$.

If this is *not* the case, one can conclude that a is composite. However, when $a^{n-1} \equiv 1 \pmod n$, one is still not able to decide that n is prime, but one has at least a good chance that it is. Repeating this test a couple of times increases the probability of a correct answer to the question whether n is prime.

However, there are composite integers n, so-called *Carmichael numbers*, for which it is very likely that the test will indicate that n is prime. A Carmichael number is a composite integer n such that $a^{n-1} \equiv 1 \pmod n$ for all integers a with $\gcd(a,n) = 1$. (If $\gcd(a,n) > 1$, then $a \pmod n$ is not invertible.) The only Carmichael number less than 1000 is 561.

Definition 9.4.15. An element a from $\mathbb{Z}/p\mathbb{Z}$ is called a *primitive element* of $\mathbb{Z}/p\mathbb{Z}$ if every element of $\mathbb{Z}/p\mathbb{Z}^\times$ is a power of a.

Example 9.4.16. The element 2 is a primitive element in $\mathbb{Z}/11\mathbb{Z}^\times$. Indeed its powers are $2^1 = 2, 2^2 = 4, 2^3 = 8, 2^4 = 5, 2^5 = 10, 2^6 = 9, 2^7 = 7, 2^8 = 3, 2^9 = 6, 2^{10} = 1$. It is not primitive in $\mathbb{Z}/7\mathbb{Z}^\times$ as $2^3 = 1$ in $\mathbb{Z}/7\mathbb{Z}^\times$.

For every prime p there exist primitive elements; but we cannot say a priori which ones.

Theorem 9.4.17. For each prime p there exists a primitive element in $\mathbb{Z}/p\mathbb{Z}$.

9.5 The RSA cryptosystem

Suppose that you want to buy your favorite book or music CD at an internet book or record shop. To submit the order to the shop, you are required to supply various private data, such as your name, home address and credit card information. However, if you send this information unprotected over the internet, it can be intercepted by unreliable persons. To secure your personal data, the internet shop makes use of so-called *public-key cryptography*.

This means the following. The shop supplies every customer with a (public) function E. With this function the customer encrypts his or her personal data, denoted by data, into $E(\text{data})$. The customer then sends the encrypted message $E(\text{data})$ to the shop.

Besides the encryption function E the shop also has a (secret) decryption function D which can be used to decrypt the message $E(\text{data})$. This means that E and D have the property that $D(E(\text{data})) = \text{data}$. The idea

is that, in case one does not know D, it is hard (or almost impossible) to discover data from the encrypted message E (data). Only the trusted shop can find the personal information in data by applying D to E (data).

We discuss the RSA cryptosystem, an example of a public-key crypto system. The RSA cryptosystem (RSA stands for Rivest, Shamir, and Adleman, the three mathematicians who designed the system) is a modern cryptosystem based on modular arithmetic. The basis for the RSA cryptosystem is Euler's Theorem 9.4.10. Its security is based on the difficulty of factoring large integers.

In the RSA cryptosystem the data to be encrypted is assumed to be an integer, x say. (If the data is computer data, one may view the string of bits representing the data as the binary representation of the integer x.)

The encryption function E, which is public, makes use of two integers, the *modulus* m, which is the product of two primes, and the *encoding number* e. These two integers are usually called the *public keys*. The *secret key* is a number d, called the decoding number, which is used for the decoding function D.

Definition 9.5.1 — RSA Decription and Encryption. Suppose that p and q are distinct primes. Let $m = p \cdot q$ and d and e be two integers such that $d \cdot e \equiv 1 \pmod{(p-1)\cdot(q-1)}$.

Then the encryption function E and decryption function D of an RSA cryptosystem are defined by

- $E(x) = \text{rem}(x^e, m)$;
- $D(x) = \text{rem}(x^d, m)$.

The RSA cryptosystem enables the owner of the decryption function D to recover an encrypted message, provided the input integer x is not too large. In practice, this can easily be achieved by splitting the input for the encryption in small separated pieces and subsequently applying D and E to the individual pieces.

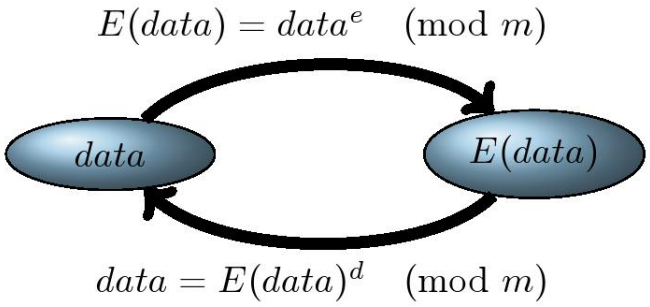


Figure 9.4: RSA.

Theorem 9.5.2 — RSA Decoding. Suppose that x is a positive integer less than both p and q. Then $D(E(x)) = x$.

Proof. Suppose that x is a positive integer less than both p and q. Then $D(E(x)) \equiv x^{d\cdot e} \pmod{m}$. By Euler's Theorem 9.4.10 we have $x^{(p-1)\cdot(q-1)} \equiv 1 \pmod{m}$. As $d \cdot e \equiv 1 \pmod{(p-1)\cdot(q-1)}$, we even have $x^{d\cdot e} \equiv x \pmod{m}$. Since x is less than both p and q, it is certainly less than m. In particular, we find x to be equal to $D(E(x))$.

□

How secure is RSA? The security of RSA depends of course on the difficulty of computing the decoding number d. To find this number it is necessary to know the two primes p and q. Once you know these primes it is a piece of cake to find d. But, as noticed in the section on Example 8.5.2, factoring the modulus $m = p \cdot q$ into p and q is an extremely time-consuming task (provided p and q are chosen sufficiently large): if one chooses two very big primes p and q, then, with current methods, it is almost impossible to find the factorization of the modulus $m = p \cdot q$.

So, at the moment, the RSA cryptosystem is believed to provide excellent security. But it remains unclear whether there exist fast methods to crack the code or not.

9.6 Exercises

Exercise 9.6.1. Show that if a and b leave the same remainder on division by n, then $a \equiv b \pmod{n}$.

Exercise 9.6.2. Show that if a and b are congruent modulo m, then a^2 and b^2 are congruent modulo m.
Give an example to show that a^2 and b^2 are not necessarily congruent modulo m^2.

Exercise 9.6.3. If a is congruent to 2 modulo 5, then to which of the integers 0, 1, 2, 3, 4 is $a^3 - 3 \cdot a + 1$ congruent?

Exercise 9.6.4. Suppose that the positive integers a and b leave remainders 3 and 4, respectively, on division by 7. Use modular arithmetic to show that $a \cdot b$ leaves remainder 5 on division by 7.

Exercise 9.6.5. Divisibility by 4 of a number which is written in the decimal system can be tested as follows: the number is divisible by 4 if and only if the number formed by the two last digits is divisible by 4.
Prove this statement.

Exercise 9.6.6. Formulate an 8-test (i.e., a test for deciding divisibility by 8) for numbers in the decimal system.
How does one decide divisibility by 8 for a binary number?

Exercise 9.6.7. Formulate a test and prove its correctness for divisibility by $a-1$ in the a-ary system.

Exercise 9.6.8. Prove that $n^4 + n^2 + 1$ is divisible by 3 if $n > 0$ is not divisible by 3.

Exercise 9.6.9. Prove the following statements:
(a) $13 | 10^6 - 1$.
(b) $17 | ((10^8) + 1)$.
(c) If $n \not\equiv 0 \pmod{5}$, then $n^4 + 64$ is not prime.
(d) The number $2^{1000} + 5$ is divisible by 3.
(e) For every $n > 0$ we find that 3 is a divisor of $2^{2 \cdot n} - 1$.

Exercise 9.6.10. Determine the multiplicative inverses of the given elements or show that this inverse does not exist.
(a) $3 \in \mathbb{Z}/37\mathbb{Z}$;
(b) $4 \in \mathbb{Z}/14\mathbb{Z}$.

Exercise 9.6.11. Fermat conjectured that numbers of the form $2^{2^n} + 1$ are prime. For $n = 5$ this conjecture does not hold. Prove, with the help of the following observations, that $641 | ((2^{2^5}) + 1)$.
(a) $641 = 2^9 + 2^7 + 1$ and so $2^7 \cdot 1 \equiv 2^7 \cdot \left(2^2 + 1\right) \equiv -1 \pmod{641}$.
(b) $2^4 \equiv -(5^4) \pmod{641}$.

Exercise 9.6.12. The binomial coefficient $\left(\begin{array}{c} p \\ k \end{array} \right)$ (pronounce: p choose k) equals $\frac{p \cdot (p-1) \cdot \ldots \cdot (p-k)}{k \cdot (k-1) \cdot \ldots \cdot 2 \cdot 1}$

If p is prime and $0 < k < p$, then the binomial coefficient $\left(\begin{array}{c} p \\ k \end{array} \right)$ is divisible by p. Prove this! In addition show that for all x and y in $\mathbb{Z}/p\mathbb{Z}$ the equality $(x+y)^p = x^p + y^p$ holds.

Exercise 9.6.13. What are the invertible elements of $\mathbb{Z}/n\mathbb{Z}$ where n is an element of $\{2, 6, 12\}$?

Exercise 9.6.14. Let p be a prime. What are the invertible elements of $\mathbb{Z}/p^2\mathbb{Z}$?

Exercise 9.6.15. Which integers are congruent to 7 modulo 17: 1734, 1127 or 1251?

Exercise 9.6.16. Which integers represent an invertible congruence class modulo 17 and which a zero divisor: 1734, 1127, 1251?

Exercise 9.6.17. Find for each of the following statements a counterexample.
If a is an invertible element in $\mathbb{Z}/n\mathbb{Z}$, and b an arbitrary nonzero element, then $a \cdot b$ is invertible.
If a and b are invertible elements in $\mathbb{Z}/n\mathbb{Z}$, then $a+b$ is invertible.
If a and b are zero divisors in $\mathbb{Z}/n\mathbb{Z}$, then $a+b$ is also a zero divisor.

Exercise 9.6.18. Let p and q be distinct primes. What are the invertible elements of $\mathbb{Z}/p \cdot q\mathbb{Z}$?

Exercise 9.6.19. Solve each of the following linear congruences:
(a) $2 \cdot x \equiv 37 \pmod{21}$
(b) $5 \cdot x \equiv 15 \pmod{25}$
(c) $3 \cdot x \equiv 7 \pmod{18}$

Exercise 9.6.20. Solve the following system of linear congruences: $2 \cdot x \equiv 37 \pmod{5}$ and $3 \cdot x \equiv 48 \pmod{7}$

Exercise 9.6.21. Solve the following system of linear congruences: $x + y \equiv 6 \pmod{11}$ and $2 \cdot x - y \equiv 8 \pmod{11}$

Exercise 9.6.22. Find the smallest positive x equal to 15 modulo 37 and 13 modulo 42.
Similarly, find the smallest positive x equal to 17 modulo 42 and 13 modulo 49.

Exercise 9.6.23. Is the converse of Fermat's Little Theorem 9.4.1,
"if $x^{p-1} \equiv 1 \pmod{p}$ for all x not equal to $0 \pmod{p}$, then p is a prime"
also true?

Exercise 9.6.24. Determine the following remainders: $\text{rem}(12312^{112311}, 7)$, $\text{rem}(13452^{5323}, 5)$ and $\text{rem}(5332^{11322}, 11)$.

Exercise 9.6.25. The hypothesis that an integer n is prime if and only if it satisfies the condition that $2^n - 2$ is divisible by n is called the "Chinese Hypothesis". Leibniz, a famous mathematician from the 17th-18th century, believed to have proved that this congruence indeed implies that n is prime. However, although this condition is necessary for n to be prime, it is not sufficient. For example, $2^{341} - 2$ is divisible by 341, but $341 = 11 \cdot 31$ is composite.
Prove that $2^{341} - 2$ is indeed divisible by 341.

Exercise 9.6.26. What value does the Euler totient function take on the integers 334, 231, and 133?

Exercise 9.6.27. How many zero divisors has $\mathbb{Z}/n\mathbb{Z}$?

Exercise 9.6.28. What is the order of $2 \pmod{35}$ in $\mathbb{Z}/35\mathbb{Z}$? And of $4 \pmod{35}$?

Exercise 9.6.29. Suppose that x is an element of order $\Phi(n)$ in $\mathbb{Z}/n\mathbb{Z}$. Then every invertible element of $\mathbb{Z}/n\mathbb{Z}$ is a power of x. Prove this!

Exercise 9.6.30. Consider the RSA cryptosystem with modulus 2623 and with encoding number $v = 37$.
If we represent the letters a, b, c, ..., z by the numbers 01, 02, ..., 26, respectively, and a space by 00, then try to decode the following text, where in each group of four figures a pair of these symbols is encoded:
0249 1133 1279 1744 0248 1188 1220 1357 1357.

Exercise 9.6.31. Consider the RSA cryptosystem with modulus 2623 and with encoding number $v = 37$.
If we represent the letters a, b, c, ..., z by the numbers 01, 02, ..., 26, respectively, and a space by 00, then how do you encode the text "math is beautiful"?

