A bridge course to higher mathematics

Valentin Deaconu

Don Pfaff

Department of Mathematics, University of Nevada, Reno NV 89557-0084, USA

Current address: Department of Mathematics, University of Nevada, Reno NV 89557-0084, USA

E-mail address: vdeaconu@unr.edu

Department of Mathematics, University of Nevada, Reno NV 89557-0084, USA

Current address: Department of Mathematics, University of Nevada, Reno NV 89557-0084, USA

E-mail address: don@unr.edu

2010 *Mathematics Subject Classification.* Primary 03F07

Contents

Introduction

It is common for a college student to stand in awe of the professor and perhaps to regard a textbook writer as a person with some kind of superhuman knowledge. What is often overlooked is the fact that we professors were once students ourselves and many of us thought that we would never attain to the lofty heights of understanding that our teachers displayed so casually during the course of their lectures. Many of us were right! Let it be known right now that a substantial number of readers of this book are much brighter and faster than we ever were. If we have an advantage over them, it is merely due to experience, not to innate ability. The purpose in writing this book is simply to share some things that we have learned over the years; ideas and techniques we have found helpful and which we believe can help students to progress faster and further along the road to deeper mathematical understanding.

There are students who have done quite well in mathematics up to and including calculus but who find that their first encounter with upper division math is a somewhat traumatic experience. The main reason for these difficulties may be the fact that excelling in the purely computational aspects of math is not sufficient for the rigors of thinking things through very carefully and writing arguments down and proving theorems in a way that would be recognizable to the professor, showing a deep understanding of what was going on.

One of us (Pfaff) has spent a substantial part of his career teaching classes for those who intend to be secondary school teachers. This experience tells us that the gap between elementary and advanced math is, for most persons, more of a yawning chasm than a gap. The problem seems to be that very few really understand the mechanics and processes that constitute a correct mathematical proof. To progress towards mathematical maturity, it is necessary to be trained in two aspects: the ability to read a proof and the ability to write a proof.

The emphasis in this book, as you may have guessed, will be on proof. But we intend to do more than simply prove a bunch of theorems. All mathematically literate persons should be conversant with the basics of math, including a knowledge of logic, sets, functions, relations and the different kinds of numbers and their properties. So, we intend to cover the fundamentals of abstract mathematics, but with special attention paid to its logical structure and especially with an emphasis on how the theorems are proved.

Many of the individual facts and examples presented in this book may be already familiar to you. This is deliberate. By dealing with material that you have already been exposed to, you will be in a better position to concentrate on the underlying thought processes and practice in a variety of applications the many theorem-proving techniques that should be part of every mathematician's arsenal.

There will be of course numerous new concepts and facts. We have in mind all the tools that will be necessary to make the transition from lower division courses like Calculus, Differential Equations and Linear Algebra to upper division classes like Abstract Algebra, Real and Complex Analysis and Topology. We assume some knowledge about basic algebra and calculus; in particular the notation $\mathbb{N}$ for the set of natural numbers, $\mathbb{Z}$ for the set of integers, $\mathbb{Q}$ for the set of rationals and $\mathbb{R}$ for the set of reals appear in many Calculus textbooks. A word of caution: different books may use different notation for the same notion. Also, the same symbol may have different meanings in different contexts. This is sometimes for historical reasons, sometimes from laziness, but many times because it is difficult to invent new and meaningful signs that will please everybody. For example, (a, b) is often used to denote an open interval, but also to denote an ordered pair or a vector in the plane; $[a, b]$ sometimes means a closed interval, but other times means an equivalence class; $\wedge$ is a logical connector, but is also used to denote the greatest lower bound, etc.

We begin our journey with elements of logic and techniques of proof, then with elementary set theory, relations and functions, giving many examples, some of them contained in exercises. Then we discuss the Peano axioms for positive integers and natural numbers, in particular mathematical induction and other forms of induction. We give the construction of integers, using an equivalence relation on pairs of natural numbers, including some elementary number theory. We continue with the notions of finite and infinite sets, cardinality of sets and then we discuss counting techniques and combinatorics, illustrating more techniques of proof. We conclude with a rigorous construction of the sets of rational numbers, the set of reals and the set of complex numbers, which is intended for more advanced readers. We included some other advanced topics, like Zorn's lemma and the axiom of choice; some of our discussions are incomplete, and we direct the interested reader to other books. Also, we included some more challenging exercises. All these materials are optional, depending on the instructor and the goals of the reader.

Throughout this book, we will emphasize creative thinking, and we will learn new tricks related to lots of abstract ideas and concepts. We will learn the language of axioms and theorems and we will write convincing and cogent proofs using quantifiers. We will solve many puzzles and encounter some mysteries and unsolved problems. Many times you will ask yourself: what can I assume to be known? what exactly do I have to show? what method and strategy should I use? Only lots of practice will help you to find good answers to these questions.

Chapter 1

Elements of logic

1.1. Statements, Propositions and Theorems

We can use words and symbols to make meaningful sentences, also called statements. For example

a) Mary snores.

b) A healthy warthog has four legs.

c) $2 + 3 = 5$.

d) $x + 5 = 7$.

e) $\displaystyle\int_0^\pi \sin x \, dx = 2$.

f) $\forall x \in \mathbb{R} \;\; \exists\, y \in \mathbb{R}$ such that $y^2 = x$.

g) $x/x = 1$.

h) $3 \in [1, 2)$.

i) Dr. Pfaff is the president of the United States.

Some of these statements have eccentric formats, using symbols that you may not have seen before. By the way, $\forall$ means for all, $\in$ means belongs to (or is an element of) and $\exists$ means there exists. The statements could be true (b, c, e), false (f, h, i) or neither (a, d, g). The last possibility occurs because we don't have enough information. For statement a, which Mary are we talking about? Is she snoring now or in general? For statement d, do we know that $x = 2$? For statement g, do we know x to be a nonzero number? We don't, but these kind of ambiguous statements (neither true or false) also appear in mathematics.

To make our life easier, let's agree that a *proposition* is a statement which is either true or false. Each proposition has a truth value denoted T for true or F for false. All statements b,c,e,f,h,i are propositions, but a,d,g are not. We can modify statements d and g as

d') $\forall x : x + 5 = 7$

g') $\exists x : x/x = 1$,

which become propositions. Of course, the proposition d' is false and the proposition g' is true.

A statement proved to be true is called a *theorem.* A proof could be straightforward, by just doing a computation. For example, e) is a true proposition, and becomes a theorem after we compute using the Fundamental Theorem of Calculus

$$\int_0^{\pi} \sin x \, dx = -\cos x \Bigg|_0^{\pi} = -\cos(\pi) + \cos(0) = -(-1) + 1 = 2.$$

The statement "There is a positive integer n such that $2^{2^n} + 1$ is not a prime" is a proposition, but not a theorem, unless we prove it. Try!

Many times a proof could be long and complicated, requiring smart ideas and tricks. One way or the other, a proof should follow the rules of logic, which will be developed below. We will illustrate in the next chapter many methods and examples of proofs. The symbol □ indicates the end of a proof.

In constructing a mathematical theory, we often start with some statements called *axioms* which are accepted to be true, and using certain rules we prove new true statements, the theorems. In the process, we may have to prove auxiliary results, called *lemmas.* A consequence of a theorem is called a *corollary.*

Example 1.1. As an abstract example of a theory, suppose that we construct statements which are words using only the symbols a, b, S. Suppose S is the only axiom, and the rules are that we can replace S by aSb, and that we can delete an S. Is $aabb$ a true statement? How about SS? It can actually be proved that the only theorems are $\underbrace{a...a}_{n} S \underbrace{b...b}_{n}$ and $\underbrace{a...a}_{n}\underbrace{b...b}_{n}$ for $n \geq 0$. Therefore, $aabb$ is a true statement, and SS is false.

We will give later examples of axioms used to define positive integers and to prove their properties. Also, we will give axioms for set theory.

An open sentence (or *predicate*) is a sentence depending on one or more variables, which could be true or false. For example, consider the sentence $P(a)$: the real function $f(x) = |x|$ is differentiable at a. Then $P(1)$ is a true proposition, but $P(0)$ is false. Can you explain why? Recall that

$$|x| = \begin{cases} x, & x \geq 0 \\ -x, & x < 0. \end{cases}$$

We will use the universal quantifier $\forall$ and the existential quantifier $\exists$ to form new propositions, using open sentences like

$$\forall x \; P(x), \;\; \exists y \; Q(y), \;\; \forall x \; \exists y \; R(x, y).$$

The expression $\exists! \; x \; P(x)$ means that there is a unique x such that $P(x)$.

1.2. Logical connectives and truth tables

It is important to understand the meanings of key words that will be used throughout mathematics. Primary words which must be clarified are the logical terms "not", "and", "or","if...then", and "if and only if". The word "and" is used to combine two sentences to form a new sentence which is always different from the original ones. For example, combining sentences c and h above we get

$$2 + 3 = 5 \text{ and } 3 \in [1, 2),$$

which is false, since 3 does not belong to the interval $[1, 2)$. The meaning of this compound sentence can be determined in a straightforward way from the meanings of its component parts. Similar remarks hold for the the other basic logical terms, called also connectives. We will think of the above basic logical terms as operations on sentences. Though there are linguistic conventions which dictate the proper form of a correctly constructed sentence, we will find it convenient to write all our compound sentences in a manner reminiscent of algebra and arithmetic. Thus, irrespective of where the word “not" should appear in a sentence in order the placate the grammarians, we will write it at the beginning. For example, though a grammar book would tell us that “not Pfaff is the president of the United States" is improper usage, and that the correct way is to write “Pfaff is not the president of the United States", it will prove easier for us to work with the first form. We regard the two as the same for our purposes.

We will use the symbolic notation. The *negation* of a statement P is denoted by $\neg P$, verbalized as “not P". The operation of negation always reverses the truth value of a sentence. We summarize this in the truth table

P	$\neg P$
T	F
F	T

We will write $P \wedge Q$ for “P and Q", the *conjunction* of two sentences. This is true precisely when both of the constituent parts are correct, but false otherwise. This is in line with normal everyday usage of the word “and”. Nobody would deny that I am telling the truth if I say

$$(2 + 2 = 4) \wedge (3 + 3 = 6)$$

nor would anyone hesitate to call me a liar if I boldly announced that

$$(2 + 2 = 4) \wedge (3 + 3 = 5).$$

Here is the truth table for the conjunction $P \wedge Q$:

P	Q	$P \wedge Q$
T	T	T
T	F	F
F	T	F
F	F	F

We write $P \vee Q$ for “P or Q". The symbol $\vee$ is called *disjunction.* There is a bit of a surprise when we consider the mathematical usage of the word “or”. This is because it is often used in ordinary language to mean the same as “either...or”, excluding the possibility of two things being true at the same time. In mathematics, however, we use the word “or” in the sense of “at least one, possibly both”. Thus all three statements

$$(2+2=4)\vee(3+3=5)$$
$$(2+2=5)\vee(3+3=6)$$
$$(2+2=4)\vee(3+3=6)$$

are true. The only “or” statement that is false is the one with both component parts false, as for example

$$(2+2=5)\vee(3+3=5).$$

In ordinary conversation, if I say “I will take you to the movies or buy you a candy bar”, you would be probably satisfied if I did either one, but I’m sure you wouldn’t call me a liar if I did both. That is an illustartion of the proper usage of “or” in the mathematical sense. The truth table of the disjunction $P \vee Q$ is

P	Q	$P \vee Q$
T	T	T
T	F	T
F	T	T
F	F	F

You may detect a note of arbitrariness in our cavalier description of how the word “or” is to be used. There are, however, good reasons for this choice, and most mathematicians use this interpretation in textbooks and journal articles. Also, this particular way of employing the disjunction allows for some nice relationships between the logical connectives, much like the basic identities and laws of algebra that you may be familiar from previous experience.

A sentence of the form “if P then Q" is written symbolically $P \Rightarrow Q$ and it is called a *conditional* or *implication.* We can also read P implies Q, P only if Q, P is sufficient for Q, or Q is necessary for P. Some authors use the notation $P \to Q$. The sentence P is called the *hypothesis* or the *antecedent* , and Q is the *conclusion* or the *consequent.*

An “if...then” statement is more precisely defined when used in a logical context than when casually bandied about in ordinary speech. For our purposes, it is most important to understand that *any* two statements can be joined together to form a conditional; the individual parts can be true or false. We will say that a conditional is false when the antecedent is true and the consequent is false (and these two eventualities eventuate, not eventually, but simultaneously!). In all other situations, the conditional is taken to be true. Thus a conditional is understood to be true whenever the sentence following “if” and preceding “then” is false. As this convention may shock your tender sensibilities, we will try to motivate our reasons for choosing it by relating to some examples.