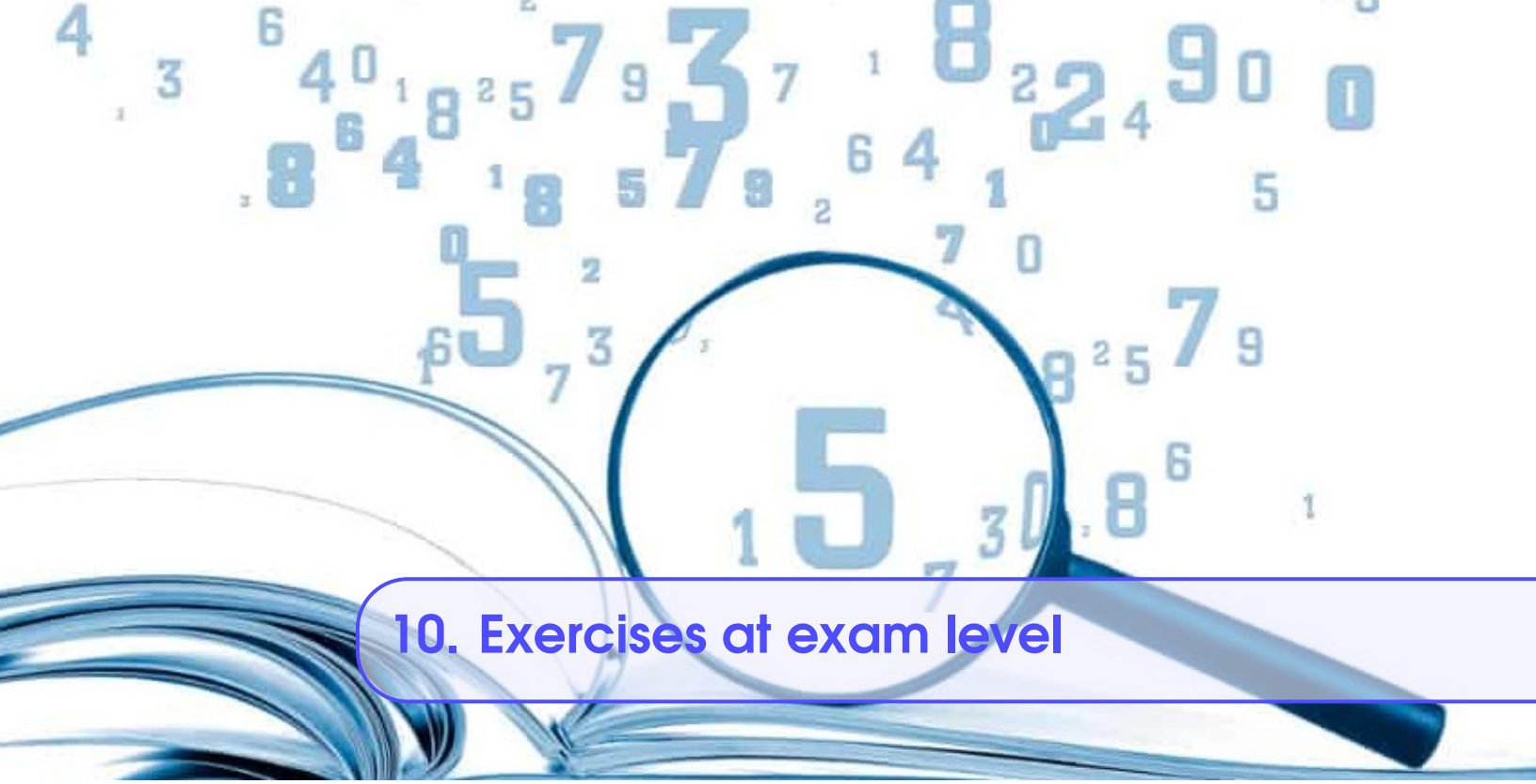
Exercise 9.6.32. In the year 46 BC Julius Caesar established the Julian calendar, which was used in the most European countries until 1582. In the Julian calendar each year contained 12 months and there were an average of 365.25 days in a year. This was achieved by having three years containing 365 days and one year containing 366 days. (In fact the first leap year was the year 8 AD).

The discrepancy between the actual length of the year, 365.24237 days, and the adopted length, 365.25 days, may not seem important but over hundreds of years the difference became obvious. The reason for this was that the seasons, which depend on the date in the tropical year, were getting progressively out of kilter with the calendar date. Pope Gregory XIII, in 1582, instituted the Gregorian calendar, which has been used since then.

Just like in the Julian Calendar the Gregorian Calendar also has ordinary years with 365 days and leap years 366 days. However the leap years are now those years x where $x \pmod 4 = 0$, except when $x \pmod{100} = 0$ and $x \pmod{400} \neq 0$. So, the year 1000 was a leap year, but the year 2000 not.

Given that January 1, 2024 will be on a Monday, find out on which day of the week the following events took place (dates are given in the Gregorian Calendar):

(a) April 2, 747: Charles the Great is born.
(b) October 12, 1492: Columbus goes on land in the Americas.
(c) July 10, 1584: Willem of Orange is killed in Delft.
(d) July 28 1914: Start of World War I.
(e) June 21, 1988: The Dutch soccer team defeats Germany with 2-1 in the semi-final of the European Championship.



10. Exercises at exam level

10.1 Logic

Exercise 10.1.1. The statements P and Q can be true or false.
When is the statement

$$R = (P \wedge Q) \vee ((\neg P \vee Q) \wedge (P \vee \neg Q))$$

true?

Solution: If P and Q are true, then $(P \wedge Q)$ and hence R is true .
If P is true and Q false, then $P \wedge Q$ and $\neg P \vee Q$ are false, so R is false.
If Q is true and P false, then $P \wedge Q$ and $P \vee \neg Q$ are false and so R is false.
If P and Q are false, then $\neg P \wedge Q$ and $P \wedge \neg Q$ are true and hence R is true.

Exercise 10.1.2. Prove or disprove:
For all statements p, q and r we have $((p \vee q) \wedge r) \Leftrightarrow ((p \wedge r) \vee (q \wedge r))$.

Solution: True, make a truth table.

Exercise 10.1.3. Prove or disprove the following statement:
for all statements P, Q and R it holds that
$[(P \Rightarrow R) \vee (P \Rightarrow Q)] \Leftrightarrow [P \Rightarrow (Q \vee R)]$.

Solution: True, make a truth table.

Exercise 10.1.4. True or false: for all statements p, q and r it holds that $((p \vee q) \wedge r) \Leftrightarrow ((p \wedge r) \vee (p \wedge q))$;

Solution: False. Take p true, q true and r false. Then $(p \vee q) \wedge r$ is false and $(p \wedge r) \vee (p \wedge q)$ true.

Exercise 10.1.5. Prove or disprove the following statement:
For all statements P and Q we have $(P \vee \neg Q) \Rightarrow \neg(Q \wedge \neg P)$. (Hint: use a truth table.)

Solution: A truth table, showing the statement is true.

P	Q	$P \vee \neg Q$	$\neg(Q \wedge \neg P)$	$(P \vee \neg Q) \Rightarrow \neg(Q \wedge \neg P)$
F	F	T	T	T
F	T	F	F	T
T	F	T	T	T
T	T	T	T	T

10.2 Sets

Exercise 10.2.1. Prove or disprove:
$(\forall x \in U[x \in (A \cap B) \Rightarrow (x \in A \vee x \in B)]) \Leftrightarrow A = B$.
(Here A and B are subsets of some universum U.)

Solution: Let $A = \{1,2\}$ and $B = \{1\}$. Then for all $x \in A \cap B$ we have $x \in A$ and then $x \in A \vee x \in B$ is true. However $A \neq B$. So the statement is false.

Exercise 10.2.2. Prove or disprove:
For all sets A, B and C we have: $A \cup (B \cap C^*) = (A \cup B) \cap C^*$.

Solution: False. Choose $A = \{1,2,3\}$, $B = \{1,4,5\}$ and $C^* = \{4,5\}$, then $A \cup (B \cap C^*) = \{1,2,3,4,5\}$ and $(A \cup B) \cap C^* = \{4,5\}$.

Exercise 10.2.3. Let A, B and C be sets. Prove that $(A \cup B) \triangle C \subseteq (A \triangle C) \cup (B \setminus A)$.

Solution: Suppose $x \in (A \cup B) \triangle C$, then $x \in A \cup B$ and $x \notin C$ or $x \in C$ and $x \notin A \cup B$. We consider both cases:
If $x \in A \cup B$ and $x \notin C$, then $x \in A$ and $x \notin C$ and hence dus $x \in A \triangle C$, or $x \notin A$ and then also $x \in B \setminus A \subseteq (A \triangle C) \cup (B \setminus A)$.
If $x \in C$ and $x \notin A \cup B$, then $x \in C$ and $x \notin A$, so $x \in A \triangle C \subseteq (A \triangle C) \cup (B \setminus A)$.
In both cases we find $x \in A \triangle C \subseteq (A \triangle C) \cup (B \setminus A)$.
This proves $(A \cup B) \triangle C \subseteq (A \triangle C) \cup (B \setminus A)$.

Exercise 10.2.4. Prove or disprove:
For all A, B and C we have $(A \cap B) \setminus C = (A \setminus C) \cap (B \setminus C)$.

Solution: Suppose $x \in (A \cap B) \setminus C$. Then $x \in A$ and $x \in B$ but not $x \in C$. So $x \in A \setminus C$ and $x \in B \setminus C$ and hence in $(A \setminus C) \cap (B \setminus C)$. This proves $(A \cap B) \setminus C \subseteq (A \setminus C) \cap (B \setminus C)$.
Now suppose $x \in (A \setminus C) \cap (B \setminus C)$. Then $x \in A \setminus C$ and $x \in B \setminus C$, so $x \in A$ and $x \in B$ but $x \notin C$. But then $x \in (A \cap B) \setminus C$. This shows $(A \cap B) \setminus C \supseteq (A \setminus C) \cap (B \setminus C)$.
We conclude $(A \cap B) \setminus C = (A \setminus C) \cap (B \setminus C)$.

Exercise 10.2.5. For all sets A, B and C we have $(A \Delta B) \cup C = (A \cup C) \Delta (B \setminus C)$. Prove this.

Solution: Let $x \in (A \Delta B) \cup C$.
If $x \in C$, then $x \in A \cup C$ and $x \notin B \setminus C$ and therefore $x \in (A \cup C) \Delta (B \setminus C)$.
If $x \notin C$, then $x \in A \Delta B$. Now we have $x \in A$ and $x \notin B$, or $x \notin A$ and $x \in B$. In the first case $x \in A \cup C$ but $x \notin B \setminus C$ and hence $x \in (A \cup C) \Delta (B \setminus C)$. In the second case $x \notin A \cup C$ but $x \in B \setminus C$ and again $x \in (A \cup C) \Delta (B \setminus C)$. This shows $(A \Delta B) \cup C \subseteq (A \cup C) \Delta (B \setminus C)$.
Now assume $x \in (A \cup C) \Delta (B \setminus C)$. If $x \in A \cup C$ and $x \notin B \setminus C$, then $x \in C$ and therefore $x \in (A \Delta B) \cup C$ or $x \notin C$ and $x \in A$ but $x \notin B \subseteq (B \setminus C) \cup C$ and hence $x \in A \Delta B \subseteq (A \Delta B) \cup C$.
If $x \notin A \cup C$ and $x \in B \setminus C$, then $x \notin A$ and $x \in B$ so $x \in A \Delta B \subseteq (A \Delta B) \cup C$.
This shows $(A \cup C) \Delta (B \setminus C) \subseteq (A \Delta B) \cup C$.
We conclude $(A \Delta B) \cup C = (A \cup C) \Delta (B \setminus C)$.

Exercise 10.2.6. Prove that for all sets A, B and C it holds that $A \cap (B \setminus C) = (A \cap B) \setminus C$.

Solution: Let $x \in A \cap (B \setminus C)$. Then $x \in A$ and $x \in B \setminus C$. So $x \in B$ and $x \notin C$. Thus $x \in A \cap B$ and $x \notin C$, hence $x \in (A \cap B) \setminus C$.

This shows that $A \cap (B \setminus C) \subseteq (A \cap B) \setminus C$.

Now assume that $x \in (A \cap B) \setminus C$. Then $x \in A$ and also $x \in B$, but not in C. So $x \in A$ and $x \in B \setminus C$ and therefore in $A \cap (B \setminus C)$. Hence $(A \cap B) \setminus C \subseteq A \cap (B \setminus C)$.

But then $A \cap (B \setminus C) = (A \cap B) \setminus C$.

Exercise 10.2.7. Prove or disprove: for all sets A, B and C it holds that: $A \cup (B \cap C) = (A \cup B) \cap C$.

Solution: False. Choose $A = \{1,2\}$, $B = \{2,3\}$ and $C = \{2\}$. Then $A \cup (B \cap C) = \{1,2\}$ and $(A \cup B) \cap C = \{2\}$.

Exercise 10.2.8. Prove or disprove the following statements:

(a) For all sets A and B it holds that, if $\mathscr{P}(A) = \mathscr{P}(B)$, then $A = B$.

(b) For all sets A, B and C it holds that $(A \cup B = A \cup C \wedge B \subseteq C) \Rightarrow A = B$.

(c) $\exists$set A $[\mathscr{P}(A) = \{A\}]$.

Solution: (a) True. If $\mathscr{P}(A) = \mathscr{P}(B)$, that means that every subset of A is also a subset of B. Since $A \in \mathscr{P}(A) = \mathscr{P}(B)$ we have that $A \subseteq B$. Similarly $B \subseteq A$, hence $A = B$.

(b) False. Suppose that $A = \{1,2\}$, $B = \emptyset$ and $C = \{2\}$. Then we have $A \cup B = \{1,2\} = A \cup C$ and $B = \emptyset \subseteq \{2\} = C$, but $A \neq B$.

(c) True, namely take $A = \emptyset$. Then $\mathscr{P}(A) = \{\emptyset\} = \{A\}$.

Exercise 10.2.9. Prove or disprove the following statement:

For all sets A, B and C we have: $A \cup (B \cap C^*) = (A \cup B) \cap C^*$.

Solution: This is false. Here is a counter example.

Let $A = \{1,2\}$, $B = \{2,3\}$ and $C = \{1,2,3\}$ in the universe $U = \{1,2,3\}$. Then $C^* = \emptyset$. We find $A \cup (B \cap C^*) = \{1,2\}$, while $(A \cup B) \cap C^* = \emptyset$.

Exercise 10.2.10. Prove $\forall m \in \mathbb{N}\ \exists n \in \mathbb{N}\ \forall k \in \mathbb{N}\ [(k > n) \Rightarrow (k^2 > m)]$.

Solution: Suppose $m \in \mathbb{N}$, then set $n = m$. Then for all $k > n$ we have $k^2 > n^2 \geq m^2 \geq m$. So for all m there is an n, namely $n = m$ such that for all $k > n$ we have $k^2 > m$.

Exercise 10.2.11. Prove that $\forall m \in \mathbb{N}\ \exists n \in \mathbb{N}\ \forall k \in \mathbb{N}\ [(k > n) \Rightarrow (\sqrt{k} > m)]$.

Solution: Suppose $m \in \mathbb{N}$, let $n = m^2$, then for $k > n$ we have $\sqrt{k} > \sqrt{n} = m$. So for all m there is an n, namely $n = m^2$ such that for all $k > n$ we have $\sqrt{k} > m$.

Exercise 10.2.12. Prove or disprove: $\forall x \in \mathbb{N}\ \exists y \in \mathbb{N}\ [x^2 - y = 0]$.

Solution: Let $x \in \mathbb{N}$, then set $y = x^2$. Now $x^2 - y = 0$. So for each $x \in \mathbb{N}$ there is a $y \in \mathbb{N}$ with $x^2 - y = 0$. The statement is true.

10.3 Relations

Exercise 10.3.1. On the set $\mathbb{Z}$ we define the relation $\equiv$ as follows Let $x, y \in \mathbb{Z}$ then

$$x \equiv y \Leftrightarrow \exists n \in \mathbb{Z}\ [x = y \cdot 10^n]$$

Prove that $\equiv$ is an equivalence relation.