Perhaps it will help if you think of a statement of the form $P \Rightarrow Q$ as a promise with a condition (in fact, this is why such statements are called *conditionals*). The promised end need not be true unless the condition is met. Suppose I promise that you will get an A in the class IF you have an average which is 90% or greater. If I am not lying, then you will certainly expect an A if your average is 92.3%. You will, of course, be upset and complain if you breeze through with a 90% average and I give you a B. And you will justified in your reaction. But if your average is 89%, I can give you any grade I want without breaking my promise. The question of what will occur for an average under 90% is simply not addressed by the promise as stated. To be more specific, suppose P is the statement "your average is 90% or better" and Q represents "your grade is A". The promise is symbolized as $P \Rightarrow Q$. Consider the four possible outcomes at semester's end:

1. Your average is 92.3% and your grade is A.
2. Your average is 92.3% and your grade is B.
3. Your average is 89% and your grade is A.
4. Your average is 89% and your grade is B.

In the context of my promise, the only blatant lie arises from sitution number 2. I have kept my promise in all three of the other cases. When you fail to fulfill your part in the bargain, as when your average is 89%, you may be resigned to the fact that you will get a B, but I do not suddenly become a liar if, because of generosity or because I'm such a swell guy, I choose to give you the A.

Comedians have known about and used the mathematical interpretation of a conditional statement for a long time. Here it is:

"If you had two million dollars, would you give me one million?"

"Of course!"

"If you had two thousand dollars, would you give me one thousand?"

"Certainly!"

"If you had twenty dollars, would you give me ten?"

"No way!"

"Why not?"

"Because I have twenty dollars!"

The whole point is the idea that, without lying, one can promise *anything* in a conditional fashion, provided that the condition is not fulfilled. An important point is that the statement $P \Rightarrow Q$ does NOT guarantee anything about the truth of P or Q individually. The truth of a conditional merely expresses a connection between a hypothesis and a conclusion. Even if the conditional is true, you know that Q is correct ONLY after you have determined that P is correct.

Here is another example to illustrate that a false statement implies anything: let's prove both

$$\text{(1) if } 2+2=5, \text{ then } 3=0, \quad \text{and (2) if } 2+2=5, \text{ then } 3=3.$$

We start with the antecedent and, applying valid algebraic principles, we try to reach the conclusion. Let's start with (1): If $2+2=5$, then $4=5$. By subtracting 5 from both sides, we get $-1=0$. Multiplying both sides with -3, we get $3=0$. What do you think? Did we prove that $3=0$? Of course not. We proved it from a false assumption. The entire statement (1) must be regarded as true.

For (2), we have the hypothesis $2+2=5$. Multiply both sides by 0 and add 3 to both sides. We obtain a valid result $3=3$ from an erroneous assumption.

To summarize, the truth table for the conditional $P \Rightarrow Q$ is

P	Q	$P \Rightarrow Q$
T	T	T
T	F	F
F	T	T
F	F	T

We write $P \Leftrightarrow Q$ for "P if and only if Q", and call it a *biconditional* or *equivalence.* We can also read P is equivalent to Q or P is necessary and sufficient for Q. Some people use the notation $P \leftrightarrow Q$. The expression "if and only if" is often abreviated as "iff". A biconditional is used when we intend to express the idea that two statements surrounding it say the same thing, albeit in different ways. Since, at this stage, we are concerned only with truth and falsity, we agree that the statement $P \Leftrightarrow Q$ asserts that P and Q are both true or both false. As usual, we must understand that merely stating a biconditional does not make it true. Also, we do not make any a priori restrictions on the kinds of sentences which may be joined by the symbol $\Leftrightarrow$. There may or may not be a perceivable relation between the component parts of such a sentence. For our purposes, the decision as to truth or falseness of the whole is determined solely by an examination of the constituent parts. Thus the statement

$$(2+2=4) \Leftrightarrow (7 \text{ divides } 1001)$$

is true. Never mind that you see no rhyme or reason for putting the two parts together. When two true sentences are made one by using the words "if and only if", the result is understood to be true. What do you think about the following sentence? True or false?

$$(7<5) \Leftrightarrow (\text{Don Pfaff played Han Solo in Star Wars}).$$

Both component parts are false. Thus they convey the same information, even though that information is wrong in both cases. The entire statement is true. It asserts nothing about whether the individual parts are correct, only that they are equivalent with respect to their truth values.

The sentence

$$(2+2=4) \Leftrightarrow (1=0)$$

is false, since the parts have not the same truth value. A biconditional is false just in case one of the component parts is right and the other is wrong. We have the following truth table for $P \Leftrightarrow Q$:

P	Q	$P \Leftrightarrow Q$
T	T	T
T	F	F
F	T	F
F	F	T

1.3. Logical equivalence

A truth table will show us that $P \Rightarrow Q$ is logically equivalent to $(\neg P) \vee Q$, in the sense that they have the same truth values in all cases. It is also logically equivalent to $(\neg Q) \Rightarrow (\neg P)$. Indeed,

P	Q	$\neg P$	$\neg Q$	$(\neg P) \vee Q$	$(\neg Q) \Rightarrow (\neg P)$	$P \Rightarrow Q$
T	T	F	F	T	T	T
T	F	F	T	F	F	F
F	T	T	F	T	T	T
F	F	T	T	T	T	T

The statement $(\neg Q) \Rightarrow (\neg P)$ is called the *contrapositive* of $P \Rightarrow Q$.

A truth table shows that $P \Leftrightarrow Q$ is logically equivalent to $(P \Rightarrow Q) \wedge (Q \Rightarrow P)$. The statement $Q \Rightarrow P$ is called the *converse* of $P \Rightarrow Q$. The contrapositive and the converse of a statement will be illustrated in the next chapter, when we talk about several techniques of proof.

Let A be a proposition formed from propositions $P, Q, R, ...$ using the logical connectives. The proposition A is called a *tautology* if A is true for every assignment of truth values to $P, Q, R, ...$ For example, $P \wedge Q \Rightarrow P$ is a tautology. The proposition A is called a *contradiction* if A is false for every assignment of truth values to $P, Q, R, ...$ For example, $P \wedge (\neg P)$ is a contradiction. The negation of any tautology is a contradiction.

By definition, two statements S_1 and S_2 are logically equivalent exactly when $S_1 \Leftrightarrow S_2$ is a tautology. We will write $S_1 \equiv S_2$ if S_1 and S_2 are logically equivalent. For example, $P \wedge P \equiv P$ and $P \wedge Q \equiv Q \wedge P$.

Theorem 1.2. *We have the following basic logical equivalences:*

a) associative laws: $P \wedge (Q \wedge R) \equiv (P \wedge Q) \wedge R, \quad P \vee (Q \vee R) \equiv (P \vee Q) \vee R$

b) commutative laws: $P \Leftrightarrow Q \equiv Q \Leftrightarrow P, \quad P \wedge Q \equiv Q \wedge P, \; P \vee Q \equiv Q \vee P$

c) idempotency laws: $P \wedge P \equiv P, \quad P \vee P \equiv P$

d) absorption laws: $P \wedge (P \vee Q) \equiv P, \quad P \vee (P \wedge Q) \equiv P$

e) distributive laws: $P \wedge (Q \vee R) \equiv (P \wedge Q) \vee (P \wedge R), \quad P \vee (Q \wedge R) \equiv (P \vee Q) \wedge (P \vee R)$

f) law of double negation $\neg(\neg P) \equiv P$

g) De Morgan laws: $\neg(P \wedge Q) \equiv (\neg P) \vee (\neg Q), \quad \neg(P \vee Q) \equiv (\neg P) \wedge (\neg Q).$

h) Contrapositive law $P \Rightarrow Q \equiv (\neg Q) \Rightarrow (\neg P).$

Proof. Indeed, we can check that the truth tables are the same. We will illustrate this with part g; the other parts are similar.

P	Q	$P \wedge Q$	$\neg(P \wedge Q)$	$\neg P$	$\neg Q$	$(\neg P) \vee (\neg Q)$
T	T	T	F	F	F	F
T	F	F	T	F	T	T
F	T	F	T	T	F	T
F	F	F	T	T	T	T

P	Q	$P \vee Q$	$\neg(P \vee Q)$	$\neg P$	$\neg Q$	$(\neg P) \wedge (\neg Q)$
T	T	T	F	F	F	F
T	F	T	F	F	T	F
F	T	T	F	T	F	F
F	F	F	T	T	T	T

□

When a long sentence contains one or more parts that are themselves compound sentences, parentheses may be needed. For example, $(\neg P) \wedge (P \vee Q)$ is different form $\neg(P \wedge (P \vee Q))$. You can check this by looking at their truth tables.

Remark 1.3. We have the following negation rules for quantifiers:

$$\neg(\forall x\ P(x)) \equiv \exists x\ \neg P(x), \quad \neg(\exists x\ P(x)) \equiv \forall x\ \neg P(x).$$

Remark 1.4. If $\forall x\ (P(x) \Rightarrow Q(x))$ is false, then $\exists x\ \neg(P(x) \Rightarrow Q(x))$ is true.

Let a such that $\neg(P(a) \Rightarrow Q(a))$ is true. This a will be called a *counterexample* for $\forall x\ (P(x) \Rightarrow Q(x))$.

Note also that $\exists! x\ P(x)$ is equivalent to $(\exists x\ P(x)) \wedge (\forall y\ (P(y) \Rightarrow y = x))$. Therefore, the negation of $\exists! x\ P(x)$ is $(\forall x(\neg P(x))) \vee (\exists y(P(y) \wedge y \neq x))$.

When we write proofs, it is important to make valid arguments. We say that B is a valid consequence of $A_1, A_2, ..., A_n$ if for every assignment of truth values that makes all the $A_1, A_2, ..., A_n$ true, B is also true.

For example, if A_1 is the statement "x is odd", A_2 is "y is odd" and B is "$x+y$ is even", then $A_1 \wedge A_2 \Rightarrow B$. Of course, if we start with wrong premises or we use wrong reasoning, we may end with wrong conclusions.

Example 1.5. Consider the statement "If $x = 1$ then $x = 0$" with the following "proof": Multiplying both sides of the equation $x = 1$ by x we obtain $x^2 = x$, hence $x^2 - x = 0$. Factoring we get $x(x-1) = 0$. Dividing by $x - 1$ yields the desired conclusion $x = 0$. The flaw in the argument comes from the fact that for $x = 1$, $x - 1$ becomes 0 and we cannot divide by 0.

Exercise 1.6. Consider the sentence

$$\text{If } 2 < 3 \text{ then } 1 + 1 = 2 \text{ or } 3 + 2 = 6 \text{ and } 5 > 7.$$

This is impossible to read accurately in this form. Use parentheses to construct four meaningful sentences, and determine if they are true or false.

Exercise 1.7. Assume x to be a real number. The statement "If $x < 0$, then $x^2 > 0$ is certainly correct. Now substitute $x = -1$, $x = 0$, and $x = 1$ to obtain three conditionals, and explain why they are true.

Exercise 1.8. Find truth tables for each of the following

a) $\neg(P \wedge Q)$;

b) $\neg[(P \vee Q) \wedge ((\neg P) \ \vee (\neg Q))]$;

c) $\neg(P \vee Q) \vee \neg(Q \wedge P)$;

d) $P \Rightarrow (Q \Rightarrow P)$;

e) $(P \Rightarrow Q) \Rightarrow ((\neg Q) \Rightarrow (\neg P))$;

f) $(P \Rightarrow Q) \Leftrightarrow ((\neg P) \vee Q)$.

Exercise 1.9. Prove the following and find counterexamples for the converse:

a) $(\forall x\ P(x) \vee \forall x\ Q(x)) \Rightarrow \forall x\ (P(x) \vee Q(x))$.

b) $\exists x\ (P(x) \wedge Q(x)) \Rightarrow \exists x\ P(x) \wedge \exists x\ Q(x)$.

c) $\forall x\ (P(x) \Rightarrow Q(x)) \Rightarrow (\forall x\ P(x) \Rightarrow \forall x Q(x))$.

d) $(\exists x\ P(x) \Rightarrow \exists x\ Q(x)) \Rightarrow \exists x (P(x) \Rightarrow Q(x))$.

Exercise 1.10. Show that the following are tautologies: $P \vee \neg P$, $P \Rightarrow P$, $P \Leftrightarrow P$.

Exercise 1.11. Are the following tautologies?

a)$((P \Rightarrow Q) \wedge P) \Rightarrow Q$,

b)$(P \Rightarrow Q) \vee (Q \Rightarrow P)$,

c)$((P \Rightarrow Q) \Rightarrow Q) \Rightarrow P$,

d)$(P \Rightarrow Q) \Rightarrow ((\neg P) \Rightarrow (\neg Q))$.

Exercise 1.12. Construct a truth table for $(P \vee Q) \Rightarrow (P \wedge \neg Q)$. Find a simpler proposition that is logically equivalent.

Exercise 1.13. Are the following arguments valid?

a) If a function f is differentiable, then f is continuous. Assume f is continuous. Therefore, f is differentiable.

b) If f is not continuous, then f is not differentiable. Assume f is differentiable. Therefore, f is continuous.

c) If a function f is differentiable, then f is continuous. Assume f is not differentiable. Therefore f is not continuous.

Exercise 1.14. Suppose we are given the following facts:

(a) I will be admitted to Greatmath University only if I am smart.

(b) If I am smart then I do not have to work hard.

(c) I have to work hard.

What can be deduced?

Chapter 2

Proofs: Structures and strategies

In this chapter, we discuss different methods of proofs, illustrating the rules of logic that we learned in the previous chapter. We will consider many simple examples of proofs; more involved examples will appear in the subsequent chapters, after new concepts will be introduced.

2.1. Direct proof

The pattern of a *direct proof* is as follows: suppose P is true and $P \Rightarrow Q$ is true. Then Q is true. This is also called the rule of *modus ponens.* If we deal with theorems in the form of conditional statements, a direct proof might be appropriate.

Example 2.1. If two integers are odd, then their product is odd.

Proof. Let $a = 2m+1, b = 2n+1$ for some integers m, n. Then $a \cdot b = (2m+1)(2n+1) = 4mn+2m+2n+1 = 2(2mn+m+n)+1 = 2k+1$, where $k = 2mn+m+n$. □

Exercise 2.2. Use the above example to prove: If x is odd, then x^2 is odd.

Example 2.3. If x, y are positive real numbers, then $x + y \geq 2\sqrt{xy}$.

Proof. We rewrite the inequality as $x + y - 2\sqrt{xy} \geq 0$. This is equivalent to $(\sqrt{x})^2 + (\sqrt{y})^2 - 2\sqrt{x}\sqrt{y} \geq 0$ or $(\sqrt{x} - \sqrt{y})^2 \geq 0$, which is true. □

Notice that we used the fact that x, y are positive. For $x = y = -1$, check that the inequality is false.

Example 2.4. Let $a \neq 0$. If $b^2 - 4ac \geq 0$, prove that the quadratic equation $ax^2 + bx + c = 0$ has real roots.

Proof. Dividing by a we get $x^2 + \frac{b}{a}x + \frac{c}{a} = 0$. The idea is to complete the square:

$$x^2 + 2\frac{b}{2a}x + \left(\frac{b}{2a}\right)^2 + \frac{c}{a} - \left(\frac{b}{2a}\right)^2 = 0,$$

$$\left(x + \frac{b}{2a}\right)^2 = \frac{b^2 - 4ac}{4a^2}.$$

Since $b^2 - 4ac \geq 0$, we can solve the last equation and get

$$x + \frac{b}{2a} = \pm\frac{\sqrt{b^2 - 4ac}}{2a}, \quad x = -\frac{b}{2a} \pm \frac{\sqrt{b^2 - 4ac}}{2a}.$$

□

Exercise 2.5. Use a direct proof to prove the statements

a. If x is odd, then x^3 is odd.

b. If a divides b and a divides c, then a divides $b + c$ (recall that a divides b if $b = au$ for some integer u).

c. If $x^2 + 5y = y^2 + 5x$, then $x = y$ or $x + y = 5$.

2.2. Contrapositive proof

A conditional statement of the form $P \Rightarrow Q$ may also be proved using a *contrapositive proof.* The idea is to prove the logically equivalent statement $(\neg Q) \Rightarrow (\neg P)$, which sometimes is easier.

Example 2.6. Let n be an integer. If n^2 is odd, then n is odd.

Proof. We prove: if n is even, then n^2 is even, which is easier. Indeed, $n = 2k$ implies $n^2 = 4k^2 = 2 \cdot 2k^2$. □

Try to give a direct proof of the same statement and compare.

Example 2.7. Let x, y be integers. If 3 does not divide xy, then 3 does not divide x and 3 does not divide y.

Proof. By De Morgan laws of negation (see Theorem 1 part g in Logic), we prove: if 3 divides x or 3 divides y, then 3 divides xy. In the case $x = 3a$, we get $xy = 3ay$ and 3 divides xy. In the second case, $y = 3b$ and $xy = 3xb$, so 3 divides xy. □

Exercise 2.8. Use the method of contrapositive proof to prove the following. In each case, think also of a direct proof, and compare them:

a. If $x^2 + 5x < 0$, then $x < 0$.

b. If both ab and $a + b$ are even, then both a and b are even.

c. If a^2 is not divisible by 4, then a is odd.

2.3. Proof by contradiction

Another method of proving conditional statements $P \Rightarrow Q$ is the *proof by contradiction*. We assume that $P \Rightarrow Q$ is false, and try to get a contradiction, usually a statement like $R \wedge (\neg R)$. Recall that $P \Rightarrow Q$ is logically equivalent to $(\neg P) \vee Q$, so its negation is $P \wedge (\neg Q)$.

Example 2.9. If a, b are integers, then $a^2 - 4b$ can not be equal to 2.

Proof. Assume the implication is false, namely that there exist integers a, b such that $a^2 - 4b = 2$. We get $a^2 = 4b + 2 = 2(2b + 1)$, so a must be even, say $a = 2c$. Plugging back in the equality $a^2 - 4b = 2$ we get $4c^2 - 4b = 2$ or $4(c^2 - b) = 2$, which says that 2 is a multiple of 4, contradiction. Something went wrong, so it must be that there are no integers a, b such that $a^2 - 4b = 2$. □

In fact, the proof by contradiction can be applied to other statements, not necessarily conditional statements.

Example 2.10. $\sqrt{2}$ is irrational (not of the form a/b with a, b integers and $b \neq 0$).

Proof. First recall that $\sqrt{2}$ is a positive number such that $(\sqrt{2})^2 = 2$. Assume $\sqrt{2}$ is rational, hence $\sqrt{2} = a/b$, with a, b integers and $b \neq 0$. By simplifying the fraction, we may assume that a and b are relatively prime (the greatest common divisor is 1). We get $a = b\sqrt{2}$. Squaring both sides, $a^2 = 2b^2$, which implies a to be even, say $a = 2n$. But then $4n^2 = 2b^2$, hence $b^2 = 2n^2$ and b must also be even, contradiction. □

Example 2.11. There are infinitely many prime numbers (here an integer p is prime if $p \geq 2$ and the only divisors are 1 and p).

Proof. For the sake of contradiction, suppose there are only finitely many primes, call them $p_1, p_2, ..., p_n$, where $p_1 < p_2 < ... < p_n$, so p_n is the largest. Consider the number $a = p_1 p_2 \cdots p_n + 1$. Like any natural number, a has a prime divisor, say p_k. We get

$$p_1 p_2 \cdots p_k \cdots p_n + 1 = c p_k.$$

Dividing both sides by p_k, it follows

$$\frac{p_1 p_2 \cdots p_n}{p_k} + \frac{1}{p_k} = c,$$

which implies that $1/p_k$ is an integer, contradiction. □

Exercise 2.12. Prove by contradiction the following statements. In each case, think also about a direct proof or a contrapositive proof, if possible.

a. If a, b are integers, then $a^2 - 4b \neq 3$.

b. $\sqrt{6}$ is irrational.

c. $\sqrt{2} + \sqrt{3}$ is irrational.

d. If a is rational and ab is irrational, then b is irrational.

e. If $a, b, \sqrt{a} + \sqrt{b}$ are rational numbers, then $\sqrt{a}, \sqrt{b}$ are also rational.

Exercise 2.13. Prove that $\sqrt{2} + \sqrt{6} < \sqrt{15}$ by contradiction.

2.4. Combining the methods of proof

How about the proof of a biconditional statement $P \Leftrightarrow Q$? There are two steps: we prove first $P \Rightarrow Q$ and then $Q \Rightarrow P$. For these,we may use any method we learned so far: direct proof, contrapositive proof or proof by contradiction.

Example 2.14. Suppose a, b are integers. Then 10 divides $a - b$ if and only if 2 divides $a - b$ and 5 divides $a - b$.

Proof. We use a direct proof for both implications. If 10 divides $a - b$, then certainly 2 divides $a - b$ and 5 divides $a - b$, since 2 and 5 divide 10.

Assuming that 2 divides $a - b$ and 5 divides $a - b$, we get $a - b = 2c = 5d$ for some c, d. Since 2 and 5 are relatively prime, it must be that 5 divides c, hence $c = 5e$ and $a - b = 10e$. □

Sometimes, we may have to prove that several statements are equivalent, like

$$P \Leftrightarrow Q \Leftrightarrow R \Leftrightarrow S.$$

We can use a circle of implications like $P \Rightarrow Q \Rightarrow R \Rightarrow S \Rightarrow P$ or split the equivalences into smaller groups.

Example 2.15. In Linear Algebra we have the following theorem

Suppose A is an $n \times n$ matrix with real entries. The following are equivalent

1) A is invertible

2) The equation $A\mathbf{x} = \mathbf{b}$ has a unique solution for every $\mathbf{b} \in \mathbb{R}^n$

3) The equation $A\mathbf{x} = \mathbf{0}$ has only the trivial solution

4) The reduced row echelon form of A is I_n

5) $\det(A) \neq 0$

6) 0 is not an eigenvalue for A.

Proof. The pattern of proof is the following:

$$1 \Rightarrow 2 \Rightarrow 3 \Rightarrow 6 \Rightarrow 4 \Rightarrow 1; 1 \Leftrightarrow 5.$$

For all terminology, consult your Linear Algebra book.

$1 \Rightarrow 2$. Assume A has an inverse A^{-1}. By multiplying with A^{-1} on the left the equation $A\mathbf{x} = \mathbf{b}$ we get $A^{-1}A\mathbf{x} = \mathbf{b}$ or $\mathbf{x} = A^{-1}\mathbf{b}$, so indeed the equation $A\mathbf{x} = \mathbf{b}$ has a unique solution, namely $\mathbf{x} = A^{-1}\mathbf{b}$.

$2 \Rightarrow 3$. We consider $\mathbf{b} = \mathbf{0}$ in the equation $A\mathbf{x} = \mathbf{b}$. We get that the equation $A\mathbf{x} = \mathbf{0}$ has only the solution $\mathbf{x} = A^{-1}\mathbf{0} = \mathbf{0}$, namely the trivial solution.

$3 \Rightarrow 6$. Indeed, the equation $A\mathbf{x} = 0 \cdot \mathbf{x} = \mathbf{0}$ has only the solution $\mathbf{x} = \mathbf{0}$, which is not acceptable as an eigenvector. Hence 0 is not an eigenvalue for A.

$6 \Rightarrow 4$. Since 0 is not an eigenvalue for A, it follows that A has n pivots, so the reduced row echelon form is I_n.

$4 \Rightarrow 1$. Suppose that A has reduced row echelon form I_n. That means that there are elementary matrices $E_1, ..., E_p$ corresponding to row operations such that $E_p \cdots E_1 A = I_n$. Then $A^{-1} = E_p \cdots E_1$, so A is invertible.

$1 \Rightarrow 5$. Suppose A is invertible. Then by performing row operations, we can find un upper triangular matrix U which is the row echelon form of A. Using the properties of the determinant, we get $\det A = \pm \det U \neq 0$, since $\det U$ is the product of the diagonal entries and A has n pivots.

$5 \Rightarrow 1$. We prove the contrapositive. Assume A not invertible. Then in the row echelon form U there is a zero diagonal entry, and hence $\det A = \pm \det U = 0$.

Exercise 2.16. Let $a \neq 0$. Prove that the quadratic equation $ax^2 + bx + c = 0$ has distinct real roots if and only if $b^2 - 4ac > 0$.

□

2.5. Proof by cases

Some proofs are based on analyzing all possible cases.

Example 2.17. Prove that the set of real solutions of $|x-1| < |x-3|$ is $(-\infty, 2)$.

Proof. Recall that for a real number x the absolute value is defined by

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

Case $x \geq 3$. The inequality becomes $x - 1 < x - 3$, so $-1 < -3$, which is false. This case gives no solution.

Case $1 \leq x < 3$. The inequality becomes $x - 1 < 3 - x$, so $2x < 4$, or $x < 2$. We get $[1, 2)$ as a solution set.

Case $x < 1$. We obtain $1 - x < 3 - x$, or $1 < 3$, which is true. We also get $(-\infty, 1)$ as part of the solution.

The conclusion is that $x \in [1, 2)$ or $x \in (-\infty, 1)$, so $x \in (-\infty, 2)$. □

Example 2.18. Show that n^4 ends in $0, 1, 5$ or 6 for any positive integer n.

Proof. Indeed, let's first find the last digit of n^4 for $n \in \{0, 1, 2, ..., 9\}$. We have $0^4 = 0, 1^4 = 1, 2^4 = 16, 3^4 = 81, 4^4 = 256, 5^4 = 625, 6^4 = 36 \cdot 36$ ends in 6, $7^4 = 49 \cdot 49$ ends in 1, $8^4 = 64 \cdot 64$ ends in 6, $9^4 = 81 \cdot 81$ ends in 1. We conclude that the last digit of n^4 is $0, 1, 5$ or 6 for any positive integer n. □

Exercise 2.19. Solve the inequality $|x + 2| < |x^2 - 1|$.