Solution: A relation is an equivalence relation if it is reflexive, symmetric and transitive. We prove $\equiv$ to satisfy these conditions from which the result follows.

Reflexive. If $x \in \mathbb{Z}$ then $x = x \cdot 10^0$, so $x \equiv x$.

Symmetric.

If $x, y \in \mathbb{Z}$ and $x \equiv y$, then there is an $n \in \mathbb{Z}$ with $x = y \cdot 10^n$. But then $y = x \cdot 10^{-n}$. So $y \equiv x$.

Transitive. If $x,y,z \in \mathbb{Z}$ such that $x \equiv y$, and $y \equiv z$, then there exist $n,m \in \mathbb{Z}$ such that $x = y \cdot 10^n$ and $y = z \cdot 10^m$, so $x = z \cdot 10^{n+m}$. But then $x \equiv z$.

Exercise 10.3.2. Let R be a relation on the set X. We call R surjective if for all $y \in X$ there is an $x \in X$ with xRy. Show that R^2 is surjective if and only if R is surjective.

Solution: Suppose R is surjective. Let $z \in X$, then there is an $y \in X$ with yRz. But, again using surjectivity of R, there is also an $x \in X$ with xRy. From xRy and yRz it follows that xR^2z.

So for each $z \in X$ there is an $x \in X$ with xR^2z. Thus, the relation R^2 is surjective.

Now assume that R^2 is surjective. Let $z \in X$. Then there is an $x \in X$ with xR^2z. This means there is a $y \in X$ with xRy and yRz. In particular, for each $z \in X$ there is a $y \in X$ with yRz. So R is surjective.

We conclude R^2 is surjective if and only if R is surjective.

Exercise 10.3.3. Let R and S be relations on the set X with $R \subseteq S$. Then the transitive closure of R is contained in the transitive closure of S. Prove this.

Solution: The transitive closure of S is a transitive relation containing S and hence also R. The transitive closure of R is contained in all transitive relations containing R, and hence also in the transitive closure of S.

Exercise 10.3.4. On $V = \{(a,b) \mid a,b \in \mathbb{Z}\}$ we define the relation $\sim$ by

$$(a,b) \sim (c,d) \Leftrightarrow a - c = 2b - 2d.$$

Prove that the relation $\sim$ is an equivalence relation.

Solution: The relation $\sim$ is an equivalence relation if and only if it is reflexive, symmetric and transitive.

We use $(a,b) \sim (c,d) \Leftrightarrow a - c = 2b - 2d \Leftrightarrow a - 2b = c - 2d$.

Reflexive: Suppose $(a,b) \in V$, then $(a,b) \sim (a,b)$ since $a - 2b = a - 2b$. The relation $\sim$ is reflexive.

Symmetric: Suppose $(a,b),(c,d) \in V$ with $(a,b) \sim (c,d)$. Then $a - 2b = c - 2d$ and hence $c - 2d = a - 2b$ from which we deduce $(c,d) \sim (a,b)$. So $\sim$ is symmetric.

Transitive: Suppose $(a,b),(c,d),(e,f) \in V$ with $(a,b) \sim (c,d)$ and $(c,d) \sim (e,f)$. Then $a - 2b = c - 2d$ and $c - 2d = e - 2f$ so $a - 2b = e - 2f$. But then $(a,b) \sim (e,f)$. The relation $\sim$ is transitive.

Exercise 10.3.5. Let R and S be two relations on the set X. Prove that $R \subseteq S \Rightarrow R^2 \subseteq S^2$.

Solution: Let $x,y \in X$ with xR^2y. Then there exists a $z \in X$ with xRz and zRy. Since $R \subseteq S$, we also have xSz and xSy, and hence xS^2y.

But that implies that $R^2 \subseteq S^2$.

Exercise 10.3.6. In $\mathbb{R}$ we define a relation $\sim$ by

$$\forall x \in \mathbb{R}\ \forall y \in \mathbb{R}\ \left[x \sim y :\Leftrightarrow x - y \in \mathbb{Z}\right].$$

Prove that $\sim$ is an equivalence relation.

Solution: The relation $\sim$ is an equivalence relation if and only if it is reflexive, symmetric and transitive.

Reflexive: Suppose $x \in \mathbb{R}$, then $x \sim x$ since $x - x = 0 \in \mathbb{Z}$. So $\sim$ is reflexive.

Symmetric: Suppose $x,y \in \mathbb{R}$ and $x \sim y$. Then $x - y \in \mathbb{Z}$. But since $x - y = y - x$, we also have $y - x \in \mathbb{Z}$ and thus $y \sim x$. Hence $\sim$ is symmetric.

Transitive: Suppose $x,y,z \in \mathbb{R}$ and $x \sim y$ and $y \sim z$. Then $x - y, y - z \in \mathbb{Z}$. We have $x - z = (x - y) + (y - z) \in \mathbb{Z}$. So $x \sim z$, thus $\sim$ is transitive.

Exercise 10.3.7. (a) On the set $V = \{(a,b) \mid a,b \in \mathbb{Z}, b \neq 0\}$ we define a relation $\sim$ by

$$(a,b) \sim (c,d) \Leftrightarrow ad = bc.$$

Show that $\sim$ is an equivalence relation.

(b) The $\sim$-equivalence class of $(a,b) \in V$ is denoted by $[(a,b)]$. We define $[(a,b)] \oplus [(c,d)] = [(ad+bc, bd)]$. Show that $\oplus$ is well defined, that means that the given definition does not depend on the chosen representatives (a,b) and (c,d) in V.

Solution: (a) **Reflexive**: Suppose $(a,b) \in V$. Then $a,b \in \mathbb{Z}$, so $ab = ba$ and thus $(a,b) \sim (a,b)$. So $\sim$ is reflexive.
Symmetric: Suppose $(a,b),(c,d) \in V$ with $(a,b) \sim (c,d)$. So $ab = cd$. Therefore it also holds that $cb = da$, and thus $(c,d) \sim (a,b)$. So $\sim$ is symmetric.
Transitive: Suppose $(a,b),(c,d),(e,f) \in V$ with $(a,b) \sim (c,d)$ and $(c,d) \sim (e,f)$. So we have $ad = bc$ and $cf = de$. Since $b,d,f \neq 0$, we get that $\frac{a}{b} = \frac{c}{d}$ and $\frac{c}{d} = \frac{e}{f}$. So $\frac{a}{b} = \frac{e}{f}$, hence $af = be$. Therefore $(a,b) \sim (e,f)$ and so $\sim$ is transitive.

(b) Suppose $(e,f),(g,h) \in V$ with $(e,f) \sim (a,b)$ (so $eb = fa$) and $(g,h) \sim (c,d)$ (so $gd = hc$). Then since $(eh+fg)bd = (eb)(hd) + (gd)(fb) = (fa)(hd) + (hc)(fb) = (fh)(ad+bc)$ we get

$$[(e,f)] \oplus [(g,h)] = [(eh+fg, fh)] = [(ad+bc, bd)] = [(a,b)] \oplus [(c,d)]$$

Exercise 10.3.8. Let R be a relation on a set X. We call R injective if for each $y \in X$ there is at most one $x \in X$ with xRy. Show that R^2 is injective, if R is injective.

Solution: Suppose R is injective. Let $y \in X$. Suppose that there are elements x_1 and x_2 with $x_1 R^2 y$ and $x_2 R^2 y$. Then there exist $z_1, z_2 \in X$ with $x_i R z_i$ and $z_i R y$ for $i = 1,2$. So $z_1 R y$ and $z_2 R y$ and, because of injectivity of R, it holds that $z_1 = z_2$. But then $x_1 R z_1$ and $x_2 R z_1$, and again because of injectivity of R we find $x_1 = x_2$. So for each $y \in X$ there is at most one $x \in X$ with xR^2 and thus is R^2 injective.

10.4 Maps

Exercise 10.4.1. Consider the sets A and B and maps $f : A \to B$ and $g : B \to A$.
Prove or disprove the following statements:
(a) If $g(f(a)) = a$ for all $a \in A$, then f is injective.
(b) Als $g(f(a)) = a$ for all $a \in A$, then f surjective.

Solution: (a) If $g(f(a)) = a$ for all $a \in A$, then f is injective. Indeed, suppose $a, a' \in A$ with $f(a) = f(a')$, then $a = g(f(a)) = g(f(a')) = a'$.
(b) If $g(f(a)) = a$ for all $a \in A$, then f need **not** be surjective. Suppose $A = \{1\}$ and $B = \{1,2\}$ and $f(1) = 1$ and $g(1) = g(2) = 1$. Then f is not surjective, but for all $a \in A$ we have $g(f(a)) = a$, as $g(f(1)) = g(1) = 1$.

Exercise 10.4.2. Let $f : X \to X$ and $g : X \to X$ be maps. Prove or disprove:
(a) if $f \circ g$ is surjective, then g is surjective.
(b) if $f \circ g$ is injective, then g is injectief.

Solution: (a) False. Here is a counterexample.
Let $X = \mathbb{N} = \{0,1,2\ldots\}$ and let $g : X \to X$ be defined by $g(x) = x+1$ for all $x \in \mathbb{N}$ and $f : X \to X$ by $f(x) = x-1$ for all $x \in \mathbb{N}$ where $x > 0$ and set $f(0) = 0$. Then $f \circ g(x) = x$ for all $x \in \mathbb{N}$, whcih is clearly surjective. The map g is **not** surjective, since 0 is not in the image of g.
(b) True. Here is a proof.
Suppose $f \circ g$ is injective. Let $x, y \in X$ with $g(x) = g(y)$. Then $f \circ g(x) = f(g(x)) = f(g(y)) = f \circ g(y)$. By injectivity of $f \circ g$ we find $x = y$. So g is injective.

Exercise 10.4.3. Given is the collection $\mathscr{F}$ of all function from $\mathbb{R}$ to $\mathbb{R}$.
The relation R on $\mathscr{F}$ is defined as follows. For all $f, g \in \mathscr{F}$ it holds that

$$f \mathrm{R} g \Leftrightarrow \exists a \in \mathbb{R}\ \forall x \in \mathbb{R}\ [x > a \Rightarrow f(x) = g(x)].$$

Show that the relation R is transitive.

Solution: Let $f,g,h \in \mathscr{F}$ with $f\mathrm{R}g$ and $g\mathrm{R}h$. Then there is an $a \in \mathbb{R}$ such that for all $x \in \mathbb{R}$ with $x > a$ we have $f(x) = g(x)$. Also there is a $b \in \mathbb{R}$ such that for all $x \in \mathbb{R}$ with $x > b$ we have $g(x) = h(x)$. Thus for $c = \max(a,b)$ we have for all $x \in \mathbb{R}$ with $x > c$ that $f(x) = g(x) = h(x)$, hence $f\mathrm{R}h$. So the relation R is transitive.

Exercise 10.4.4. Suppose X is a finite set and $f : X \to X$ and $g : X \to X$ are maps. Prove or disprove the following statement: If $f \circ g$ surjective, then f is surjective.

Solution: True. Here is a proof:

Suppose $f \circ g$ is surjective. Then for every $b \in X$ there is an $a \in X$ such that $f(g(a)) = b$. Since $g(a) \in X$, we know that for every $b \in X$ there is a $c = g(a) \in X$ such that $f(c) = b$. Hence f is surjective.

Exercise 10.4.5. Investigate if the statement below is true for all sets A and B and all maps $F : A \to B$. Motivate your answer.

$$\forall A_1 \subseteq A\ \forall A_2 \subseteq A\ [F(A_1 \Delta A_2) = F(A_1)\Delta F(A_2)].$$

Here $A_1 \Delta A_2$ is the symmetric difference of A_1 and A_2.

Solution: The statement is false. For a very simple counterexample let $A = \{a_1, a_2\}$, $A_1 = \{a_1\}$, $A_2 = \{a_2\}$, $B = \{b\}$ and let F be a map that maps all elements from A to $b \in B$. Now since $A_1 \Delta A_2 = At$ we find $F(A_1 \Delta A_2) = B$, but $F(A_1)\Delta F(A_2) = \emptyset$.

Exercise 10.4.6. Let $f : V \to V$ be a map. Prove: $\forall A \subseteq V\ \forall B \subseteq V\ \left[f(f^{-1}(A) \cap B) = A \cap f(B)\right]$,
where $f^{-1}(A) = \{v \in V \mid f(v) \in A\}$.

Solution: Suppose $A, B \subseteq V$. Let $x \in f(f^{-1}(A) \cap B)$. Then $x = f(y)$ for some element $y \in f^{-1}(A) \cap B \subseteq f^{-1}(A)$ and hence in A. Moreover, as $y \in B$ we also have $x = f(y) \in f(B)$. So $x \in f(A) \cap B$. We conclude that $f(f^{-1}(A) \cap B) \subseteq A \cap f(B)$.

On the other hand, let $x \in A \cap f(B)$. The $x = f(z)$ for some $z \in B$. As $x = f(z) \in A$, we find $z \in f^{-1}(A) \cap B$ and $x \in f(f^{-1}(A) \cap B)$. This proves $f(f^{-1}(A) \cap B) \supseteq A \cap f(B)$.

From the above we can conclude that $f(f^{-1}(A) \cap B) = A \cap f(B)$.

Exercise 10.4.7. True or false: the map $f : \mathbb{R} \to \mathbb{R}$ with $f(x) = (x-1)^3$ is bijective.

Solution: True. The function $g : \mathbb{R} \to \mathbb{R}$ defined by $g(x) = \sqrt[3]{x} + 1$ is the inverse of f.

Exercise 10.4.8. Suppose X is a set and $f : X \to X$ a map. Then prove or disprove:

$$\forall y \in X\ \exists x \in X\ [f \circ f \circ f(x) = y] \Leftrightarrow f \text{ is a bijection.}$$

Solution: First of all, suppose f is a bijection. Then $\forall y \in X\ \exists x_1 \in X\ [f(x_1) = y]$. Repeating this argument gives that $\exists x_2 \in X\ [f(x_2) = x_1]$ and $\exists x_3 \in X\ [f(x_3) = x_2]$. So now $f \circ f \circ f(x_3) = f \circ f(x_2) = f(x_1) = y$. So $\forall y \in X\ \exists x \in X\ [f \circ f \circ f(x) = y]$.

Now assume $\forall y \in X\ \exists x \in X\ [f \circ f \circ f(x) = y]$. Then also $\forall y \in X\ \exists x \in X\ [f(x) = y]$, and thus f is surjective.

However, f need not be injective. Here is a counter example. Let $f : \mathbb{N} \to \mathbb{N}$ be defined by $f(n) = \max(n-1, 0)$. Then $f \circ f \circ f \circ f(n) = \max(n-3, 0)$, so $f \circ f \circ f$ is clearly surjective. However, f is not injective as $f(1) = f(0) = 0$.

Exercise 10.4.9. For sets X and Y we say X is "just as large as" Y if and only if there is a bijection from X to Y.

(a) Show that $\mathbb{N}$ is "just as large as" $\mathbb{Z}$.

(b) Prove that the relation "just as large as" is an equivalence relation.

Solution: (a) The map $f : \mathbb{N} \to \mathbb{Z}$ defined by

$$f(n) = \begin{cases} n/2 & \text{if } n \text{ is even} \\ (1-n)/2 & \text{if } n \text{ is odd} \end{cases}$$

is a bijection from $\mathbb{N}$ to $\mathbb{Z}$.

(b) The relation is an equivalence relation if it is reflexive, symmetric and transitive.
Reflexive The identity function on the space X is a bijection so X is "just as large as" X.
Symmetric Suppose X is "just as large as" Y. Then there is a bijection f from X to Y. But then f^{-1} is a bijection from y to X and thus Y is "just as large as" X.
Transitive: Suppose X is "just as large as" Y and Y is "just as large as" Z. Then there is a bijection f from X to Y and a bijection g from Y to Z. But then $g \circ f$ is a bijection from X to Z and thus X is "just as large as" Z.

Exercise 10.4.10. Suppose f and g are maps such that $f \circ g$ is a bijection.
Prove the following statements or give a counterexample:
(a) g is injective.
(b) f is bijective.

Solution: (a) The statement is true. We prove by contradiction. Suppose g is not injective. Then there exist $x \neq y$ such that $g(x) = g(y)$. But then also $f(g(x)) = f(g(y))$ and thus $(f \circ g)(x) = (f \circ g)(y)$. So $f \circ g$ is not injective, which is in contradiction with the fact that $f \circ b$ is a bijection.
(b) This statement is not true. The function f does not need to be injective. It can map two elements which are not in the range of g to the same element.

Exercise 10.4.11. Let $f : X \to Y$ be a map. Then by $\hat{f}$ we denote the map from $\mathscr{P}(X)$ to $\mathscr{P}(Y)$, which for each subset S of X is defined by

$$\hat{f}(S) = \{f(x) \mid x \in S\}.$$

Prove that f is surjective if and only if $\hat{f}$ is surjective.

Solution: Let f be surjective and suppose Y_0 is a subset of Y. Then let X_0 be the subset $\{x \in X \mid f(x) \in Y_0\}$ of X. Then $\hat{f}(X_0) \subseteq Y_0$, and as, by surjectivity of f there is for each element $y \in Y_0$ an element $x \in X$ with $f(x) = y$, we even find $x \in X_0$. Hence $\hat{f}(X_0) = Y_0$. This proves $\hat{f}$ to be surjective.

Now assume that $\hat{f}$ is surjective and let $y \in Y$ and set $Y_1 = \{y\}$. Then there is a subset $X_1 \subseteq X$ with $\hat{f}(X_1) = Y_1$. In particular, there is an $x \in X_1$ with $f(x) = y$. This proves surjectivity of f.

So, f is surjective if and only if $\hat{f}$ is surjective.

Exercise 10.4.12. On the set $\mathscr{F}$ of all functions from $\mathbb{R}$ to $\mathbb{R}$ we define the relation $\equiv$ in the following way:

$$f \equiv g \Leftrightarrow \exists \varepsilon > 0 \; \forall x \in \mathbb{R} \; [|x| \leq \varepsilon \Rightarrow f(x) = g(x)].$$

Prove that $\equiv$ is an equivalence relation.

Solution: We prove that $\equiv$ is reflexive, symmetric and transitive.

Reflexive: $f \equiv f$ since for $\varepsilon = 1$ we have for all x that $|x| \leq \varepsilon \Rightarrow f(x) = f(x)$.

Symmetry: suppose $f \equiv g$, then there is an $\varepsilon > 0$ such that for all x that $|x| \leq \varepsilon \Rightarrow f(x) = g(x)$ and then also $|x| \leq \varepsilon \Rightarrow g(x) = f(x)$, implying $g \equiv f$.

Transitive: suppose $f \equiv g$ and $g \equiv h$, then there is an $\varepsilon_1 > 0$ such that for all x that $|x| \leq \varepsilon_1 \Rightarrow f(x) = g(x)$ and there is an $\varepsilon_2 > 0$ such that for all x that $|x| \leq \varepsilon_2 \Rightarrow g(x) = h(x)$.

For $\varepsilon = \min(\varepsilon_1, \varepsilon_2)$ we have for all x that $|x| \leq \varepsilon \Rightarrow f(x) = g(x) = h(x)$. So $f \equiv h$.

The relation is an equivalence relation.

Exercise 10.4.13. The permutation $\pi \in \mathrm{Sym}_7$ is given by the matrix:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 4 & 1 & 5 & 7 & 2 & 6 \end{pmatrix}.$$

(a) Write π as a product of disjoint cycles and determine its sign.
(b) Does there exist a $\sigma \in \mathrm{Sym}_7$ with $\sigma\pi\sigma^{-1}$ equal to $(7,6)(5,4,3,2,1)$?
Or to $(1,2,3)(4,5,6,7)$? If so, find such a σ. If not, explain why.

Solution: (a) $\pi = (1,3)(2,4,5,7,6)$, and has sign $-1 \cdot 1 = -1$.

(b) Let $\sigma = \begin{pmatrix} 1 & 3 & 2 & 4 & 5 & 7 & 6 \\ 7 & 6 & 5 & 4 & 3 & 2 & 1 \end{pmatrix}$, then $\sigma\pi\sigma^{-1} = (7,6)(5,4,3,2,1)$.
For $(1,2,3)(4,5,6,7)$ there is no σ, since π and $(1,2,3)(4,5,6,7)$ have different cycle structures.

Exercise 10.4.14. Prove $\forall n \in \mathbb{N}\ \forall \sigma \in \mathrm{Sym}_n\ \forall_{\tau \in \mathrm{Sym}_n} \exists \rho \in \mathrm{Sym}_n\ [\tau \circ \rho = \sigma]$.

Solution: Suppose $n \in \mathbb{N}$, then for all $\sigma \in \mathrm{Sym}_n$ and $\tau \in \mathrm{Sym}_n$ we can find a $\rho \in \mathrm{Sym}_n$, namely $\rho = \tau^{-1} \circ \sigma$ with $\tau \cdot \rho = \tau \circ \tau^{-1} \circ \sigma = \sigma$.

Exercise 10.4.15. On $\mathrm{Sym}(n)$ we define the relation $\equiv$ by $\sigma \equiv \tau$ if and only if

$$\exists \rho \in \mathrm{Sym}(n)\ [\rho\sigma\rho^{-1}\tau^{-1} = \varepsilon].$$

Here ε is the identity in $\mathrm{Sym}(n)$.

(a) Prove $\equiv$ to be an equivalence relation.

(b) Suppose $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 4 & 6 & 5 & 3 & 1 & 8 & 9 & 7 \end{pmatrix}$ and $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 3 & 1 & 5 & 6 & 7 & 8 & 9 & 4 \end{pmatrix}$ are elements of Sym_9.
Does it hold that $\sigma \equiv \tau$ in Sym_9 ? If so, give a $\rho \in \mathrm{Sym}_9$ with $\rho\sigma = \tau\rho$. If not, explain why not.

(c) Prove that for each $\sigma \in \mathrm{Sym}_n$ we have $\sigma \equiv \sigma^{-1}$.

(d) Let K be the $\equiv$-equivalence class of an element $\sigma \in \mathrm{Sym}_n$. If K contains an odd number of elements, then the order of σ is at most 2. Prove this.

(e) What are the different $\equiv$-equivalence classes of Sym_3?

Solution: (a) We prove $\equiv$ to be reflexive, symmetric and transitive.
Reflexive: Let $\sigma \in \mathrm{Sym}_n$, then with $\rho = \varepsilon$. we have $\rho\sigma\rho^{-1}\tau^{-1} = \sigma\sigma^{-1} = \varepsilon$. So $\sigma \equiv \sigma$.
Symmetric: Suppose $\sigma \equiv \tau$, then there is a ρ with $\rho\sigma\rho^{-1}\tau^{-1} = \varepsilon$. But then also $(\rho\sigma\rho^{-1}\tau^{-1})^{-1} = \tau\rho\sigma^{-1}\rho^{-1} = \varepsilon$ and hence $\rho^{-1}\tau\rho\sigma^{-1} = \rho^{-1}\varepsilon\rho = \varepsilon$ and $(\rho^{-1})\tau(\rho^{-1})^{-1}\sigma^{-1} = \varepsilon$. So $\tau \equiv \sigma$.
Transitive Suppose $\mu \equiv \sigma$ and $\sigma \equiv \tau$, Then there are ρ and ϕ with $\rho\mu\rho^{-1}\sigma^{-1} = \varepsilon$ and $\phi\sigma\phi^{-1}\tau^{-1} = \varepsilon$. So $\sigma\phi^{-1}\tau^{-1} = \phi^{-1}$ and $\rho\mu\rho^{-1}\sigma^{-1}\sigma\phi^{-1}\tau^{-1} = \phi^{-1}$. This means $(\phi\rho)\mu(\phi\rho)^{-1}\tau^{-1} = \varepsilon$. So $\mu \equiv \tau$.

A different approach: By definition we have $\sigma \equiv \tau$ if and only if $\tau = \rho\sigma\rho^{-1}$ for some ρ, so, if and only if σ is geconjugated with τ. Being conjugated is an equivalence relation, and hence so is $\equiv$.

(b) Yes, $\sigma \equiv \tau$ holds. Because we can write $\sigma = (1,2,4,5,3,6)(7,8,9)$ and $\tau = (4,5,6,7,8,9)(1,2,3)$, we can use

$$\rho = \begin{pmatrix} 1 & 2 & 4 & 5 & 3 & 6 & 7 & 8 & 9 \\ 4 & 5 & 6 & 7 & 8 & 9 & 1 & 2 & 3 \end{pmatrix}$$

which can also be written as $\rho = (1,4,6,9,3,8,2,5,7)$.

(c) For each σ we have σ and σ^{-1} have the same cycle structure. So $\sigma \equiv \sigma^{-1}$.

(d) For each $\sigma \in K$ we find σ^{-1} also in K. As $(\sigma^{-1})^{-1} = \sigma$, we find K to have an even number of elements, unless there is a $\sigma \in K$ with $\sigma^{-1} = \sigma$. But then $\sigma^2 = \sigma \cdot \sigma^{-1} = 1$, and σ has order at most 2.

(e) The 6 possible permutations in Sym_3 are in cycle notation: *Id*, (1,2), (1,3), (2,3), (1,2,3) and (1,3,2). Since $(2,3) \cdot (1,3) = (1,2) \cdot (2,3)$ and $(1,3) \cdot (2,3) = (1,2) \cdot (1,3)$ we have $(1,2) \equiv (1,3) \equiv (2,3)$. Also since $(1,2) \cdot (1,3,2) = (1,2,3) \cdot (1,2)$ we have $(1,2,3) \equiv (1,3,2)$. Note that these last permutations are not equivalent tot the first ones, and also *Id* is not equivalent to any of the above permutations. So there are three equivalence classes in Sym_3.

Exercise 10.4.16. The permutation $\pi \in \mathrm{Sym}_7$ is given by the following matrix:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 1 & 4 & 5 & 7 & 3 & 6 \end{pmatrix}.$$

(a) Write π as a product of disjunct cycles and determine the sign of π.

(b) Determine π^{-1} and the sign of π^{-1}.

(c) Determine a $\sigma \in \mathrm{Sym}_7$ with $\sigma\pi\sigma^{-1}$ equal to π^{-1}.

Solution: (a) $\pi = (1,3)(3,4,5,7,6)$, and has sign -1.
(b) $\pi^{-1} = (1,3)(3,6,7,5,4)$ and also has sign -1.
(c) $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 7 & 6 \\ 1 & 2 & 3 & 6 & 7 & 5 & 4 \end{pmatrix}$ or in cycle notation $\sigma = (1)(2)(3)(4,6)(5,7)$.

Exercise 10.4.17. The permutation $\pi \in \mathrm{Sym}_7$ is given by the following matrix:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 1 & 2 & 5 & 7 & 4 & 6 \end{pmatrix}.$$

(a) Write π as a product of disjunct cycles and determine the sign of π.
(b) Is there a $\sigma \in \mathrm{Sym}_7$ with $\sigma\pi\sigma^{-1}$ equal to $(7,6)(5,4,3,2,1)$?
Or $(1,2,3)(4,5,6,7)$? If so, determine a σ, if not, explain why not.

Solution: (a) $\pi = (1,3,2)(4,5,7,6)$ with sign $+1$.
(b) For $(7,6)(5,4,3,2,1)$ there is no σ, since π and $(7,6)(5,4,3,2,1)$ have different cycle structures. As for $(1,2,3)(4,5,6,7)$, let

$$\sigma = \begin{pmatrix} 1 & 3 & 2 & 4 & 5 & 7 & 6 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 \end{pmatrix}$$

then $\sigma\pi\sigma^{-1} = (1,2,3)(4,5,6,7)$.

Exercise 10.4.18. The permutation $\pi \in \mathrm{Sym}_7$ is given by the following matrix:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 1 & 2 & 5 & 6 & 7 & 4 & 9 & 8 \end{pmatrix}.$$

(a) Write π as a product of disjunct cycles and determine the sign of π.
(b) What is the order of π? Explain your answer.

Solution: (a) $\pi = (1,3,2)(4,5,6,7)(8,9)$, and thus has sign $1 \cdot -1 \cdot -1 = 1$.
(b) The order of π is the least common multiple of the cycle lengths, so $\mathrm{lcm}(3,4,2) = 12$.

Exercise 10.4.19. A subset G of Sym_n is called a subgroup of Sym_n if it holds that:
- Id, the identity, is an element of G;
- if $\sigma, \tau \in G$, then also σ^{-1} and $\sigma\tau \in G$.

(a) Prove that Alt_n, the subset of all even permutations, is a subgroup of Sym_n.
(b) Prove that $\{\sigma \in \mathrm{Sym}_n \mid \sigma(1) = 1\}$ is a subgroup of Sym_n.
(c) Suppose G and H are subgroups of Sym_n. Prove that $G \cap H$ is also a subgroup of Sym_n, or give a counterexample.