2.6. Existence proofs

To prove a statement of the form $\exists x P(x)$, where x is a number, one can try to construct directly a value x_0 such that the statement $P(x_0)$ is valid. If this is not possible, we can try proving that the negation of $\exists x P(x)$ is false.

Example 2.20. Show that there is a real number x such that $x^2 = 3$.

Proof. We can directly check that $x_0 = \sqrt{3}$ works. Of course, $x_1 = -\sqrt{3}$ is another choice. □

Exercise 2.21. Prove that there is a prime number between 100 and 200.

Another method to prove $\exists x P(x)$ is by contradiction: we assume that the negation of the statement holds, in other words assume that $\forall x \neg P(x)$, and derive a contradiction.

Example 2.22. Let a be a positive real number. Prove that there is x_0 such that $x_0^2 = a$.

Proof. Suppose that for any real number x we have $x^2 \neq a$. Consider the continuous function $f(x) = x^2 - a$. The assumption implies that $f(x) \neq 0$ for all x. But $f(a+1) = a^2 + a + 1 > 0$ while $f(0) = -a < 0$, which contradicts the Intermediate Value Theorem from Calculus. □

Example 2.23. Prove that there is a positive integer n such that $2^{2^n} + 1$ is not a prime.

Proof. It turns out that

$$2^{2^1} + 1 = 5, 2^{2^2} + 1 = 17, 2^{2^3} + 1 = 257, 2^{2^4} + 1 = 65537$$

are primes (verify!) but

$$2^{2^5} + 1 = 4294967297 = 641 \cdot 6700417$$

is not, so the statement is true for $n = 5$. The numbers $F_n = 2^{2^n} + 1$ are called Fermat numbers. □

Exercise 2.24. Prove that there is a positive integer n such that $2^n - 1$ is divisible by 11.

Remark 2.25. Although an example is sufficient to prove an existence statement, this is not the case for a conditional statement. The fact that you can find a particular x such that $P(x) \Rightarrow Q(x)$ holds true does not mean that it is true for all x.

2.7. Proof by counterexample

To prove the negation of the statement $\forall x P(x)$, in other words to prove that $\exists x \neg P(x)$, we must find at least one x_0 such that $P(x_0)$ does not hold. Such an object is called a *counterexample* to $P(x)$.

Example 2.26. Prove that the following statement is false: Every continuous function on an interval $[a, b]$ is differentiable on (a, b).

Proof. It suffices to consider $f(x) = |x|$ on the interval $[-1, 1]$ which is continuous, but not differentiable at $0 \in (-1, 1)$. □

Exercise 2.27. Prove the negation of the following statements by giving counterexamples.

a. The sum of two irrational numbers is irrational.

b. The product of two irrational numbers is irrational.

c. If a and b are positive integers and $a \cdot b$ is a perfect square (there is k with $a \cdot b = k^2$), then a and b are perfect squares.

d. We have $\sqrt{a+b} = \sqrt{a} + \sqrt{b}$ for all $a, b \geq 0$.

2.8. Proof by induction

Recall that the principle of *mathematical induction* refers to the following: to prove that a sequence of statements $S(1), S(2), ..., S(n), ...$ is true, it suffices to prove two steps

1. Basis step: $S(1)$ is true,

2. Inductive step: For any (fixed) positive integer $k \geq 1$, if $S(k)$ is true, then $S(k+1)$ is true.

This principle is based on the properties of positive integers, discussed in a separate chapter. We will consider there other forms of induction, like strong induction or complete induction, with more examples.

Example 2.28. For all $n \geq 1$ we have $1 + 2 + \cdots + n = \dfrac{n(n+1)}{2}$.

Proof. We call $S(n)$ the statement to be proved. For $n = 1$ the statement becomes $1 = \dfrac{1 \cdot 2}{2}$, which is true.

Assume $S(k)$ is true, i.e. $1 + \cdots + k = \dfrac{k(k+1)}{2}$. Then

$$1 + \cdots + k + (k+1) = \frac{k(k+1)}{2} + k + 1 = \frac{(k+1)(k+2)}{2},$$

hence $S(k+1)$ is also true.

Since both steps were verified, it follows by induction that $S(n)$ is true for all $n \geq 1$. □

Example 2.29. Suppose x is a real number with $x \neq 1$. Prove that for any positive integer n we have

$$1 + x + \cdots + x^n = \frac{1 - x^{n+1}}{1 - x}.$$

Proof. The basis step is $1 + x = \dfrac{1 - x^2}{1 - x}$, true since $(1 + x)(1 - x) = 1 - x^2$.

Assume $1 + x + \cdots + x^k = \dfrac{1 - x^{k+1}}{1 - x}$ for a fixed $k \geq 1$. Adding x^{k+1} both sides we get

$$1 + x + \cdots + x^k + x^{k+1} = \frac{1 - x^{k+1}}{1 - x} + x^{k+1} = \frac{1 - x^{k+1} + x^{k+1}(1 - x)}{1 - x} =$$
$$= \frac{1 - x^{k+1} + x^{k+1} - x^{k+2}}{1 - x} = \frac{1 - x^{(k+1)+1}}{1 - x}.$$

□

Example 2.30. Prove that for each $n \geq 1$ we have $|\sin(nx)| \leq n \cdot \sin(x)$ for all $x \in [0, \pi]$.

Proof. For $n = 1$ we need to show that $|\sin(x)| \leq \sin(x)$. Since $x \in [0, \pi]$, we have $\sin(x) \geq 0$, hence $|\sin(x)| = \sin(x)$ and the inequality is true.

Assume $|\sin(kx)| \leq k\sin(x)$ for a fixed $k \geq 1$ and $x \in [0,\pi]$. Then

$$|\sin((k+1)x)| = |\sin(kx+x)| = |\sin(kx)\cos(x) + \cos(kx)\sin(x)| \leq$$

$$|\sin(kx)||\cos(x)| + |\cos(kx)||\sin(x)| \leq k\sin(x) + \sin(x) = (k+1)\sin(x).$$

We used the fact that $\sin(a+b) = \sin(a)\cos(b)+\cos(a)\sin(b)$, the triangle inequality $|u+v| \leq |u|+|v|$ and the fact that $|\cos(kx)| \leq 1$ for all $k \geq 1$. The proof by induction is complete. □

Example 2.31. Find the sum of the first n odd positive integers.

Proof. This exercise has two parts: first we need to look for a pattern and guess the formula, and second we prove the formula by induction. We have $1 = 1 = 1^2, 1+3 = 4 = 2^2, 1+3+5 = 9 = 3^2, 1+3+5+7 = 16 = 4^2$, so a good guess for the sum of the first n odd integers looks like

$$1 + 3 + 5 + \cdots + (2n-1) = n^2,$$

and indeed, there are n terms on the left hand side. Obviously, we already know that this is true for $n = 1 : 1 = 1^2$. Assume now that $1 + 3 + \cdots + (2k-1) = k^2$ for a fixed arbitrary $k \geq 1$. Adding $2k+1$ both sides, we get

$$1 + 3 + \cdots + (2k-1) + (2k+1) = k^2 + 2k + 1 = (k+1)^2.$$

We conclude that the conjectured formula is true for any $n \geq 1$. □

Exercise 2.32. Prove by induction that $1 + 5 + 9 + \cdots + (4n-3) = 2n^2 - n$.

Exercise 2.33. Prove by induction that $1^2 + 3^2 + \cdots + (2n-1)^2 = (4n^3 - n)/3$.

Exercise 2.34. For $n \geq 1$, let $s_n = 1^2 + 2^2 + \cdots + n^2$.

a. Compute s_1, s_2, s_3, s_4 and conjecture a general formula for s_n.

b. Prove your formula for s_n by induction.

Exercise 2.35. Consider the Fibonacci numbers f_n, where $f_1 = f_2 = 1, f_n = f_{n-2} + f_{n-1}$ for $n \geq 3$. Prove that

a. $f_{n+1}^2 + 2f_nf_{n+1} = f_nf_{n+1} + f_{n+1}f_{n+2}$.

b. $f_1^2 + f_2^2 + \cdots + f_n^2 = f_nf_{n+1}$.

Exercise 2.36. For each positive integer n and any real number $x \geq -1$ prove by induction that $(1+x)^n \geq 1 + nx$.

Exercise 2.37. Here is a "proof" by induction that any two positive integers are equal. Find the mistake:

For a, b positive integers, $\max(a,b)$ is defined to be the largest of a and b if $a \neq b$, and $\max(a,a) = a$. Let $P(n)$ be the statement: if a and b are positive integers such that $\max(a,b) = n$, then $a = b$. We use induction to prove that $P(n)$ is true for $n \geq 1$. For $n = 1$, since $\max(a,b) = 1$, we get $a = b = 1$. Assume $P(n)$ true. Let a, b such that $\max(a,b) = n+1$. Then $\max(a-1, b-1) = n$. Since we are assuming $P(n)$ true, we get $a - 1 = b - 1$, hence $a = b$. Therefore $P(n+1)$ is true, and by induction $P(n)$ is true for all $n \geq 1$. As a consequence, any two positive integers a, b are equal.

Exercise 2.38. Suppose f is a function defined on the set of real numbers such that $f(x+y) = f(x) + f(y)$ for all x, y. Prove by induction that $f(kx) = kf(x)$ for any positive integer k. Conclude that $f(x/n) = f(x)/n$ and that $f(mx/n) = mf(x)/n$ for all positive integers m, n.

Exercise 2.39. Prove by induction that

$$1 \cdot 2 + 2 \cdot 3 + 3 \cdot 4 + \cdots + n(n+1) = \frac{n(n+1)(n+2)}{3}.$$

Exercise 2.40. Prove by induction that

$$(1 + 2^5 + \cdots + n^5) + (1 + 2^7 + \cdots + n^7) = 2\left[\frac{n(n+1)}{2}\right]^4.$$

Exercise 2.41. Prove by induction that the sum of internal angles in an n-sided polygon is $(n-2)\pi$.

Exercise 2.42. If we draw n straight lines in the plane, no three going through the same point, and no two parallel, how many regions do they determine in the plane? Prove by induction that the formula is $(n^2 + n + 2)/2$.

Exercise 2.43. Some straight lines are drawn in the plane, forming regions. Show that it is possible to color each region either red or blue, in such a way that no two neighboring regions (regions separated by a line segment or a halfline) have the same color.

Chapter 3

Elementary theory of sets

When you study physics, economics, psychology, mathematics, or any other subject, there are certain key words which you must learn to use correctly. You may not completely understand them when you begin, but continued usage helps you become familiar with them. In some cases, a perfectly precise definition of a term may never be available, but with experience you may be able to understand and use the idea represented by the term. For example, it is very difficult to pin down exactly what "force" is, but enough is known about force that all sorts of things can be proved about it.

In the same way, when we investigate the structure of a mathematical theory, there are always some concepts which are so basic that they do not admit any simple definition. They can really only be understood by the properties they have or, putting it another way, by statements which use them correctly. These basic concepts are referred to by words or symbols that we call "primitive" or "undefined" terms.

The most basic statements we write down (using the undefined terms) are the *Postulates* or *Axioms*. These are often understood to be so obvious that no proof is required, though in a sense that is inadequate as a description. More specifically, we will here understand postulates as statements which are not necessarily true or false, but which are the basis for an ongoing reasoning process.

In a sense, while we are developing a theory, we regard the postulates as true, but whether they really are or not is generally irrelevant to the theory. The typical daily project in mathematics is to discover a consequence of one or more hypotheses and, hopefully, to prove it. In practice, that's what mathematics is all about.

3.1. Axioms for set theory

The notion of a set is a relatively recent development in mathematical history. Created at the end of nineteenth century, the idea of a set has become the cornerstone for virtually all contemporary mathematics. In its simplest form, a set is simply a bunch of things gathered together to form a new entity which is considered to be a single object. The English language is rich in words that could be regarded as synonymous with the word “set”; among them are: collection, group, family, class, club, flock, herd, or team. Note that when we refer to a club, for example, we are not generally thinking of the individual members, but of the totality of all members, presumed to be a single entity. In fact, a club (or team, family, class, etc.) is always referred to in the singular.

We will usually denote the sets by capital letters and we will mostly be interested in sets of mathematical entities like numbers, functions, etc. The fact that an element x belongs to a set A is written $x \in A$. The sets can be specified by the roster notation using braces, like $A = \{a, b, c\}$, an enumeration of its elements, or by the set-builder notation, which will be explained below after the Axiom of Separation. When we enumerate the elements, a repetition should count only once. For example, the set $\{1, 2, 3, 1, 2\}$ is the same as $\{1, 2, 3\}$.