Solution: (a) The identity is an even permutation, and thus contained in Alt_n. Also, if $\sigma, \tau \in \mathrm{Alt}_n$ then they are both even permutations. Since σ is even, σ^{-1} is also even. Also, since both σ and τ have an even number of 2-cycles, the combination $\sigma\tau$ also has an even number of 2-cycles. So indeed, Alt_n is a subgroup of Sym_n.
(b) We will write $G = \{\sigma \in \mathrm{Sym}_n \mid \sigma(1) = 1\}$. Clearly $\mathrm{Id} \in G$, since it fixes all elements including 1. Now suppose that $\sigma, \tau \in G$, then $\sigma(1) = 1$ and $\tau(1) = 1$. Therefore we also have $\sigma^{-1}(1) = \sigma^{-1}(\sigma(1)) = 1$, hence $\sigma^{-1} \in G$. Also $\sigma\tau(1) = \sigma(\tau(1)) = \sigma(1) = 1$, hence $\sigma\tau \in G$. So G is a subgroup of Sym_n.
(c) Since G and H are both subgroups of Sym_n, they both contain the identity. Thus $G \cap H$ also contains the identity. Also, if $\sigma, \tau \in G \cap H$, then $\sigma, \tau \in G$ and $\sigma, \tau \in H$, so since they are subgroups of Sym_n we know that they both contain σ^{-1} and $\sigma\tau$. So $\sigma^{-1}, \sigma\tau \in G \cap H$. Therefore $G \cap H$ is also a subgroup of Sym_n.

Exercise 10.4.20. Suppose $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 4 & 6 & 5 & 3 & 1 & 8 & 9 & 7 \end{pmatrix}$ and $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 3 & 1 & 5 & 6 & 7 & 8 & 9 & 4 \end{pmatrix}$.

(a) Write σ and τ as a product of disjunct cycles and determine the sign of σ and τ.
(b) Does there exist a ρ with $\rho\sigma = \tau\rho$? If so, give such a ρ. If not, explain why not.

Solution: (a) $\sigma = (1,2,4,5,3,6)(7,8,9)$ with sign -1 and $\tau = (1,2,3)(4,5,6,7,8,9)$ with sign -1.
(b) Yes, namely

$$\rho = \begin{pmatrix} 1 & 2 & 4 & 5 & 3 & 6 & 7 & 8 & 9 \\ 4 & 5 & 6 & 7 & 8 & 9 & 1 & 2 & 3 \end{pmatrix}$$

or in cycle notation $\rho = (1,4,6,9,3,8,2,5,7)$.

10.5 Orders

Exercise 10.5.1. Let $\sqsubseteq$ be an order (so, a reflexive, anti-symmetric and transitive relation) on the set X. Let $x, y \in X$. An element $z \in X$ with

$$z \sqsubseteq x, y$$

and

$$\forall u \in X \left[(u \sqsubseteq x \ \wedge \ u \sqsubseteq y) \Rightarrow u \sqsubseteq z\right]$$

is called a largest lowerbound of x and y.
(a) Suppose $x, y \in X$. Prove that there is at most one largest lowerbound of x and y. (which we denote by $x \sqcap y$.)
(b) Let $x, y, z \in X$. Assume $x \sqcap z$ and $y \sqcap z$ to exist. Prove $x \sqsubseteq y \Rightarrow x \sqcap z \sqsubseteq y \sqcap z$.

Solution: (a) Let $x, y \in X$ and assume that z_1 and z_2 are largest lower bounds of x and y. Then $z_1 \sqsubseteq x$ and $z_1 \sqsubseteq y$. As z_2 is a largest lower bound, we find $z_1 \sqsubseteq z_2$.
Similarly we find $z_2 \sqsubseteq z_1$.
By anti-symmetry of $\sqsubseteq$ we have $z_1 = z_2$. We conclude that there is at most one largest lower bound of x, y.
(b) Let $x, y, z \in X$. Assume $x \sqsubseteq y$ and that $x \sqcap z$ and $y \sqcap z$ exist.
We have $x \sqcap z \sqsubseteq x$ and $x \sqsubseteq y$, and then by transitivity of $\sqsubseteq$ also $x \sqcap z \sqsubseteq y$. Moreover $x \sqcap z \sqsubseteq z$. But then $x \sqcap z \sqsubseteq y \sqcap z$.

Exercise 10.5.2. Let both $\sqsubseteq_1$ and $\sqsubseteq_2$ be partial orders on a set X. Then their intersection $\sqsubseteq$ defined by

$$\forall x, y \in X [x \sqsubseteq y \Leftrightarrow (x \sqsubseteq_1 y \wedge x \sqsubseteq_2 y)]$$

is again a partial order.
Prove this.

Solution: We prove that $\sqsubseteq$ is reflexive, antisymmetric and transitive.
Let $x, y, z \in X$.
By reflectiveness of $\sqsubseteq_1$ and $\sqsubseteq_2$, we have $x \sqsubseteq_1 x$ and $x \sqsubseteq_2 x$, so $x \sqsubseteq x$. Thus $\sqsubseteq$ is reflexive.
Suppose $x \sqsubseteq y$ and $y \sqsubseteq x$. Then $x \sqsubseteq_1 y$ (and $x \sqsubseteq_2 y$) and $y \sqsubseteq_1 x$ (and $y \sqsubseteq_2 x$).
By antisymmetry of $\sqsubseteq_1$ (and $\sqsubseteq_2$) we find $x = y$. So, $\sqsubseteq$ is antisymmetric.
Now suppose $x \sqsubseteq y$ and $y \sqsubseteq z$. Then $x \sqsubseteq_1 y$ and $y \sqsubseteq_1 z$, and by transitivity of $\sqsubseteq_1$ we also have $x \sqsubseteq_1 z$.
We also have $x \sqsubseteq_2 y$ and $y \sqsubseteq_2 z$, and then, by transitivity of $\sqsubseteq_2$, we also have $x \sqsubseteq_2 z$. Thus $x \sqsubseteq z$. This shows transitivity of $\sqsubseteq$.
We can conclude that $\sqsubseteq$ is a partial order.

Exercise 10.5.3. Let $\mathscr{F}$ be the set of all functions from $\mathbb{R}$ to $\mathbb{R}$. The relation $\sqsubseteq$ on $\mathscr{F}$ is defined as follows. For $f, g \in \mathscr{F}$ it holds that:

$$f \sqsubseteq g \Leftrightarrow \exists \varepsilon > 0 \ \forall x \in \mathbb{R} \ [|x| < \varepsilon \Rightarrow f(x) \leq g(x)].$$

Prove that $\sqsubseteq$ is reflexive and transitive.
Is it also an order?

Solution:

Reflexive: Since for all $x \in \mathbb{R}$ it holds $f(x) \leq f(x)$, it holds that $f \sqsubseteq f$.

Transitive: Let $f \sqsubseteq g$ and $g \sqsubseteq h$. Then $\exists_{\varepsilon_1} \forall_{x \in \mathbb{R}} [|x| < \varepsilon_1 \Rightarrow f(x) \leq g(x)]$ and $\exists_{\varepsilon_2} \forall_{x \in \mathbb{R}} [|x| < \varepsilon_2 \Rightarrow g(x) \leq h(x)]$. Now for $\varepsilon = \min(\varepsilon_1, \varepsilon_2)$ we have $|x| < \varepsilon \Rightarrow f(x) \leq g(x) \leq h(x)$, and thus $f \sqsubseteq h$.

The relation $\sqsubseteq$ is not an order. Take the function f with $f(x) = 0$ for all x and the function g with

$$g(x) = \begin{cases} 0 & \text{if } |x| < 1 \\ 1 & \text{else.} \end{cases}$$

Then $f \sqsubseteq g$ and $g \sqsubseteq f$, but $f \neq g$.

10.6 Recursion and induction

Exercise 10.6.1. Prove by natural induction that for $n \geq 3$ we have

$$\sum_{k=1}^{n} \frac{1}{\sqrt{k}} > \sqrt{n+1}.$$

Solution: Let $P(n)$ be the above statement. For $n = 3$ we use that $\sqrt{2} < \sqrt{3} < 2$ and hence $\sum < 1 + \frac{1}{2} + \frac{1}{2} = 2 = \sqrt{3+1}$. So, $P(3)$ is true. Now $P(n-1) \Rightarrow P(n)$. So suppose $P(n-1)$ holds. Then

$$\sum_{k=1}^{n} \frac{1}{\sqrt{k}} = \sum_{k=1}^{n-1} \frac{1}{\sqrt{k}} + \frac{1}{\sqrt{n}} > \sqrt{n} + \frac{1}{\sqrt{n}} = \sqrt{n + 2 + \frac{1}{n}} > \sqrt{n+1}.$$

Thus by induction the statement $P(n)$ is true for all $n \geq 3$.

Exercise 10.6.2. Prove by induction that for all $n \in \mathbb{N}$ we have $\sum_{i=1}^{n} i^2 < \frac{1}{3}(n+1)^3$.

Solution: We provide a proof by induction.

Basis: For $n = 1$ we have $\sum_{i=1}^{n} i^2 = 1 < \frac{8}{3} = \frac{1}{3}2^3 = \frac{1}{3}(n+1)^3$.

Step: Assume for some $k \in \mathbb{N}$ we have $\sum_{i=1}^{k} i^2 < \frac{1}{3}(k+1)^3$. Then for $n = k+1$ we find

$$\begin{array}{ll} \sum_{i=1}^{n} i^2 & = (\sum_{i=1}^{k} i^2) + (k+1)^2 \\ \text{by assumption} & < \frac{1}{3}(k+1)^3 + (k+1)^2 \\ & = \frac{1}{3}(n^3 + 3n^2) \\ & < \frac{1}{3}(n^3 + 3n^2 + 3n + 1) \\ & = \frac{1}{3}(n+1)^3. \end{array}$$

.

Conclusion: Using Natural Induction we have shown that $\sum_{i=1}^{n} i^2 < \frac{1}{3}(n+1)^3$ for all $n \in \mathbb{N}$.

Exercise 10.6.3. Prove that for all $n \in \mathbb{N}$ with $n > 3$ we have $2^n < n!$.

Solution: We use induction to prove that for all $n \in \mathbb{N}$ with $n > 3$ we have $2^n < n!$.

Basis: For $n = 4$ we have $2^4 = 16 < 24 = 4!$.

Induction step: Suppose for some $k \in N$, with $k > 3$, we have $2^k < k!$. Then for $n = k+1$ it holds that

$$\begin{array}{ll} 2^n & = 2^{k+1} \\ & = 2 \cdot 2^k \\ \text{by assumption} & < 2 \cdot k! \\ & < (k+1) \cdot k! \\ & = n! \end{array}$$

Conclusion: By induction it follows that for all $n \in \mathbb{N}$ with $n > 3$ it holds that $2^n < n!$.

Exercise 10.6.4. Use induction to prove that for all $n \geq 2$ we have

$$\prod_{i=2}^{n}(i-\frac{1}{i}) = \frac{(n+1)!}{2n}.$$

Solution: We use induction to prove that

$$\prod_{i=2}^{n}(i-\frac{1}{i}) = \frac{(n+1)!}{2n}.$$

Basis: For $n = 2$

$$\prod_{i=2}^{n}(i-\frac{1}{i}) = 2-\frac{1}{2} = \frac{6}{4} = \frac{(2+1)!}{2\cdot 2} = \frac{(n+1)!}{2n}.$$

Step: Now assume that for $n = k \geq 2$ we have

$$\prod_{i=2}^{n}(i-\frac{1}{i}) = \frac{(n+1)!}{2n}.$$

Then for $n = k+1$ it follows that

$$\begin{aligned}
\prod_{i=2}^{n}(i-\frac{1}{i}) &= \prod_{i=2}^{k+1}(i-\frac{1}{i}) \\
&= \prod_{i=2}^{k}(i-\frac{1}{i})\cdot(k+1-\frac{1}{k+1}) \\
\text{by assumption} \quad &= \tfrac{(k+1)!}{2k}\cdot(k+1-\tfrac{1}{k+1}) \\
&= \tfrac{(k+1)!}{2k}\cdot\tfrac{(k+1)^2-1}{k+1} \\
&= \tfrac{(k+1)!}{2k}\cdot\tfrac{k(k+2)}{k+1} \\
&= \tfrac{(k+2)!}{2(k+1)} \\
&= \tfrac{(n+1)!}{2n}.
\end{aligned}$$

Conclusion: So, for all $n \geq 2$ we find

$$\prod_{i=2}^{n}(i-\frac{1}{i}) = \frac{(n+1)!}{2n}.$$

Exercise 10.6.5. Prove that for all $n \in \mathbb{N}$ with $n > 1$ it holds that $\sum_{i=1}^{n} \frac{1}{i^2} < 2 - \frac{1}{n}$.

Solution: We provide a proof by induction.
For $n = 2$ we have $\sum_{i=1}^{n} \frac{1}{i^2} = 1 + \frac{1}{4} < 2 - \frac{1}{2}$.
Now assume for $n = k$ we have $\sum_{i=1}^{k} \frac{1}{i^2} < 2 - \frac{1}{k}$. Then for $n = k+1$ we find

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

By our assumption we find

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

So, by induction we find that for all $n > 1$ we have $\sum_{i=1}^{n} \frac{1}{i^2} < 2 - \frac{1}{n}$ for all $n \geq 2$.

Exercise 10.6.6. Binary trees are graphs with a special point, called the root. They can be defined as follows:

- The graph consisting of a single point r is a binary tree with root r.
- If $T_1 = (V_1, E_1)$ and $T_2 = (V_2, E_2)$ binary are binary trees with roots $r_1 \in V_1$ and $r_2 \in V_2$ and $V_1 \cap V_2 = \emptyset$, then for $r \notin V_1 \cup V_2$ the graph $T = (V_1 \cup V_2 \cup \{r\}, E_1 \cup E_2 \cup \{\{r, r_1\}, \{r, r_2\}\})$ is a binary tree with root r.

Use this recursive definition to prove that binary trees have an even number of edges.

Solution: The graph consisting of a single vertex has an even number of edges.

If $T_1 = (V_1, E_1)$ and $T_2 = (V_2, E_2)$ are binary trees with roots $r_1 \in V_1$ and $r_2 \in V_2$, and an even number of edges, then for $r \notin V_1 \cup V_2$ the graph $T = (V_1 \cup V_2 \cup \{r\}, E_1 \cup E_2 \cup \{\{r, r_1\}, \{r, r_2\}\})$ is a binary tree with root r. The number of edges of T equals $2 + |E_1| + |E_2|$, whic is again even.

So, structural induction yields that the number of edges in any binary tree is even.