Example 3.1. The following are examples of sets

$$A = \{a, b, c, d, ..., z\}, B = \{\{1, 2, 5\}, +, -, A\},$$

$$C = \{2, 4, 6, ...\}, D = \{..., -2, -1, 0, 1, 2, ...\}.$$

Note that $10 \in C$ but $3 \notin C$. The dots here indicate that the list continues indefinitely. You may recognize that C is the set of even positive integers, and D is the set of integers, also denoted by $\mathbb{Z}$.

A set could be an element of another set. For example, notice that $\{1, 2, 5\} \in B$ and $A \in B$.

The main things that are needed in talking about sets are knowledge as to when sets are really the same and how to form sets. These are addressed in Axioms 1 and 2 below. Later, we will add a third axiom, called the Axiom of Choice. This will be explained in the next chapter.

Axiom 1 (The Axiom of Extent).

$$(A = B) \Leftrightarrow \forall x\ (x \in A \Leftrightarrow x \in B).$$

This axiom asserts that equality of sets is determined by the members of the sets and by no other criteria. Thus if A is described as the set of even integers and B is the set of all numbers that are obtained by increasing odd numbers by 1, then we are really dealing with the same set, even though the definitions of A and B are different.

In view of the Axiom of Extent, in order to prove that two sets are equal we must show two separate things, namely that each element of one set is also in the other and vice versa. This will usually be accomplished by breaking the proof into two parts. The first part will begin with a hypothesis of the form $x \in A$, from which the conclusion $x \in B$ will be drawn. The second part amounts to the converse of this. A proof of equality for sets is incomplete until the sentences $x \in A$ and $x \in B$ are shown to be equivalent.

Axiom 2 (The Axiom of Set Formation, or Axiom of Separation). If $S(x)$ is an open sentence in x (or predicate), then there is a set whose elements are exactly those x for which $S(x)$ is true. In symbols,

$$\exists A\ \forall x\ (x \in A \Leftrightarrow S(x)).$$

Because Axiom 2 allows formation of a set by collecting together all objects that make an open sentence true, you can see why the set formed is often called the *truth set* or *solution set* of the open sentence. Notice, however, that uniqueness of the solution set is not explicitly stated in Axiom 2.

As it happens, though, putting our two axioms together does show that the set formed in Axiom 2 is unique.

Theorem 3.2. $\exists! A\ \forall x\ (x \in A \Leftrightarrow S(x))$.

The fact that there is a set A satisfying the condition $x \in A \Leftrightarrow S(x)$ follows directly from Axiom 2. Now suppose A_1 and A_2 are any sets like A. Then we have

$$x \in A_1 \Leftrightarrow S(x) \Leftrightarrow x \in A_2.$$

Since the relation $\Leftrightarrow$ is transitive, in the sense that $P \Leftrightarrow Q$ and $Q \Leftrightarrow R$ implies $P \Leftrightarrow R$, we get $A_1 = A_2$ by Axiom 1.

In mathematics, when we know that something of interest exists and is unique, it is usually appropriate to give it a name. Thus we now introduce the standard notation for the truth set of an open sentence.

Definition 1. If $S(x)$ is an open sentence, the set A mentioned in the above theorem is denoted by $A = \{x : S(x)\}$. This is the set-builder notation (read: the set of all x such that $S(x)$).

Remark 3.3. The idea of set builder notation works two ways. First, if you know that a is an element such that the sentence $S(a)$ is true, then it follows that a is an element of A. For example, since $2^3 - 2 = 6$, we know that $2 \in \{x : x^3 - x = 6\}$. Second, if you are presented with an element of A, then you know that the condition defining the set A is true. An example of this is that if you happen to run across an object, say b, which is definitely in $\{x : x^3 - x - 1 = 0\}$, even if you don't know a precise value for it, you can say with confidence that $b^3 - b - 1 = 0$.

Here is another, more symbolic way, of expressing what was said above:

Theorem 3.4. $\forall a\ (a \in \{x : S(x)\} \Leftrightarrow S(a))$.

3.2. Inclusion of sets

As we have seen, Axiom 1 deals with equality of sets. We define now the notion of subset, which illustrates the idea of a smaller set sitting inside a bigger set. More precisely,

Definition 2. We say that A is a subset of B or that A is contained in B whenever $\forall x(x \in A \Rightarrow x \in B)$. We write $A \subseteq B$. We may also express this by saying that B is a superset of A and write $B \supseteq A$. If $A \subseteq B$ and $A \neq B$, we say that A is a proper subset of B, and we write $A \subset B$.

Example 3.5.

$$\{1, 2, 3\} \subseteq \{1, 2, 3, 5\},\ \mathbb{N} \subseteq \mathbb{Z}.$$

Our choice of notation is parallel with inequality $\leq$ and strict inequality $<$ of numbers. **Warning**: some authors use $\subset$ for inclusion, and $\subsetneq$ for proper inclusion.

Note how the definition of subset resembles Axiom 1; the only difference is that the biconditional has been replaced by a single conditional. This means that being a subset of is a weaker notion than being equal to. In fact, A will be a subset of B if and only if all the elements of A are also elements of B. Note that the converse may not be true.

Here are the fundamental properties about the notion of subset.

Theorem 3.6. *The inclusion of sets has properties*

1. *Reflexivity: For all A, $A \subseteq A$.*
2. *Antisymmetry: $(A \subseteq B) \wedge (B \subseteq A) \Leftrightarrow A = B$.*
3. *Transitivity: $(A \subseteq B) \wedge (B \subseteq C) \Rightarrow A \subseteq C$.*

Proof. 1. This is clear, since $x \in A$ implies $x \in A$.

2. This is exactly the double implication used in Axiom 1 to conclude that two sets are equal.

3. Suppose $x \in A$. We can apply the subset definition to the first hypothesis and conclude that $x \in B$. But now this new assertion can be used with the second hypothesis to deduce that $x \in C$. This establishes the conditional $x \in A \Rightarrow x \in C$ for every x, so the result follows. □

Since Axiom 2 guarantees that there is a set associated with any open sentence, in particular we can define a set from a condition that can never be satisfied. And why not? After all, sets are often used to describe the solutions of various problems, and some problems have no solutions whatever. In the next definition we use a standard universally false statement to define the set we will refer to as the empty, null, or void set, denoted $\emptyset$.

Definition 3. By definition, $\emptyset = \{x : x \neq x\}$.

To understand the empty set, it might help if you consider the fact that a subset can be gotten from a set by removing some of its elements. If you take them all out, what do you get? Of course, you reach $\emptyset$.

Theorem 3.7. *We have*

1. *$\forall x \; (x \notin \emptyset)$.*
2. *For all A, $\emptyset \subseteq A$.*

Proof. 1. This is true since $\emptyset$ has no element.

2. Substitute $\emptyset$ for A and A for B in the definition of inclusion. Since the right side of the biconditional is a universal statement about an implication whose hypothesis is always false (by Theorem 3.6), it is itself automatically true. Thus we can say that $\emptyset \subseteq B$.

For another proof, suppose that the empty set is not a subset of a certain set A. That means that for some choice of x the sentence $x \in \emptyset \Rightarrow x \in A$ is false. This can only occur if, for this x, we have both $x \in \emptyset$ and $x \notin A$. As there is no element of the empty set, this is a contradiction. It must follow that $\emptyset \subseteq A$.

□

Definition 4. Given a set X, the power set $\mathcal{P}(X)$ is defined as

$$\mathcal{P}(X) = \{A : A \subseteq X\},$$

the set of all subsets of X.

Note that $\emptyset, X \in \mathcal{P}(X)$ since $\emptyset \subseteq X$ and $X \subseteq X$.

Example 3.8. $\mathcal{P}(\{a, b, c\}) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}$.

Exercise 3.9. Prove by induction that if X has n elements, then $\mathcal{P}(X)$ has 2^n elements.

Remark 3.10. Obviously, some sets do not contain themselves. For example, let X be the set of integers. Then X is not an element of X, since X is not an intger. A set which contains itself must be a set containing sets as elements. Consider for example the set Y of sets which can be defined using 15 words or less. Clearly Y contains itself. Here is a surprising result, which will convince us that is best to avoid sets which contain themselves.

Theorem 3.11. *(Russell's Paradox) The set $X = \{A : A \notin A\}$ is contradictory.*

Proof. Indeed, if the set X exists, then let's check if $X \in X$ or not. If we assume $X \in X$, then by definition $X \notin X$, contradiction. If we assume $X \notin X$, then we conclude $X \in X$, contradiction. □

In particular, there is no set containing all sets. Such a thing is a new concept, usually called the class of all sets or the category of sets. We are not discussing category theory in this book. For those interested, there is an extensive literature on classes and category theory.

In the next sections, we will define several operations with sets, give examples, and prove the rules of algebra with sets. To avoid Russell's Paradox, it is convenient to assume that all the sets we work with are subsets of a fixed large set U, called the universe. Many times, this set U will be understood from the context.

3.3. Union and intersection of sets

The two basic operations with sets are the *union* and the *intersection*. In the first, we gather together all those objects which appear in at least one of the sets. The second is obtained by putting together the common members of both sets into a single set. Recall that we assume our sets to be subsets of a fixed universe U.

Definition 5. The union of the sets A and B is

$$A \cup B = \{x \in U : x \in A \vee x \in B\}.$$

The intersection of A and B is the set

$$A \cap B = \{x \in U : x \in A \wedge x \in B\}.$$

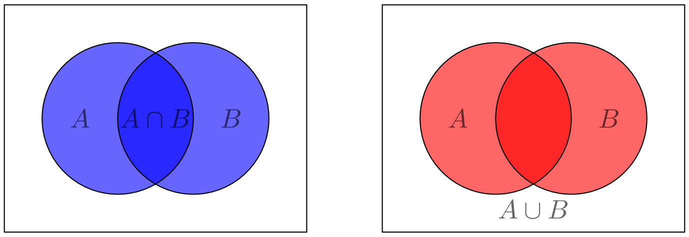


Figure 1. $A \cap B$ and $A \cup B$.

Note especially the conditions written within braces that determine the qualifications required for an object to be a member. Sometimes we visualize these operations with pictures, called Venn diagrams. When we prove theorems about operations with sets, Venn diagrams are a useful visual aid, see Figure 1.

Definition 6. Two sets A, B are called *disjoint* if $A \cap B = \emptyset$.

Example 3.12. Let $A = \{1, 2, c\}$, $B = \{a, b, c\}$ and $C = \{1, x\}$. Then

$$A \cup B = \{1, 2, a, b, c\}, \quad A \cup C = \{1, 2, c, x\}, \quad A \cap B = \{c\},$$
$$A \cap C = \{1\}, \quad B \cup C = \{1, a, b, c, x\}, \quad B \cap C = \emptyset.$$

In particular, B and C are disjoint.

Example 3.13. Consider the sets

$$A = \{n \in \mathbb{Z} : n = 2k \text{ for some } k \in \mathbb{Z}\}, \quad B = \{n \in \mathbb{Z} : n = 3m \text{ for some } m \in \mathbb{Z}\}.$$

Then

$$A \cup B = \{n \in \mathbb{Z} : (n = 2k) \vee (n = 3m) \text{ for some } k, m \in \mathbb{Z}\},$$
$$A \cap B = \{n \in \mathbb{Z} : n = 6r \text{ for some } r \in \mathbb{Z}\}.$$

Here are some properties about intersection of sets.

Theorem 3.14. *For arbitrary sets A, B, C we have*

1. $A \cap A = A$
2. $A \cap B = B \cap A$.
3. $(A \cap B) \cap C = A \cap (B \cap C)$.

Proof. The first thing to realize is that right now, as well as in many other situations, the only way to establish equality of sets is by a two pronged attack. We must, in view of Axiom 1, prove the validity of a biconditional statement, and, as we already mentioned, this is typically done by proving two conditional statements separately.

1. Suppose that $x \in A \cap A$. By definition, $x \in A$ and $x \in A$. Thus $x \in A$. This establishes the implication $x \in A \cap A \Rightarrow x \in A$, and one direction of the desired biconditional is established. Note the logical principle used here: whenever you have a statement of the form $P \wedge Q$ in a proof, you are entitled to simply write down P as a consequence. Of course, you may also properly infer the statement Q.

For the other direction of the biconditional, we now suppose that $x \in A$ and try to prove that $x \in A \cap A$. But this amounts to stating our hypothesis twice (which is surely valid; if a sentence P is true, then forming its conjunction with itself $P \wedge P$ will also produce a true sentence), and then using the definition of intersection.

The two steps used in the above proof are typical of the pattern used to prove equality of sets. You will generally divide the proof into two parts. In the first, introduce a symbol to stand for an arbitrary member of the left-hand set and proceed to show that it must also be in the right-hand set. Then do the reverse by considering a typical element of the right-hand set and proving that it must be in the other set. This technique will be called *proof by double inclusion*, see also part two in Theorem 3.6.