Exercise 10.6.7. Binary trees are graphs with a special point, called the root. They can be defined as follows:

- The graph consisting of a single point r is a binary tree with root r.
- If $T_1 = (V_1, E_1)$ and $T_2 = (V_2, E_2)$ are binary trees with roots $r_1 \in V_1$ and $r_2 \in V_2$, and disjoint vertex sets, then for $r \notin V_1 \cup V_2$ the graph $T = (V_1 \cup V_2 \cup \{r\}, E_1 \cup E_2 \cup \{\{r, r_1\}, \{r, r_2\}\})$ is a binary tree with root r.

A leaf of a binary tree T is a point which is on at most one edge.

Use structural induction to prove that in a binary tree $T = (V, E)$ the number of leafs equals $(|V| + 1)/2$.

Solution: The graph with a single vertex is a binary tree. It has one leaf. So the nuber of leafs equals $(|V| + 1)/2$.

Assume that $T_1 = (V_1, E_1)$ and $T_2 = (V_2, E_2)$ are two trees with roots r_1 and r_2, and $V_1 \cap V_2 = \emptyset$ and having $(|V_1| + 1)/2$ and $(|V_2| + 1)/2$ leafs, respectively.

Let r be a point not in $V_1 \cup V_2$. Then $T = (V, E)$, where $V = V_1 \cup V_2 \cup \{r\}$ and E consists of $E_1 \cup E_2$ and the two edges $\{r, r_1\}$ and $\{r, r_2\}$ is also a binary tree.

The number of leafs of T equals the number of leafs in T_1 plus the number of leafs in T_2 and hence equals $(|V_1| + 1)/2 + (|V_2| + 1)/2 = (|V_1| + |V_2| + 1 + 1)/2 = (|V| + 1)/2$.

So, structural induction proves that in every binary tree $T = (V, E)$ we find $(|V| + 1)/2$ leafs.

Exercise 10.6.8. The Fibonnaci numbers are defined recursively gedefinieerd: $F_1 = 1$, $F_2 = 1$ and $F_{n+2} = F_{n+1} + F_n$ for $n \geq 1$.

Prove by induction that

$$\begin{pmatrix} F_{n+2} \\ F_{n+1} \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^n \begin{pmatrix} F_2 \\ F_1 \end{pmatrix}.$$

Solution: We provide a proof by induction.

For $n = 1$ we have

$$\begin{pmatrix} F_{n+2} \\ F_{n+1} \end{pmatrix} = \begin{pmatrix} F_3 \\ F_2 \end{pmatrix} = \begin{pmatrix} F_2 + F_1 \\ F_2 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} F_2 \\ F_1 \end{pmatrix}.$$

Now suppose that for some n we have

$$\begin{pmatrix} F_{n+2} \\ F_{n+1} \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^n \begin{pmatrix} F_2 \\ F_1 \end{pmatrix}.$$

Then we find for $n + 1$ that

$$\begin{pmatrix} F_{n+1+2} \\ F_{n+1+1} \end{pmatrix} = \begin{pmatrix} F_{n+2} + F_{n+1} \\ F_{n+1} \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} F_{n+2} \\ F_{n+1} \end{pmatrix}.$$

Using our assumption we get

$$\begin{pmatrix} F_{n+1+2} \\ F_{n+1+1} \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} F_{n+2} \\ F_{n+1} \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^n \begin{pmatrix} F_2 \\ F_1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^{n+1} \begin{pmatrix} F_2 \\ F_1 \end{pmatrix}.$$

So, by inductie we have proven that for all $n \in \mathbb{N}$ we have

$$\begin{pmatrix} F_{n+2} \\ F_{n+1} \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^n \begin{pmatrix} F_2 \\ F_1 \end{pmatrix}.$$

Exercise 10.6.9. Prove with induction that for all $n \in \mathbb{N}$ it holds that $\prod_{i=2}^{n} \frac{i}{i^2-1} = \frac{2n}{(n+1)!}$.

Solution: For $n = 2$

$$\prod_{i=2}^{n} \frac{i}{i^2-1} = \frac{2}{4-1} = \frac{2}{3} = \frac{4}{6} = \frac{2 \cdot 2}{(2+1)!} = \frac{2n}{(n+1)!}.$$

Now assume that for $n = k \geq 2$ we have

$$\prod_{i=2}^{n} \frac{i}{i^2-1} = \frac{2n}{(n+1)!}.$$

Then for $n = k+1$ it follows that

$$\begin{aligned} \prod_{i=2}^{n} \frac{i}{i^2-1} &= \prod_{i=2}^{k+1} \frac{i}{i^2-1} \\ &= \frac{k+1}{(k+1)^2-1} \cdot \prod_{i=2}^{k} \frac{i}{i^2-1} \\ &= \frac{k+1}{k(k+2)} \cdot \frac{2k}{(k+1)!} \\ &= \frac{2(k+1)}{(k+2)!} \\ &= \frac{2n}{(n+1)!} \end{aligned}$$

So for all $n \geq 2$ we find

$$\prod_{i=2}^{n} \frac{i}{i^2-1} = \frac{2n}{(n+1)!}.$$

Exercise 10.6.10. Prove using induction that for all $n > 1$ it holds that $\prod_{i=2}^{n} \frac{i^2}{i^2-1} = \frac{2n}{n+1}$.

Solution: For $n = 2$

$$\prod_{i=2}^{n} \frac{i^2}{i^2-1} = \frac{4}{4-1} = \frac{4}{3} = \frac{2 \cdot 2}{(2+1)} = \frac{2n}{(n+1)}.$$

Now assume that for $n = k \geq 2$ we have

$$\prod_{i=2}^{n} \frac{i^2}{i^2-1} = \frac{2n}{(n+1)}.$$

Then for $n = k+1$ it follows that

$$\begin{aligned} \prod_{i=2}^{n} \frac{i^2}{i^2-1} &= \prod_{i=2}^{k+1} \frac{i^2}{i^2-1} \\ &= \frac{(k+1)^2}{(k+1)^2-1} \cdot \prod_{i=2}^{k} \frac{i^2}{i^2-1} \\ &= \frac{(k+1)^2}{k(k+2)} \cdot \frac{2k}{(k+1)} \\ &= \frac{2(k+1)}{(k+2)} \\ &= \frac{2n}{(n+1)} \end{aligned}$$

So for all $n \geq 2$ we find

$$\prod_{i=2}^{n} \frac{i^2}{i^2-1} = \frac{2n}{(n+1)}.$$

Exercise 10.6.11. The Fibonacci numbers F_n, with $n \in \mathbb{N}$, are defined as follows: $F_1 = F_2 = 1$, and $F_{n+2} = F_{n+1} + F_n$. Prove by using induction that F_{3n} is even for all $n \in \mathbb{N}$.

Solution: For $n = 1$ we have

$$F_{3n} = F_3 = F_2 + F_1 = 1 + 1 = 2,$$

which is even.

Now assume that for $n = k \geq 2$ we have that F_{3n} is even. Then for $n = k+1$ it follows that

$$F_{3n} = F_{3(k+1)} = F_{3k+2} + F_{3k+1} = 2 \cdot F_{3k+1} + F_{3k}.$$

Since F_{3k} is even by assumption and $2 \cdot F_{3k+1}$ is even as well, we have that $F_{3(k+1)}$ is also even.

So for all $n \in \mathbb{N}$ we have that F_{3n} is even.

Exercise 10.6.12. Prove, by using the Principal of Natural Induction, that for all $n \in \mathbb{N}$ it holds that $3^n < (n+2)!$.

Solution: For $n = 1$ we have $3^n = 3 < 6 = 3! = n!$.

Now assume that for some $k \in \mathbb{N}$ we have $3^k < (k+2)!$. Then $3^{k+1} = 3 \cdot 3^k < 3 \cdot (k+2)! < (k+3)!$ (since $3 < k+3$ for all $k > 0$).

So, with induction, it follows that for all $n \in \mathbb{N}$ it holds that $3^n < (n+2)!$.

Exercise 10.6.13. Prove that for all $n \geq 1$ it holds that

$$\sum_{i=1}^{n} (i^2 + i) = \frac{1}{3} n(n+1)(n+2).$$

Solution: For $n = 1$ we have

$$\sum_{i=1}^{n} (i^2 + i) = 1^2 + 1 = 2 = \frac{1}{3} \cdot 1 \cdot 2 \cdot 3 = \frac{1}{3} n(n+1)(n+2).$$

Now suppose that for some $k \geq 1$ it holds that

$$\sum_{i=1}^{k} (i^2 + i) = \frac{1}{3} k(k+1)(k+2).$$

Then we have

$$\begin{aligned}
\sum_{i=1}^{k+1} (i^2 + i) &= (k+1)^2 + (k+1) + \sum_{i=1}^{k} (i^2 + i) \\
&= k^2 + 3k + 2 + \frac{1}{3} k(k+1)(k+2) \\
&= (k+1)(k+2) + \frac{1}{3} k(k+1)(k+2) \\
&= (1 + \frac{1}{3} k)(k+1)(k+2) \\
&= \frac{1}{3} (k+1)(k+2)(k+3).
\end{aligned}$$

So with induction we have proven that for all $n \geq 1$ it holds that

$$\sum_{i=1}^{n} (i^2 + i) = \frac{1}{3} n(n+1)(n+2).$$

Exercise 10.6.14. Suppose $f, g : \mathbb{R} \to \mathbb{R}$ are differentiable functions. Then the product rule for differentiating says that $f \cdot g$ is also differentiable, with derivative $(f \cdot g)' = f' \cdot g + f \cdot g'$.

Suppose $f_1 = f$. For $n \geq 1$ we define $f_{n+1} = f \cdot f_n$.

Use induction and only this product rule (so not the chain rule) to prove that for all $n \geq 2$ it holds that $f_n : \mathbb{R} \to \mathbb{R}$ is differentiable with derivative $n \cdot f_{n-1} \cdot f'$.

Solution: For $n = 2$ we have $f_2 = f \cdot f_1 = f \cdot f$. Since f is differentiable, we have that $f \cdot f$ and therefore f_2 is differentiable. With the product rule we get that $f_2' = (f \cdot f)' = f' \cdot f + f \cdot f' = 2 \cdot f \cdot f' = 2 \cdot f_1 \cdot f$. So we have an induction basis.

Now suppose that for some $k \geq 2$ it holds that $f_k : \mathbb{R} \to \mathbb{R}$ is differentiable with derivative $k \cdot f_{k-1} \cdot f'$. Then we have that $f_{k+1} = f \cdot f_k$. Since f is differentiable and f_k is also differentiable by our assumption, we have that $f \cdot f_k$ and therefore f_{k+1} is differentiable. Furthermore, by the product rule and our assumption, we have

$$f_{k+1}' = (f \cdot f_k)' = f' \cdot f_k + f \cdot f_k' = f' \cdot f_k + f \cdot k \cdot f_{k-1} \cdot f' = (k+1) \cdot f_k \cdot f'.$$

By induction we have proven the assertion.

Exercise 10.6.15. Suppose R and S are relations on the set X with $R \subseteq S$.

(a) Use induction to prove that $R^n \subseteq S^n$ for all $n \in \mathbb{N}$.

(b) Prove that the transitive closure of R is contained in the transitive closure of S.

Solution: (a) We prove with induction that $R^n \subseteq S^n$ for all $n \in \mathbb{N}$.

If $n = 1$, then $R \subseteq S$ by assumption.

Now suppose $R^n \subseteq S^n$ for some $n \in \mathbb{N}$.

Then it holds that $R^{n+1} \subseteq S^{n+1}$. After all, let $xR^{n+1}y$, then there exist a z with xR^nz and zRy. But, then also by our assumption xS^nz and zSy. So $xS^{n+1}y$.

So by the Principle of Natural Induction it holds that $R^n \subseteq S^n$ for all $n \in \mathbb{N}$.

(b) The transitive closure of R is equal to $\bigcup_{n\in\mathbb{N}} R^n$. According to (a) this is contained in $\bigcup_{n\in\mathbb{N}} S^n$ and that is the transitive closure of S.

An alternative proof is the following: The transitive closure of S is a transitive relation which contains S and thus also R. The transitive closure of R is contained in each transitive relation which contains R, and thus also in the transitive closure of S.

Exercise 10.6.16. For $n \geq 2$ is $\binom{n}{2} = \dfrac{n(n-1)}{2}$. Let $m \in \mathbb{N}$, with $m \geq 2$.

Prove, by using the Principal of Natural Induction, that for all $n \in \mathbb{N}$ with $n \geq m$ it holds that

$$\binom{n}{2} - \binom{m}{2} = \frac{(n-m)(n+m-1)}{2}.$$

(Use induction of m.)

Solution: We prove that for all $n \in \mathbb{N}$ with $n \geq m$ it holds that

$$\binom{n}{2} - \binom{m}{2} = \frac{(n-m)(n+m-1)}{2}$$

using induction on m.

For $m = 2$ we have for all $n \geq m$ that

$$\binom{n}{2} - \binom{m}{2} = \binom{n}{2} - \binom{2}{2} = \frac{n(n-1)}{2} - 1 = \frac{n^2-n-2}{2} = \frac{(n-2)(n+1)}{2} = \frac{(n-m)(n+m-1)}{2}.$$

Now suppose that for m equal to some $k \in \mathbb{N}$ with $k \geq 2$ we have for all $n \in \mathbb{N}$ with $n \geq m$ that

$$\binom{n}{2} - \binom{m}{2} = \frac{(n-m)(n+m-1)}{2}.$$

Let $m = k+1$ Then we get for $n \geq m$ that

$$\begin{aligned}
\binom{n}{2} - \binom{m}{2} &= \binom{n}{2} - \binom{k+1}{2} \\
&= \binom{n}{2} - \frac{(k+1)k}{2} \\
&= \binom{n}{2} - \frac{(k-1)k}{2} - k \\
&= \binom{n}{2} - \binom{k+1}{2} - k \\
&= \frac{(n-k)(n+k-1)}{2} - k \\
&= \frac{n^2-n+k}{2} - k \\
&= \frac{n^2-n-k}{2} \\
&= \frac{(n-k-1)(n+k)}{2} \\
&= \frac{(n-m)(n+m-1)}{2}.
\end{aligned}$$

So by using induction we proved that for all $n, m \in \mathbb{N}$ with $n \geq m$ it holds that

$$\binom{n}{2} - \binom{m}{2} = \frac{(n-m)(n+m-1)}{2}.$$

Exercise 10.6.17. Suppose $f, g \in \mathbb{R}[X]$ are two polynomials. The set S is recursively defined by the following:

- $f, g \in S$;
- if $h, k \in S$, then $ah + bk \in S$ for all $a, b \in \mathbb{R}[X]$.

Prove by structural induction that S equals $\gcd(f,g)\mathbb{R}[X] = \{\gcd(f,g) \cdot k \mid k \in \mathbb{R}[X]\}$.

Solution: Let $T = \gcd(f,g)\mathbb{R}[X]$.

We prove by structural induction that $S \subseteq T$ by showing that each element of S is a multiple of $\gcd(f,g)$.

First of all $f, g \in T$ as both f, g are multiples of a.

Now if $h, k \in S$ are multiples of $\gcd(f,g)$, then also $ah + bk$ is a multiple of $\gcd(f,g)$. So, indeed, all elements of S are multiples of $\gcd(f,g)$. Next we show that all multiples of $\gcd(f,g)$ are in S.

As $f, g \in S$ and $\gcd(f,g)$ equals $af + bg$ for some $a, b \in \mathbb{R}[X]$, we find $\gcd(f,g) \in S$. But then clearly, also every multiple of the $\gcd(f,g)$ is in S.

But this implies that $S \subseteq T$ and $T \subseteq S$ and hence $S = T$.

Exercise 10.6.18. The Fibonacci numbers F_n, where $n \geq 1$, are defined recursively by:

$$F_1 = 1, F_2 = 1, \text{ and, for } n \geq 1, \ F_{n+2} = F_{n+1} + F_n.$$

Let $\phi = \frac{\sqrt{5}+1}{2}$, then $\phi^2 = \phi + 1$ (you do not need to prove this).

Prove by induction that $\phi^{n-2} \leq F_n \leq \phi^{n-1}$ for all $n \geq 1$.

Solution: We provide a proof using strong induction.

For $n = 1$ we have $\phi^{-1} \leq 1 = F_1 = \phi^0$.

Now suppose that $\phi^{k-2} \leq F_k \leq \phi^{k-1}$ for all $1 \leq k \leq n$. Then for $F_{n+1} = F_n + F_{n-1}$ we find

$$\phi^{n-3} + \phi^{n-2} \leq F_{n+1} \leq \phi^{n-2} + \phi^{n-1}.$$

As

$$\phi^{n-3} + \phi^{n-2} = \phi^{n-3}(1+\phi) = \phi^{n-3} \cdot \phi^2 = \phi^{n-1}$$

and

$$\phi^{n-2} + \phi^{n-1} = \phi^{n-2}(1+\phi) = \phi^{n-2} \cdot \phi^2 = \phi^n$$

we obtain

$$\phi^{n-1} \leq F_{n+1} \leq \phi^n.$$

By strong induction we have now proven that $\phi^{n-2} \leq F_n \leq \phi^{n-1}$ for all $n \geq 1$.

Exercise 10.6.19. Let R be a symmetric relation on a set X.

(a) Prove, for example using natural induction, that for $n \geq 1$ also R^n is symmetric.
(b) Use part (a) to prove that the transitive closure of R is symmetric.

Solution: (a) Let $P(n)$ be the above statement. For $n = 1$ the statement is obviously true.
Now suppose R^n is symmetric and consider $R^{n+1} = R^n; R$.
Let $aR^{n+1}c$. Then there is a $b \in X$ with aR^nb and bRc. But as, by assumption R^n and R are symmetric, we also find cRb and bR^na. But then $aR; R^nc$ and $aR^{n+1}c$.
Thus by induction the statement $P(n)$ is true for all $n \geq 1$.
(b) As the union of symmetric relations is symmetric, we find the the transitive closure of R, which equals $\bigcup_{n\geq 1} R^n$ is symmetric.

Exercise 10.6.20. Binary trees are graphs with a special point, called the root. They can be defined as follows:

- The graph consisting of a single point r is a binary tree with root r.
- If $T_1 = (V_1, E_1)$ and $T_2 = (V_2, E_2)$ are binary trees with roots $r_1 \in V_1$ and $r_2 \in V_2$, respectively, and disjoint vertex sets, then for $r \notin V_1 \cup V_2$ the graph $T = (V_1 \cup V_2 \cup \{r\}, E_1 \cup E_2 \cup \{\{r, r_1\}, \{r, r_2\}\})$ is a binary tree with root r.

A leaf of a binary tree T is a point which is on at most one edge. A vertex which is not a leaf, is called an internal vertex.

Let l be the number of leafs of a binary tree and k be the number of internal vertices.

Use structural induction to prove that in a binary tree $T = (V, E)$ one has $l = k + 1$.

Solution: We prove that $l = k + 1$ by structural induction.

First consider the tree with just one vertex. In this tree we have $l = 1$ and $k = 0$. So indeed, $l = k + 1$.

Now assume that the binary tree T_1 contains l_1 leaves and $k_1 = l_1 - 1$ internal vertices and the tree T_2 has l_2 leaves and $k_2 = l_2 - 1$ internal vertices.

Then the tree T constructed out of T_1 and T_2 as in the definition, has as leaves the leaves from T_1 and from T_2. So, the number of leaves l equals $l_1 + l_2$.

The internal vertices of T are those of T_1 and of T_2, together with r. Hence k, the number of internal vertices of T equals $k_1 + k_2 + 1$.

But then $l = l_1 + l_2 = (k_1 + 1) + (k_2 + 1) = (k_1 + k_2 + 1) + 1 = k + 1$.

So, by structural induction we find that for all binary trees the number of leaves is the number of internal vertices plus 1.

10.7 Cardinalities

Exercise 10.7.1. Prove that a collection of pairwise disjunct open intervals is countable.
(Hint: Suppose $x < y$ are two real numbers, then the open interval (x, y) contains a rational number.)

Solution: Consider a set $\mathscr{I}$ of disjoint open intervals. Assign to each interval $I \in \mathscr{I}$ a rational number $q_I \in \mathbb{Q} \cap I$. The map $\phi : \mathscr{I} \to \mathbb{Q}$ defined by $\phi(I) = q_I$ is injective.

As $\mathbb{Q}$ is countable, so is $\mathscr{I}$.

Exercise 10.7.2. Let $b \in \mathbb{R}$ and A be a subset of $\mathbb{R}^+$ with the property that for each finite subset $\{a_1, \ldots, a_n\}$ of A it holds that $a_1 + \cdots + a_n \leq b$.

(a) Show that for each $n \in \mathbb{N}$ it holds that $A_n := \{x \in A \mid x \geq \frac{1}{n}\}$ is finite.
(b) Prove that A is countable.

Solution: (a) We will prove by contradiction. Suppose the set A_n has an infinite number of elements. Then take $b \cdot n + 1$ element from this set. Together they form a finite subset of A and since for each element a_i from this set we have $a_1 \leq \frac{1}{n}$ the sum of all these elements is larger then b, which is a contradiction.
(b) Note that $A = \bigcup_{n\in\mathbb{N}} A_n$. So A is a union of a countable number of sets each containing a finite number of elements. This means also A must be countable.

Exercise 10.7.3. A integer polynomial function is a function $f : \mathbb{C} \to \mathbb{C}$ with $f(x) = a_n x^n + \cdots a_1 x + a_0$, where $a_i \in \mathbb{Z}$ for all $1 \leq i \leq n$. Such integer polynomial function f is said to have degree n if $a_n \neq 0$.

The set $\mathbb{A}$ consists of all $z \in \mathbb{C}$ with $f(z) = 0$ for some integer polynomial function f. The set $\mathbb{A}$ is called the set of algebraic integers.

Prove that $\mathbb{A}$ is countable.

Solution: The set S_n of integer polynomial functions of degree n is countable. Clearly the map $F : \mathbb{Z}^{n+1} \to S_n$ with $F(a_n, \ldots, a_0)$ being the function f with $f(x) = a_n x^n + \cdots a_1 x + a_0$ is a surjective map from $\mathbb{Z}^{n+1}$ into S_n.

As each such function has at most n roots, (Principle Theorem of Algebra), we find the set $\mathbb{A}_n$ consisting of all $z \in \mathbb{C}$ which are a root of an integer polynomial of degree n is the union of countably many sets of size at most n, and therefore countable. Indeed

$$\mathbb{A}_n = \bigcup_{f \in S_n} \{z \in \mathbb{C} \mid f(z) = 0\}.$$

Now

$$\mathbb{A} = \bigcup_{n \in \mathbb{N}} \mathbb{A}_n,$$

and hence also a union of countably many countable sets. In particular, $\mathbb{A}$ is countable.

Exercise 10.7.4. Suppose A and B are two sets and $f : A \to B$ is surjective. Then there is a subset $A_0 \subseteq A$ such that A_0 has the same cardinality as B.

Hint Use the Axiom of Choice.

Solution: Suppose $f : A \to B$ is surjective.

Let C be the collection of sets $f^{-1}(b)$ for $b \in B$. As f is surjective, each of these sets is nonempty. Moreover, any two of them are disjoint. So, C has the same cardinality as B.

By the Axiom of Choice, there is a choice function g with $g(f^{-1}(b)) \in f^{-1}(b)$ for each b. Clearly g is injective.

The set $A_0 = g(C)$ is now a subset of A with the same cardinality as C and hence also as B.

Exercise 10.7.5. Let X be an infinite but countable set and $\mathscr{F}\mathscr{P}(X)$ be the set of all finite subsets of X. Show that $\mathscr{F}\mathscr{P}(X)$ is also countable.

Solution: For each n we have that X^n is countable.

So, if $\mathscr{F}\mathscr{P}_n$ denotes the set of all subsets of size n, then the map that assign to each member $Y = \{x_1, \ldots, x_n\} \in \mathscr{F}\mathscr{P}(X)$ the element $(x_1, \ldots, x_n) \in X^n$ (in any fix chosen order) is injective. So, $\mathscr{F}\mathscr{P}_n$ is also countable.

But as $\mathscr{P}\mathscr{F}(X)$ is the union of all the sets $\mathscr{F}\mathscr{P}_n$ it is also countable.

Exercise 10.7.6. Suppose A is uncountable and B an infinite countable subset disjoint from A. We will prove that A and $A \cup B$ have the same cardinality.

(a) Show that there is an injection from A into $A \cup B$.

(b) The set A contains a countable sunset A_0. Fix bijections $g : B \to \mathbb{N}$ and $h : \mathbb{N} \to A_0$.
Let $f : A \cup B \to A$ be defined as follows.

$$f(a) = \begin{cases} a \text{ if } a \notin A_0 \\ h(2k) \text{ if } a = h(k) \in A_0 \text{ for some } k \in \mathbb{N} \\ h(2g(a)+1) \text{ if} a \in B \end{cases}$$

Prove that f is an injection.

(c) Conclude that A and $A \cup B$ have the same cardinality.

Solution: (a) As A is a subset of $A \cup B$, the identity map is injective.

(b) Let $x,y \in A$ with $f(x) = f(y)$. If $x,y \in A \setminus A_0$, then $x = f(x) = f(y) = y$ and hence $x = y$. If $x \in A_0 \cup B$ and $y \in A \setminus A_0$ (or vice versa), then $f(x) \in A_0$ and $f(y) \notin A_0$, contradicting $f(x) = f(y)$. So, we may assume that $x,y \in A_0 \cup B$.
If both $x,y \in A_0$, then $x = h(n)$ and $y = f(m)$ for some $n,m \in \mathbb{N}$ and $f(x) = h(2n) = f(y) = h(2m)$. But as h is a bijection, we find $2n = 2m$ from which it follows that $n = m$ and hence $x = y$.
If both $x,y \in B$, then $f(x) = h(2g(x)+1) = f(y) = h(2g(y)+1)$. But as h is a bijection we get $2g(x)+1 = 2g(y)+1$ and $g(x) = g(y)$ implying $x = y$, since g is a bijection.
Finally we have to consider the case that $x \in A_0$ and $y \in B$ (or vice versa). But then $f(x)$ is equal to h applied to an even number while $f(y)$ equals h applied to some odd number. As h is a bijection this implies that $f(x) \neq f(y)$, contradicting our assumption.

(c) The Cantor-Bernstein-Schröder theorem implies that there exists a bijection between A and $A \cup B$, proving that $A \cup B$ and A have the same cardinality.

10.8 Integer Arithmetic

Exercise 10.8.1. Write the integer $x = 3000$ in base 5.

Solution:

x	quotient after division by 5	remainder after division by 5
3000	600	0
600	120	0
120	24	0
24	4	4
4	0	4

So, 3000 equals $(44000)_5$.
Check: $(44000)_5 = 4 \cdot 5^4 + 4 \cdot 5^3 = 4 \cdot 625 + 4 \cdot 125 = 2500 + 500 = 3000$.

Exercise 10.8.2. Let $z \in \mathbb{Q}$. If $z^n \in \mathbb{Z}$ for some $n \in \mathbb{N}$, $n > 0$, then $z \in \mathbb{Z}$. Prove this.

Solution: Suppose $z \in \mathbb{Q}$, then there are $a,b \in \mathbb{Z}$ with $z = \frac{a}{b}$ and $\gcd(a,b) = 1$.
If $z^n = c \in \mathbb{Z}$, then $(\frac{a}{b})^n = c$ and hence $a^n = c \cdot b^n$. Since $\gcd(a,b) = 1$, we also have $\gcd(a^n,b^n) = 1$ and hence $a^n \mid c$. But then, if $|b| > 1$, we have $|z^n| < |a^n| \leq |c|$ and find a contradiction. So, $b = \pm 1$ and $z \in \mathbb{Z}$.

Exercise 10.8.3. Prove that the sum of 7 consecutive integers is divisible by 7.
(For example, $3+4+5+6+7+8+9 = 42$ and so divisible by 7. But does this always hold?)

Solution: First of all, we can write 7 consecutive integers as $n, n+1, \ldots, n+5, n+6$. So the sum of these is $\sum_{i=0}^{i=6} n+i = 7n+21$, which is divisible by 7 for all $n \in \mathbb{N}$.

Exercise 10.8.4. Of $a,b,c \in \mathbb{Z}$ it is given that $\gcd(a,b) = 21$ and $\gcd(b,c) = 16$. Show that there exist $x,y,z \in \mathbb{Z}$ with $xa+yb+zc = 1$.

Solution: Since $\gcd(a,b) = 21$ there exist $x_1,y_1 \in \mathbb{N}$ such that $x_1a + y_1b = 21$. Also since $\gcd(b,c) = 16$ we can find y_2,z_2 such that $y_2b + z_2c = 16$. Now since $\gcd(21,16) = 1$ there exists α and β such that $21\alpha + 16\beta = 1$ and thus $\alpha(x_1a + y_1b) + \beta(y_2b + z_2c) = 1$. So for $x = \alpha x_1$, $y = \alpha y_1 + \beta y_2$ and $z = \beta z_2$ we have $xa + yb + zc = 1$.