2. Suppose that $x \in A \cap B$. From the definition of intersection, we may infer that $x \in A$ and $x \in B$. But since asserting that two statements are both true can be done by mentioning either one first, it follows that $x \in B$ and $x \in A$ (see the commutative property in Theorem 1 in Logic). Thus $x \in B \cap A$. This completes the first part of the proof, and normally we would write the details of the other direction. This time, however, the proof can be written by simply interchanging the letters A and B in the previous part, so it will be omitted.

3. The proof uses the fact that there is an associative type law for the word "and", see part a) in the same Theorem 1 in Logic, and it will also be omitted. □

Theorem 3.15. *We have*

1. $A \cup A = A$.
2. $A \cup B = B \cup A$.
3. $(A \cup B) \cup C = A \cup (B \cup C)$.

Proof. Exercise. □

As you can see from the preceding results, union and intersection obey some of the more common laws of algebra (think addition and multiplication). In the next theorem, you will see that there are some more similarities, but also some significant differences between real number algebra and set algebra.

Theorem 3.16. *We have*

1. $A \cap (A \cup B) = A$.
2. $A \cup (A \cap B) = A$.
3. $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.
4. $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.

Proof. 1. Suppose $x \in A \cap (A \cup B)$. Then $x \in A$ and $x \in A \cup B$. In particular, $x \in A$, which means that $A \cap (A \cup B) \subseteq A$. On the other hand, assume $x \in A$. By definition of union, we have $x \in A \cup B$. Hence $x \in A \cap (A \cup B)$, and we get $A \subseteq A \cap (A \cup B)$, hence equality by part 2 of Theorem 3.6.

2. Exercise.

3. Let us examine an element of $A \cap (B \cup C)$, call it x. Clearly $x \in A$ and $x \in B \cup C$. Since the last part of the preceding sentence implies that $x \in B$ or $x \in C$, we consider two cases.

a) If $x \in B$, then since we already know that $x \in A$, we clearly have that $x \in A \cap B$. But then the statement

$$x \in A \cap B \vee x \in A \cap C$$

is also true. Thus, by definition of union,

$$x \in (A \cap B) \cup (A \cap C).$$

b) If $x \in C$, then we have virtually the same argument as in part a). Check it out and see for yourself that this is so. Thus in any case, x appears in the right-hand set.

Now choose an element x of $(A \cap B) \cup (A \cap C)$. Clearly $x \in A \cap B$ or $x \in A \cap C$. In either case, we have $x \in A$. However, in the first case x is in B, while in the second case x is an element of C; thus, no matter what, $x \in B \cup C$. Evidently we now know that $x \in A \cap (B \cup C)$, and the second part of the biconditional needed to apply Axiom 1 has been proved.

4. Exercise. □

Exercise 3.17. We have

a. $A \cap \emptyset = \emptyset$.

b. $A \cup \emptyset = A$.

The parts of the following theorem give some relationships between the various concepts described so far. They are fairly useful in everyday reasoning about sets.

Theorem 3.18. *We have*

1. $A \subseteq B \Leftrightarrow A \cap B = A$.

2. $A \subseteq B \Leftrightarrow A \cup B = B$.

3. $A \subseteq A \cup B$.

4. $A \cap B \subseteq A$.

5. $A \subseteq C \wedge B \subseteq C \Rightarrow A \cup B \subseteq C$.

6. $A \subseteq B \wedge A \subseteq C \Rightarrow A \subseteq B \cap C$.

Proof. We will prove part 1 and leave the others as exercise. Notice first that the first statement is expressed as a biconditional, so there will be two parts to the proof. First we will assume that $A \subseteq B$ and use this to prove that $A \cap B = A$. Then we will assume the truth of the equation and prove the inequality without referring to anything we did in the first part. Here goes!

i) Suppose $A \subseteq B$. Since we are trying to establish the equality of two sets, it behooves us to divide this portion of the proof into two parts.

a) Suppose $x \in A \cap B$. Then $x \in A$ and $x \in B$. Hence, $x \in A$.

b) Now suppose $x \in A$. Because we know that $A \subseteq B$, we can invoke the definition of inclusion to conclude $x \in B$. Thus $x \in A \cap B$.

Steps a) and b) together show that

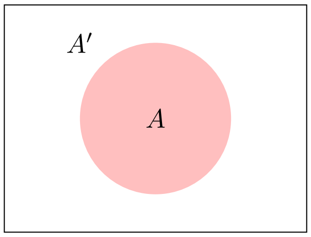
$x \in A \cap B \Leftrightarrow x \in A$, so by Axiom 1 we see that the sets are equal.

ii) Now assume that $A \cap B = A$. We wish to show that $A \subseteq B$. Let $x \in A$. Because A is exactly the same as $A \cap B$, we then know that $x \in A \cap B$. By definition of intersection, we have $x \in B$, and we are done. □

3.4. Complement, difference and symmetric difference of sets

Recall that all our sets are subsets of a universe U.

Definition 7. The complement of the set A is $A' = \{x \in U : x \notin A\}$.



Another notation for the complement is A^c. The complement of A consists of all those objects in U which are not elements of A. For our purposes, it is usually understood what the largest set U under consideration is, and complements are taken with respect to that set. Thus if we were studying the positive integers and we would consider $\{x : x < 5\}'$, then we would be referring to the set $\{5, 6, 7, ...\}$, whereas in a discussion of the set of digits in base eight $\{0, 1, 2, ..., 7\}$, then $\{x : x < 5\}'$ would be the set $\{5, 6, 7\}$.

The next theorem is the set-theoretic analogue of the double negation law of logic.

Theorem 3.19. *We have* $(A')' = A$.

Proof. $x \in (A')' \Leftrightarrow x \notin A' \Leftrightarrow \neg(x \in A') \Leftrightarrow \neg(\neg(x \in A)) \Leftrightarrow x \in A$.

By the Axiom of Extent, $(A')' = A$.

□

We prove now other properties of the complement.

Theorem 3.20. *We have*

1. $(A \cap B)' = A' \cup B'$.
2. $(A \cup B)' = A' \cap B'$.
3. $A \subseteq B \Leftrightarrow B' \subseteq A'$.
4. $A \cap A' = \emptyset$.
5. $\forall x\ (x \in A \cup A')$.

Proof. The first two parts of this theorem are often called the De Morgan's Laws for complements. They are much like the laws of logic in Theorem 1.2 which show what happens when you negate a conjunction or disjunction. In fact, if you know that the sentence $\neg(P \wedge Q) \Leftrightarrow (\neg P) \vee (\neg Q)$ is a tautology (i.e., it is always true), then a simple proof of part 1 is:

$x \in (A \cap B)'$
$\Leftrightarrow \neg(x \in A \cap B)$
$\Leftrightarrow \neg(x \in A \wedge x \in B)$
$\Leftrightarrow \neg(x \in A) \vee \neg(x \in B)$
$\Leftrightarrow x \in A' \vee x \in B'$
$\Leftrightarrow x \in A' \cup B'$.

Let's prove part 2 in a more standard fashion. Suppose $x \in (A \cup B)'$. Then x is not an element of the set $A \cup B$. There doesn't seem to be any direct way to continue, but we can always ask and try to answer questions as we go. Right here a good question would be: "is x a member of A"? The answer, naturally, is "no", because otherwise x would also be in $A \cup B$. In answering this question, we have discovered some useful information about x. Since the same process obviously leads to the conclusion that $x \notin B$, we can conclude that $x \in A' \wedge x \in B'$, so $x \in A' \cap B'$.

Now suppose that $x \in A' \cap B'$. Then x is not in A and also x is not in B. Could x be in the union of two sets if it is known that it is in neither? Of course not. Thus $x \notin (A \cup B)$, so by the definition of the complement, we get $x \in (A \cup B)'$.

We leave the other properties as exercise. □

Definition 8. The dual of a formula involving set variables, unions, and intersections, is the formula obtained by interchanging $\cup$ and $\cap$. The dual of an equation is the equation obtained by dualizing both sides.

For example: the dual of $A \cup B$ is $A \cap B$, the dual of $B \cap (A \cup B)$ is $B \cup (A \cap B)$, and the dual of A is A itself. Looking back at some of the theorems of the algebra of sets, it is hard not to be struck by the fact that many of them appear in dual pairs. This is not an accident. To see why, let's look at the equation

$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$. We have already proved this to be true for all sets A, B, and C by a simple element argument. But if it is true for all sets, then we can replace the letters in it by symbols denoting any set and still obtain a valid statement. In particular, the following is true:

$A' \cap (B' \cup C') = (A' \cap B') \cup (A' \cap C')$. By taking complements of both sides and using De Morgan's Laws, we obtain

$$(A' \cap (B' \cup C'))' = ((A' \cap B') \cup (A' \cap C'))',$$

and

$$(A')' \cup ((B')' \cap (C')') = ((A')' \cup (B')') \cap ((A')' \cup (C')').$$

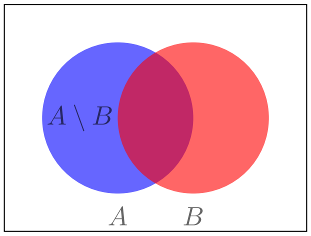
This clearly reduces to

$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C).$$

In other words, we have a mechanical method for proving the dual of the original statement. This always works for every union-intersection identity. This fact is summarized in the next

Metatheorem. (Principle of Duality) The dual of any identity involving only set variables and union or intersection symbols is also an identity.

Definition 9. Let X be a set and let $A, B \in \mathcal{P}(X)$. The difference of A and B, denoted by $A \setminus B$, is the set $\{x : x \in A \wedge x \notin B\}$.



Example 3.21.

$$\{1,2,4,5\} \setminus \{3,4,6\} = \{1,2,5\}, \quad \{3,4,6\} \setminus \{1,2,4,5\} = \{3,6\}.$$

Note that $A \setminus B$ may be different from $B \setminus A$. In particular we have $A' = X \setminus A$. Another notation for the set difference is $A - B$. We prefer $A \setminus B$ since, for A and B sets of numbers,

$$A - B = \{a - b : a \in A, b \in B\}$$

has a different meaning. For example,

$$\{1,2,3\} - \{1\} = \{0,1,2\}.$$

An object is in $A \setminus B$ if and only if it is in A and it is not in B. Looking at the other side of the coin, how will an element fail to be in $A \setminus B$? Clearly there are two ways: 1) if $x \notin A$, then x doesn't satisfy the first requirement, so x is not an element of $A \setminus B$; or 2) if $x \in B$, then x is not in the difference because the second part of the definition is wrong. Thus we have the equivalence $x \notin A \setminus B \Leftrightarrow [x \notin A \vee x \in B]$.

Theorem 3.22. *For arbitrary sets A, B, C we have*

1. $A \setminus B = A \cap B'$.
2. $(A \cup B) \setminus C = (A \setminus C) \cup (B \setminus C)$.
3. $A \setminus (B \setminus C) = (A \setminus B) \cup (A \cap C)$.
4. $A \setminus (B \cup C) = (A \setminus B) \setminus C$.

Proof. 1. by definition.

2. $(A \cup B) \setminus C = (A \cup B) \cap C' = A \cap C' \cup B \cap C' = (A \setminus C) \cup (B \setminus C)$.

3. $A \setminus (B \setminus C) = A \cap (B \cap C')' = A \cap (B' \cup C) = (A \cap B') \cup (A \cap C) = (A \setminus B) \cup (A \cap C)$.

4. $A \setminus (B \cup C) = A \cap (B \cup C)' = A \cap B' \cap C'$ and $(A \setminus B) \setminus C = (A \cap B') \cap C' = A \cap B' \cap C'$. □

Exercise 3.23. For sets A, B, C prove that $A \setminus (B \cap C) = (A \setminus B) \cup (A \setminus C)$.

Remark 3.24. Let A_1, A_2 be arbitrary sets. Then there are disjoint sets B_1, B_2 such that

$$A_1 \cup A_2 = B_1 \cup B_2.$$

(Recall that X, Y are disjoint if $X \cap Y = \emptyset$).

Proof. Take $B_1 = A_1, B_2 = A_2 \setminus A_1$. □

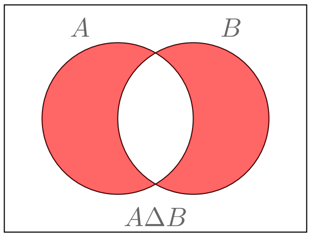
Exercise 3.25. Let $A_1, A_2, ..., A_n$ be arbitrary sets. Prove that there are disjoint sets $B_1, B_2, ..., B_n$ such that

$$\bigcup_{k=1}^{n} A_k = \bigcup_{k=1}^{n} B_k.$$

Definition 10. The symmetric difference of two sets A and B is defined as

$$A\Delta B = (A \setminus B) \cup (B \setminus A).$$

Another notation for the symmetric difference is $A \oplus B$.



Example 3.26. Let $A = \{a, b, c, d\}, B = \{c, d, e, f\}$. Then

$$A\Delta B = \{a, b, e, f\}.$$

Theorem 3.27. *The symmetric difference has the following properties:*

1. $A\Delta B = B\Delta A$ *(commutativity).*
2. $(A\Delta B)\Delta C = A\Delta(B\Delta C)$ *(associativity).*
3. $A\Delta\emptyset = \emptyset\Delta A = A$ *and* $A\Delta A = \emptyset$.
4. $A\Delta B = C \Leftrightarrow A\Delta C = B$.
5. $A \cap (B\Delta C) = (A \cap B)\Delta(A \cap C)$ *(distributivity).*

Proof. 1. $A\Delta B = (A \setminus B) \cup (B \setminus A) = (B \setminus A) \cup (A \setminus B) = B\Delta A$.

2. We have

$$(A\Delta B)\Delta C = [((A \cap B') \cup (B \cap A')) \cap C'] \cup [C \cap ((A \cap B') \cup (B \cap A'))'] =$$
$$(A \cap B' \cap C') \cup (B \cap A' \cap C') \cup [C \cap ((A \cap B')' \cap (B \cap A')')] =$$
$$(A \cap B' \cap C') \cup (B \cap A' \cap C') \cup [C \cap ((A' \cup B) \cap (B' \cup A))] =$$
$$(A \cap B' \cap C') \cup (B \cap A' \cap C') \cup [C \cap ((A' \cap B') \cup (B \cap B') \cup (A' \cap A) \cup (B \cap A))] =$$
$$(A \cap B' \cap C') \cup (B \cap A' \cap C') \cup (C \cap A' \cap B') \cup (C \cap B \cap A)$$

since $B \cap B' = A' \cap A = \emptyset$. Notice that the expression for $(A\Delta B)\Delta C$ is symmetric in A, B, C. Starting with the right hand side $A\Delta(B\Delta C)$, we get the same expression (convince yourself!).

3. It follows from the definition.

4. Assume $A\Delta B = C$. Taking the symmetric difference with A we get $A\Delta(A\Delta B) = A\Delta C$. Using associativity, $(A\Delta A)\Delta B = A\Delta C$. Since $A\Delta A = \emptyset$ and $\emptyset\Delta B = B$, we get $B = A\Delta C$. The converse is proved similarly (convince yourself!).

5. $A \cap (B\Delta C) = A \cap ((B \cap C') \cup (B' \cap C)) = (A \cap B \cap C') \cup (A \cap B' \cap C)$. On the other hand, $(A \cap B)\Delta(A \cap C) = ((A \cap B) \cap (A \cap C)') \cup ((A \cap B)' \cap (A \cap C)) = (A\cap B\cap A')\cup(A\cap B\cap C')\cup(A'\cap A\cap C)\cup(B'\cap A\cap C) = (A\cap B\cap C')\cup(B'\cap A\cap C)$. □

Other properties related to the symmetric difference are

Theorem 3.28. *We have*

a. $A\Delta B = (A \cup B) \setminus (A \cap B)$.

b. $A \cup B = (A\Delta B) \cup (A \cap B)$.

c. $A \setminus B = A\Delta(A \cap B)$.

Proof. Exercise. □

Exercise 3.29. (Ecuations with sets). Find sets X and Y satisfying all the conditions

a. $X \cup Y = \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$.

b. $X \cap Y = \{4, 6, 9\}$.

c. $X \cup \{3, 4, 5\} = \{1, 3, 4, 5, 6, 8, 9\}$.

d. $Y \cup \{2, 4, 8\} = \{2, 4, 5, 6, 7, 8, 9\}$.

Solution. We know that

$$\{4, 6, 9\} \subseteq X, Y \subseteq \{1, 2, 3, 4, 5, 6, 7, 8, 9\}.$$

From part c it follows that $1, 8 \in X$ and from d we get that $5, 7 \in Y$. Now $2, 3 \in X \cup Y$, so they belong to one of the sets, but not to both since $2, 3 \notin X \cap Y$. It follows that there are several soutions:

$$X_1 = \{1, 2, 3, 4, 6, 8, 9\}, Y_1 = \{4, 5, 6, 7, 9\},$$

$$X_2 = \{1, 2, 4, 6, 8, 9\}, Y_2 = \{3, 4, 5, 6, 7, 9\},$$

$$X_3 = \{1, 3, 4, 6, 8, 9\}, Y_3 = \{2, 4, 5, 6, 7, 9\},$$

$$X_4 = \{1, 4, 6, 8, 9\}, Y_4 = \{2, 3, 4, 5, 6, 7, 9\}.$$

Exercise 3.30. Find sets X and Y satisfying all the conditions

a. $X \cup Y = \{1, 2, 3, 4, 5, 6\}$.

b. $X \cap Y = \{1, 2, 3, 4\}$.

c. $\{4, 6\}$ is not a subset of X.

d. $\{5, 6\}$ is not a subset of $Y \setminus X$.

Exercise 3.31. Find all sets X and Y satisfying $X\Delta Y = \{1, 2, 3, 4\}$ and $X \cap Y = \{5, 6\}$. How many solutions do we have?

Exercise 3.32. Solve each of the equations for X:

a. $A \cup (B \setminus X) = B \cup X$ if $A = \{1,2,3\}, B = \{3,4,5\}$;

b. $\{1,2\}\Delta X = \{1,2,3\}$;

c. $(\{1,2\}\Delta X)\Delta\{1,2,3\} = \{1,2,3,4\}$

3.5. Ordered pairs and the Cartesian product

Definition 11. The ordered pair of x and y, denoted by $\langle x, y\rangle$, is the set $\{\{x\},\{x,y\}\}$.

Many books will use (x, y) for the ordered pair. We prefer $\langle x, y\rangle$ over (x, y) because of the conflict with the open interval notation (a, b) for $a, b \in \mathbb{R}$.

Theorem 3.33. $\langle y, z\rangle = \langle u, v\rangle \Leftrightarrow y = u$ *and* $z = v$.

Proof. Assuming $\langle y, z\rangle = \langle u, v\rangle$, we get $\{\{y\},\{y,z\}\} = \{\{u\},\{u,v\}\}$. It follows that either $\{y\} = \{u\}$ and $\{y,z\} = \{u,v\}$, or $\{y\} = \{u,v\}$ and $\{y,z\} = \{u\}$. In the first case it follows that $y = u$ and $z = v$. In the second case we get $u = v = y = z$. The converse is trivial. □

Definition 12. The Cartesian product of two sets X and Y is

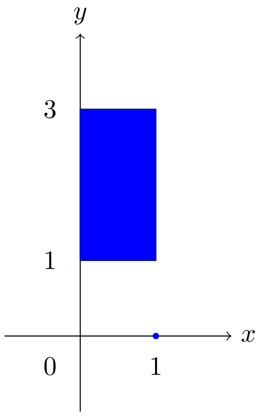
$$X \times Y = \{\langle x, y\rangle : x \in X, y \in Y\}$$

i.e., the set of all ordered pairs with first component taken from X and second component taken from Y.

Example 3.34. If $X = \{1,2,3\}$ and $Y = \{a,b\}$, then

$$X \times Y = \{\langle 1,a\rangle,\langle 2,a\rangle,\langle 3,a\rangle,\langle 1,b\rangle,\langle 2,b\rangle,\langle 3,b\rangle\}.$$

You probably already used $\mathbb{R}^2$ for $\mathbb{R}\times\mathbb{R}$ and $\mathbb{R}^3$ for $\mathbb{R}^2\times\mathbb{R}$ or Cartesian products of intervals like $[0,1]\times[1,3]$ in Calculus. You can visualize $[0,1]\times[1,3]$ as a rectangle in the plane $\mathbb{R}^2$:

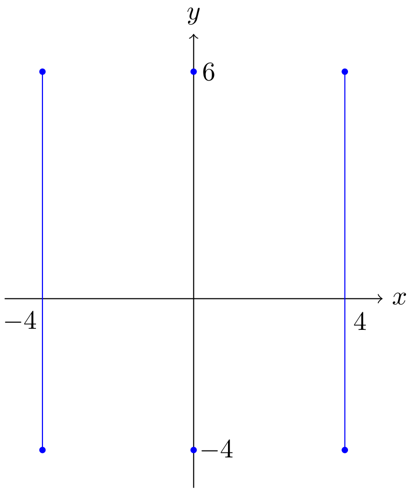


Exercise 3.35. Find $X\times Y$ if $X = \{x \in \mathbb{Z} : x^2 = 16\}$ and $Y = \{y \in \mathbb{R} : |y-1| \le 5\}$.

Solution. We have $X = \{-4, 4\}$ and $Y = [-4, 6]$. It follows that

$$X \times Y = \{\langle x, y\rangle : x = \pm 4,\ y \in [-4, 6]\}.$$

We can visualize this Cartesian product as a union of two segments in the plane:



Here are some properties of the Cartesian product in regards to other set operations:

Theorem 3.36. *We have*

1. $(A \cup B) \times C = (A \times C) \cup (B \times C)$.
2. $(A \cap B) \times C = (A \times C) \cap (B \times C)$.
3. $(A \setminus B) \times C = (A \times C) \setminus (B \times C)$.

Proof. 1. We have $\langle x, y\rangle \in (A \cup B) \times C$ equivalent to $x \in A \cup B$ and $y \in C$. This is the same as $x \in A$ and $y \in C$ or $x \in B$ and $y \in C$, in other words $\langle x, y\rangle \in A \times C$ or $\langle x, y\rangle \in B \times C$, which means $\langle x, y\rangle \in (A \times C) \cup (B \times C)$.

2. The proof is similar to the proof of 1.

3. We have $\langle x, y\rangle \in (A \setminus B) \times C \Leftrightarrow x \in A \setminus B \wedge y \in C \Leftrightarrow x \in (A \cap B') \wedge y \in C \Leftrightarrow x \in A \wedge x \notin B \wedge y \in C \Leftrightarrow \langle x, y\rangle \in A \times C \wedge \langle x, y\rangle \notin B \times C \Leftrightarrow \langle x, y\rangle \in (A \times C) \setminus (B \times C)$. □

Exercise 3.37. Are the following statements true?

1. $A \times (B \cup C) = (A \times B) \cup (A \times C)$.
2. $A \times (B \cap C) = (A \times B) \cap (A \times C)$.
3. $A \times (B \setminus C) = (A \times B) \setminus (A \times C)$.

Exercise 3.38. Prove the following

a. $(A \cup B) \times (C \cup D) = (A \times C) \cup (B \times C) \cup (A \times D) \cup (B \times D)$.

b. $(A \cap B) \times (C \cap D) = (A \times C) \cap (B \times C) \cap (A \times D) \cap (B \times D)$.

Definition 13. The disjoint union of two sets X, Y, denoted $X \sqcup Y$ is defined as $(X \times \{1\}) \cup (Y \times \{2\})$.

The idea is that if $X \cap Y \neq \emptyset$, the elements in the intersection need new labels to be distinguished. For example,

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

The sets X, Y can be identified with the subsets $X \times \{1\}, Y \times \{2\}$ of $X \sqcup Y$.

Chapter 4

Functions

The notion of function is central in many branches of Mathematics. You already met real functions of real variables in Calculus, like $f(x) = x^2, f(x) = \ln x$ or $f(x) = \tan x$. Here the domain and the set of values for these functions were subsets of $\mathbb{R}$, and a function was defined as a formula (or algorithm) which associates to each input a precise output. We will need to work with more general functions between all kinds of sets, not just subsets of the reals.

Even though a function is a particular case of a relation, we first study functions and define relations in the next chapter.

4.1. Definition and examples of functions

Definition 14. A *function* from a set X to a set Y is a subset f of the Cartesian product $X \times Y$ such that for all $x \in X$ there is a unique $y \in Y$ with $\langle x, y\rangle \in f$.

The set X is called the *domain* of f, denoted $\mathrm{dom}(f)$, and the set

$$\{y \in Y : \exists x \in X \text{ with } \langle x, y\rangle \in f\}$$

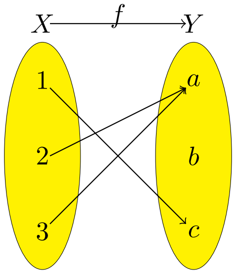
is called the *range* of f, denoted $\mathrm{ran}(f)$. The set Y is the set where f takes values, called also the *codomain* of f. Note that the range $\mathrm{ran}(f)$ may be a proper subset of the codomain Y. We write $f : X \to Y$, and for each $x \in X$ the unique element $y \in Y$ such that $\langle x, y\rangle \in f$ is denoted $f(x)$.

The set of ordered pairs $\langle x, f(x)\rangle$ is called the *graph* of f. Note that in the general definition of a function, we define f using its graph, which is a subset of $X \times Y$.