Exercise 10.8.5. Show that each odd prime can be written as the difference of two squares of a natural number in exactly one way. (For example, $5 = 3^2 - 2^2$ or $11 = 6^2 - 5^2$.)

Solution: Note that for every odd natural number p we can write $p = 2n+1 = (n+1)^2 - n^2$. So every odd natural number can be written as the difference between two squares. The uniqueness property only holds for primes. Namely if $p = x^2 - y^2$ then also $p = (x+y)(x-y)$. Now since p is prime either $x+y = 1$ or $(x-y) = 1$. Since x and y are both positive this gives us that $x-y = 1$ and thus $x+y = p$. This system has a unique solution $x = \frac{p+1}{2}$, $y = \frac{p-1}{2}$.

Exercise 10.8.6. (a) Let $z \in \mathbb{Q}$. If $z^n \in \mathbb{Z}$ for some $n \in \mathbb{N}$, $n > 0$, then $z \in \mathbb{Z}$. Prove this.
Given are $a, b, x, y \in \mathbb{N}$ with $\gcd(a,b) = 1$ en $x^a = y^b$.
(b) Show that there are $\lambda, \mu \in \mathbb{Z}$ with $x = (y^\lambda x^\mu)^b$.
(c) Prove that there is a $z \in \mathbb{N}$ with $x = z^b$ and $y = z^a$.

Solution: (a) Since $z \in \mathbb{Q}$ we can write $z = \frac{a}{b}$, with $a, b \in \mathbb{N}$. Now let $n \in \mathbb{N}$ such that $z^n \in \mathbb{N}$. Since $z^n = \frac{a^n}{b^n}$ it must follow that $b^n = \pm 1$ and thus $b = \pm 1$, but then also $z \in \mathbb{N}$.
(b) Since $\gcd(a,b) = 1$ there exist $\lambda, \mu \in \mathbb{Z}$ such that $a\lambda + b\mu = 1$. Now for these λ, μ we have $(y^\lambda x^\mu)^b = (y^b)^\lambda x^{b\mu} = (x^a)^\lambda x^{b\mu} = x^{a\lambda + b\mu} = 1$.
(c) Let $z = y^\lambda x^\mu$ as in exercise (b). So $x = z^b$ is satisfied. Also $z^a = (y^\lambda x^\mu)^a = y^{a\lambda}(x^a)^\mu = y^{a\lambda}(y^b)^\mu = y^{a\lambda + b\mu} = y$.

Exercise 10.8.7. (a) Suppose $\sigma \in \mathrm{Sym}_n$ is a cycle of length c. Let m be a positive integer with $\sigma^m = \mathrm{Id}$, the identity map, then $c \mid m$.
(b) Suppose σ is a permutation in Sym_n with cycle structure $c_1, c_2, \ldots, c_k$. Prove that the order of σ equals $\mathrm{lcm}(c_1, c_2, \ldots, c_k)$.

Solution: (a) Suppose $\sigma \in \mathrm{Sym}_n$ is a cycle of length c and let m be a positive integer with $\sigma^m = \mathrm{Id}$. Then the order of σ equals c.
Write $m = qc + r$, where q is the quotient and r the remainder of division of m by c. Now

$$\sigma^m = \sigma^{qc+r} = (\sigma^c)^q \sigma^r = \sigma^r = \mathrm{Id}.$$

As $0 \le r < c$, and σ has order c, we can conclude that $r = 0$ and $m \mid c$.
(b) Let σ be a permutation in Sym_n with cycle structure $c_1, c_2, \ldots, c_k$ and write σ as a product $\sigma_1 \cdots \sigma_k$ of disjoint cykels σ_i of length c_i, where $1 \le i \le k$.
Then with $\ell = \mathrm{lcm}(c_1, \ldots, c_k)$ we have $\sigma^\ell = \sigma_1^\ell \cdots \sigma_k^\ell = \mathrm{Id}$. So, the order of σ is at most ℓ.
Now for $1 \le m < \ell$ we find that $\sigma^m = \sigma_1^m \cdots \sigma_k^m$. As $m < \ell$ there is an index i such that c_i does not divide m. Hence σ_i^ℓ is not the identity (see part (a)) and there is an element x in the support of σ_i which is not fixed by σ_i^ℓ. But as x is fixed by all σ_j with $j \ne i$, we find that σ^ℓ does not fix x and hence is not the identity.
We conclude that the order of σ is at least ℓ and hence equals ℓ.

10.9 Modular Arithmetic

Exercise 10.9.1. How many n with $1 \le n \le 2016$ satisfy $\gcd(n, 2016) = 6$?

Solution: $n = 6m$ with $\gcd(m, \frac{2016}{6}) = 1$. The number of n equals $\Phi(\frac{2016}{6}) = \Phi(336) = \Phi(2^4 \cdot 3 \cdot 7) = \Phi(2^4) \cdot \Phi(3) \cdot \Phi(7) = (2^4 - 2^3) \cdot 2 \cdot 6 = 96$.

Exercise 10.9.2. Find the smallest nonnegative integer x with

$$x = 131^{20} - 25^{45} \cdot 22^{45} \mod 19.$$

Solution: We work modulo 19, a prime, so we can reduce the exponents mod 18. This yields $x = (-2)^2 - 6^7 \cdot 3^9 = 4 - 2^7 \cdot 3^{16} = 4 - 14 \cdot (-2) = 13 \mod 19$.

Exercise 10.9.3. Find the remainder of 54321^{12345} after division by 11.

Solution: we have $54321 \mod 11 = 3$ By Fermat's Little Theorem we have $3^{10} = 1 \mod 11$. So $54321^{12345} = 3^{12345} = 3^5 = 243 = 1 \mod 11$.

Exercise 10.9.4. For each $a \in \mathbb{Z}/3000\mathbb{Z}$ we define the map $f_a : \mathbb{Z}/3000\mathbb{Z} \to \mathbb{Z}/3000\mathbb{Z}$ by $f_a(x) = ax$ for all $x \in \mathbb{Z}/3000\mathbb{Z}$.
How many of these maps f_a are injective?

Solution: f_a is injective if and only if a is invertible. The number of invertible elements in $\mathbb{Z}/3000\mathbb{Z}$ equals $\Phi(3000) = \Phi(2^3 \cdot 3 \cdot 5^3) = (2^3 - 2^2) \cdot (2) \cdot (5^3 - 5^2) = 4 \cdot 2 \cdot 100 = 800$. (Here Φ is the Euler Φ function.)

Exercise 10.9.5. Determine all integer x which satisfy $12x = 14 \bmod 22$.

Solution: Using the extended Euclidean algorithm we find $\gcd(12, 22) = 2 = 2 \cdot 12 - 1 \cdot 22$. A solution for $12x = 14 \bmod 22$ is $x = 7 \cdot 2 = 14$, all other solutions are then of the form $14 + \lambda 22$ where $\lambda \in \mathbb{Z}$.

Exercise 10.9.6. Let p be prime. Then prove that it holds that $\forall_{x,y \in \mathbb{Z}/p\mathbb{Z}}[x \neq 0 \Rightarrow (\exists_{z \in \mathbb{Z}/pZ}[xz = y])]$.

Solution: Since p is prime we have $\gcd(x, p) = 1$. This means by using the extended Euclidean algorithm we find a, b such that $ax + bp = 1$. Now for $z = y \cdot a$ we have $xz = y \bmod p$.

Exercise 10.9.7. Let p be an odd prime. We call $a \in \mathbb{Z}/p\mathbb{Z}$ a square if and only if there is a $b \in \mathbb{Z}/p\mathbb{Z}$ with $a = b^2$.

Prove that $\mathbb{Z}/p\mathbb{Z}$ has exactly $1 + \frac{p-1}{2}$ squares.

Solution: Suppose $a^2 = b^2 \bmod p$, then $(a-b)(a+b) = 0 \bmod p$. So $a = b \bmod p$ or $a = -b \bmod p$.

As p is odd, we have $a \neq -a \mod p$ for all $a \neq 0 \mod p$. So, we find $1 + \frac{p-1}{2}$ distinct squares.

Exercise 10.9.8. Prove that $n^{13} - n$ is divisible by 78 for all $n \in \mathbb{Z}$.

Solution: We will use that in general $n^{1+(p-1)k} = n$ mod p. This can be proven by using Fermats theorem:

$$\begin{aligned} n^{1+(p-1)k} &= n \cdot (n^{p-1})^k \\ &= n \cdot 1^n \\ &= n \,(\text{mod } p). \end{aligned}$$

Now this gives $n^{13} - n = n^{1+(2-1)12} = n \,(\text{mod } 2)$, $n^{13} = n^{1+(3-1)6} = n \,(\text{mod } 2)$, and $n^{13} = n^{1+(13-1)1} = n \,(\text{mod } 13)$. But then $n^{13} - n = 0 \,(\text{mod } 78 = 2 \cdot 3 \cdot 13)$.

Exercise 10.9.9. Let p be an odd prime.

(a) For which invertible elements $a \in \mathbb{Z}/p\mathbb{Z}$ does it hold that $a^{-1} = a$?

(b) Prove that $\prod_{i=1}^{p-1} i = -1 \,(\text{mod } p)$.

Solution: (a) Suppose $a \in \mathbb{Z}/p\mathbb{Z}$ satisfies $a^{-1} = a$. Then $a^2 = 1$ and hence $a^2 - 1 = (a-1)(a+1) = 0$. But that implies that $a = \pm 1 \,(\text{mod } p)$.

(b) For each i with $1 < i < p-1$ theer is a unique j with $1 < i < p-1$ different from i with $ij = 1 \,(\text{mod } n)$. This implies that $\prod_{i=1}^{p-1} i = 1 \cdot -1 \cdot 1 = -1 \,(\text{mod } p)$.

Exercise 10.9.10. Let $n, m \in \mathbb{N}$, $n > 1$. The map $f_m : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ given by $f_m(x \,(\text{mod } n)) = mx \,(\text{mod } n)$ is a bijection if and only if $\gcd(n, m) = 1$.

Proof this statement.

Solution: Suppose f_m is a bijection. Then there is an x with $f_m(x \,(\text{mod } n)) = mx \,(\text{mod } n) = 1 \,(\text{mod } n)$. So, $m \,(\text{mod } n)$ has an inverse, which is equivalent with $\gcd(m, n) = 1$.

Now assume that $\gcd(n, m) = 1$. Then $m \,(\text{mod } n)$ has an inverse, say $k \,(\text{mod } n)$. Now $f_k f_m(x \,(\text{mod } n)) = kmx \,(\text{mod } n) = x \,(\text{mod } n) = f_m f_k(x \,(\text{mod } n))$. Thus f_k is the inverse of f_m which therefore is bijective.

Exercise 10.9.11. Let m_1 and m_2 be two positive integers with $\gcd(m_1, m_2) = 1$ and suppose a_1 and a_2 are two arbitrary integers. Then the Chinese Remainder Theorem tells us that there is, modulo $m := m_1 m_2$, a unique element $p \in \mathbb{Z}$ such that

$$p = a_1 \,(\text{mod } m_1) \text{ and } p = a_2 \,(\text{mod } m_2). \quad (*)$$

This exercise will provide a proof of this result using the map

$$\phi : \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z}$$

with for all $a \pmod m \in \mathbb{Z}/m\mathbb{Z}$

$$\phi(a \pmod m) = (a \pmod{m_1}, a \pmod{m_2}).$$

(a) Show that the map ϕ is well defined (i.e., if $a' \pmod m) = a \pmod m$ then $\phi(a' \pmod m) = \phi(a \pmod m)$.)
(b) Prove that ϕ is injective.
(c) Use the Pigeon Hole Principle to prove that ϕ is surjective and hence also bijective, and explain why this bijectivity of ϕ proves the Chinese Remainder Theorem (*).

Solution: (a) If $a' \pmod m) = a \pmod m$, then $a' \pmod{m_1}) = a \pmod{m_1}$ and $a' \pmod{m_2}) = a \pmod{m_2}$. So ϕ is well defined.
(b) Suppose $\phi(a \pmod m) = \phi(b \pmod m)$ then $a \pmod{m_1}) = b \pmod{m_1}$ and $a \pmod{m_2}) = b \pmod{m_2}$. But then $a \pmod{\operatorname{lcm}(m_1,m_2)}) = b \pmod{\operatorname{lcm}(m_1,m_2)}$. As $\gcd(m_1,m_2) = 1$, we find $\operatorname{lcm}(m_1,m_2) = m$, and find $a \pmod m) = b \pmod m$.
This proves ϕ to be injective.
(c) Since $\mathbb{Z}/m\mathbb{Z}$ and $\mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z}$ have the same number of elements, and ϕ is injective, the Pigeon Hole Principle shows ϕ is bijective. So, for each a_1 and a_2 there is, modulo $m := m_1m_2$, a unique element $p = \phi^{-1}(a_1 \pmod{m_1}, a_2 \pmod{m_1}) \in \mathbb{Z}$ such that

$$p = a_1 \pmod{m_1} \text{ and } p = a_2 \pmod{m_2}.$$

This proves the Chinese Remainder Theorem.

Exercise 10.9.12. Let $m > 1$ be an integer. Eulers Theorem implies that each invertible element $a \in \mathbb{Z}/m\mathbb{Z}$ satisfies

$$a^{\Phi(m)} = 1 \pmod m.$$

Suppose $a \in \mathbb{Z}/m\mathbb{Z}$ is invertible. The smallest positive $n \in \mathbb{N}$ for which $a^n = 1 \pmod m$ is called the order of a.
(a) Let $a \in \mathbb{Z}/m\mathbb{Z}$ be invertible and have order n. Prove that n divides $\Phi(m)$.
(b) Inside $\mathbb{Z}/1451\mathbb{Z}$ we find invertible elements with order 50 and 29, repspectively. Use this to prove that 1451 is a prime.

Solution: (a) Suppose $a \in \mathbb{Z}/m\mathbb{Z}$ is an element of order k. Division with remainder yields

$$\Phi(m) = qk + r$$

for some integers q, r with $0 \le r < k$. But then

$$a^r = a^{\Phi(m)-q\cdot k} = a^{\Phi(m)} \cdot (a^k)^{-q} = 1 \pmod m.$$

As $r < k$, we find $r = 0$ and $k \mid \Phi(m)$.
(b) By (a) we find that $\Phi(1451)$ is divisible by 50 and 29 and hence by $\operatorname{lcm}(50,29) = 29 \cdot 50 = 1450$. But then $\Phi(1451) = 1450$ and 1451 is a prime.

Index