Two functions are equal if they have the same domain, the same codomain and the same graph.

Example 4.1. Let $X = \{1, 2, 3\}, Y = \{a, b, c\}$ and $f = \{\langle 1, c\rangle, \langle 2, a\rangle, \langle 3, a\rangle\}$. Then f is a function from X to Y such that $f(1) = c, f(2) = a, f(3) = a$ and $\mathrm{ran} f = \{a, c\}$.

We can visualize this function by a diagram:



Example 4.2. For X a set we define the *identity* function $id_X : X \to X, id_X(x) = x$. Its graph is the diagonal

$$\{\langle x, x\rangle : x \in X\}.$$

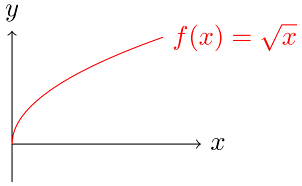
Remark 4.3. In Calculus a function was specified by a formula, like $f(x) = \sqrt{x}$, with the understanding that the domain is the largest set of real numbers for which $f(x)$ makes sense. In this case, $\operatorname{dom}(f) = [0, \infty)$, $\operatorname{ran}(f) = [0, \infty)$ and we can write

$$f : [0, \infty) \to \mathbb{R}, f(x) = \sqrt{x}$$

or

$$f : [0, \infty) \to Y, f(x) = \sqrt{x},$$

where Y is any set such that $[0, \infty) \subseteq Y \subseteq \mathbb{R}$. By changing Y we get different functions, since they have different codomains. The graph of $f : [0, \infty) \to \mathbb{R}, f(x) = \sqrt{x}$ is a subset of $[0, \infty) \times \mathbb{R}$:



Exercise 4.4. Explain what is wrong with the following "functions“:

a. Let $f : \mathbb{R} \to \mathbb{R}, f(x) = \dfrac{1}{x^2 - 1}$.

b. Let $g : [0, 5] \to [0, 2], g(x) = x - 1$.

c. Let $h : [-1, \infty) \to [3, 4), h(x) = \sqrt{x - 1}$.

Solution. a. Note that x can not be ±1, since these values vanish the denominator. The correct domain of f should be $\mathbb{R} \setminus \{\pm1\}$ or $(-\infty, -1) \cup (-1, 1) \cup (1, \infty)$.

b. When $x \in [0, 5], g(x) = x - 1 \in [-1, 4]$, so the correct codomain of g is $[-1, 4]$ or any set containing this interval.

c. The square root $\sqrt{x - 1}$ is defined only for $x \geq 1$ and it takes values in $[0, \infty)$. The correct domain of h is $[1, \infty)$ and the correct codomain is $[0, \infty)$ or any set containing this interval.

Exercise 4.5. The equation $f(x) = \dfrac{x^2+9}{x^2-9}$ is used to define a real function of real variable. Find the largest domain and the range of f.

Exercise 4.6. Given two functions f, g with real values, define $f+g, f-g, f\cdot g$ and f/g to be new functions such that

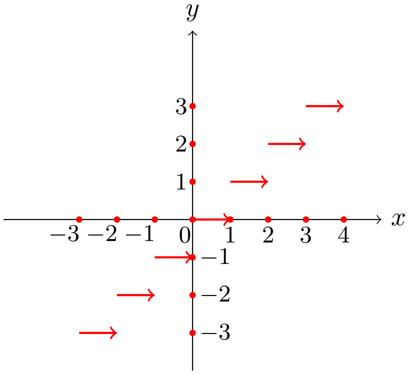
$$(f+g)(x) = f(x) + g(x),\ \ (f-g)(x) = f(x) - g(x),$$
$$(f\cdot g)(x) = f(x)\cdot g(x),\ \ (f/g)(x) = f(x)/g(x),$$

whenever this makes sense. Find $f+g, f-g, f\cdot g,\ f/g$ and their domains if

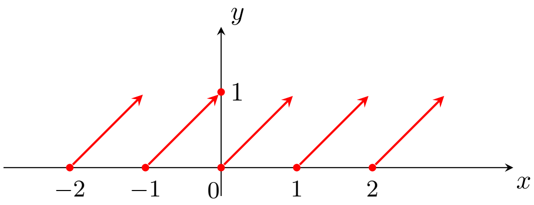
$$f,g:\mathbb{R}\to\mathbb{R}, f(x) = \begin{cases} x+2 & \text{if} \quad x\le 3 \\ -x+3 & \text{if} \quad x>3 \end{cases},\ \ g(x) = \begin{cases} x-2 & \text{if} \quad x\le 0 \\ x+1 & \text{if} \quad x>0 \end{cases}.$$

Exercise 4.7. Find all functions from $\{a,b,c\}$ to $\{1,2\}$ and specify their diagrams as in Example 4.1. Note that there are 8 such functions.

Definition 15. For any real number x, denote by $\lfloor x\rfloor$ the largest integer k such that $k\le x$. For example, $\lfloor 1.2\rfloor = 1, \lfloor -5.3\rfloor = -6$. Then $f:\mathbb{R}\to\mathbb{Z}, f(x) = \lfloor x\rfloor$ is a function, called the *integer part* function or the *floor* function, with the following graph. There is also a *ceiling* function, denoted $\lceil x\rceil$, the smallest integer larger or equal to x.



Definition 16. Let $f:\mathbb{R}\to[0,1), f(x) = x - \lfloor x\rfloor$. Then f is called the *fractional part* function. It has the following graph



Exercise 4.8. Prove that $x-1 < \lfloor x\rfloor \le x$. Use this inequality to show that for $x\ge 1$ we have

$$\frac{1}{2} < \frac{\lfloor x\rfloor}{x} \le 1.$$

Exercise 4.9. Graph the ceiling function $f : \mathbb{R} \to \mathbb{Z}, f(x) = \lceil x \rceil$.

Example 4.10. (Characteristic function) For X a set and $A \subseteq X$, denote by χ_A the function

$$\chi_A : X \to \{0, 1\}, \;\; \chi_A(x) = \begin{cases} 1 & \text{if } x \in A \\ 0 & \text{if } x \notin A. \end{cases}$$

This is called the *characteristic* (or indicator) function of A.

The characteristic function has the following properties

Theorem 4.11. *Consider a set X and $A, B \in \mathcal{P}(X)$. Then*

a. $A = B$ *iff* $\chi_A = \chi_B$.

b. $\chi_{A\cap B} = \chi_A \cdot \chi_B$.

c. $\chi_{A\cup B} = \chi_A + \chi_B - \chi_A \cdot \chi_B$.

d. $\chi_{A'} = 1 - \chi_A$.

e. $\chi_{A\setminus B} = \chi_A - \chi_A \cdot \chi_B$.

f. $\chi_{A\Delta B} = \chi_A + \chi_B - 2\chi_A \cdot \chi_B$.

Proof. a. If $A = B$, then it is clear that $\chi_A, \chi_B : X \to \{0, 1\}$ have the same values, so $\chi_A = \chi_B$. Conversely, assume $\chi_A = \chi_B$ and suppose $x \in A$. This happens if and only if $\chi_A(x) = 1 = \chi_B(x)$ i.e. $x \in B$. By double inclusion we get $A = B$.

b. We can directly check that $\chi_A(x)\chi_B(x) = 1$ precisely when $\chi_A(x) = \chi_B(x) = 1$ i.e. when $x \in A \cap B$, and otherwise $\chi_A(x)\chi_B(x) = 0$.

c. We have $\chi_{A\cup B}(x) = 1$ when $x \in A$ or $x \in B$, and otherwise $\chi_{A\cup B}(x) = 0$. Now $\chi_A(x) + \chi_B(x) = 2$ precisely when $x \in A \cap B$. It follows that in any case $\chi_{A\cup B} = \chi_A + \chi_B - \chi_A \cdot \chi_B$.

d. We have $x \in A'$ precisely when $x \notin A$, so $\chi_{A'}(x) = 1$ when $\chi_A(x) = 0$ and $\chi_{A'}(x) = 0$ when $\chi_A(x) = 1$. It follows that $\chi_{A'} = 1 - \chi_A$.

e. We have $A \setminus B = A \cap B'$ and we can apply properties b and d.

f. We have $A\Delta B = (A \cup B) \setminus (A \cap B)$, so

$$\chi_{A\Delta B} = \chi_{A\cup B} - \chi_{A\cup B}\chi_{A\cap B} = \chi_A + \chi_B - \chi_A\chi_B - (\chi_A + \chi_B - \chi_A\chi_B)\chi_A\chi_B =$$

$$\chi_A + \chi_B - \chi_A\chi_B - \chi_A^2\chi_B + \chi_A\chi_B^2 - \chi_A^2\chi_B^2 = \chi_A + \chi_B - 2\chi_A \cdot \chi_B$$

since $\chi_A^2 = \chi_A, \chi_B^2 = \chi_B$. □

Exercise 4.12. Use the above properties of the characteristic function to prove that $A\Delta(B\Delta C) = (A\Delta B)\Delta C$ for arbitrary sets $A, B, C \in \mathcal{P}(X)$.

Definition 17. For $x, y \in \mathbb{R}$ define the maximum and the minimum functions by

$$\max(x, y) = \begin{cases} x & \text{if} \;\; x \geq y \\ y & \text{if} \;\; x < y \end{cases}$$

and

$$\min(x, y) = \begin{cases} x & \text{if} \;\; x \leq y \\ y & \text{if} \;\; x > y, \end{cases}$$

respectively. Here the domain of both functions is $\mathbb{R} \times \mathbb{R}$ and the range is $\mathbb{R}$.

Remark 4.13. Sometimes we use the notation $\max\{x,y\}$ and $\min\{x,y\}$ for the same functions. This notation is particularly useful when we will take the maximum and minimum of more than two numbers.

Exercise 4.14. Prove that

$$\max(x,y) = \frac{x+y+|x-y|}{2}, \quad \min(x,y) = \frac{x+y-|x-y|}{2},$$

where $|x| = \begin{cases} x & \text{if} \quad x \geq 0 \\ -x & \text{if} \quad x < 0. \end{cases}$

Example 4.15. The *sign* function is $sgn : \mathbb{R} \to \{-1,0,1\}$ such that

$$sgn(x) = \begin{cases} -1 & \text{if} \quad x < 0 \\ 0 & \text{if} \quad x = 0 \\ 1 & \text{if} \quad x > 0. \end{cases}$$

Exercise 4.16. Graph the sign function.

Sometimes a function $f : X \to Y$ can be defined using a certain property satisfied by ordered pairs $\langle x,y\rangle$. More precisely, we have

Theorem 4.17. *Suppose X,Y are sets and suppose $P(x,y)$ is an open sentence depending on $\langle x,y\rangle \in X \times Y$ such that $\forall x \in X\ \exists! y \in Y$ such that $P(x,y)$. Then $\{\langle x,y\rangle : x \in X \wedge P(x,y)\}$ is a function with domain X and codomain Y.*

Proof. Since for all $x \in X$ there is a unique $y \in Y$ satisfying $P(x,y)$, by taking $f(x) = y$ we get a function $f : X \to Y$. □

Example 4.18. Consider $P(x,y)$ to be $2x + y = 1$ for $x,y \in \mathbb{Z}$. Then, since we can solve for y and there is a unique solution $y = 1-2x$, we can define the function $f : \mathbb{Z} \to \mathbb{Z}, f(x) = 1-2x$.

Exercise 4.19. Let $X = \{1,3,5,6\}$, and let $Y = \{0,1,2,3,5\}$. Which of the following open sentences with $x \in X, y \in Y$ define a function from X to Y? How about a function from Y to X?

a. $x + y = 6$;

b. $y - x = 1$;

c. $y = x^2$;

d. $x = y$.

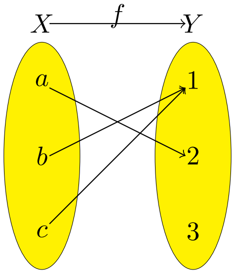
4.2. Direct image, inverse image

Definition 18. (Direct image function) Given $f : X \to Y$, we define a new function $f_{\mathcal{P}} : \mathcal{P}(X) \to \mathcal{P}(Y)$ such that

$$f_{\mathcal{P}}(A) = \{f(a) : a \in A\}.$$

Many times we drop the subscript $\mathcal{P}$ and denote the new function also by f, even though this is now a function of sets. The set $f(A)$ is called the direct image of A. In particular note that $f(X)$ =ran(f). It should be clear from the context if we talk about $f : X \to Y$ or about $f : \mathcal{P}(X) \to \mathcal{P}(Y)$.

Example 4.20. If $X = \{a, b, c\}$, $Y = \{1, 2, 3\}$ and $f(a) = 2, f(b) = f(c) = 1$, then $f(\emptyset) = \emptyset, f(\{a\}) = \{2\}, f(\{b\}) = f(\{c\}) = \{1\}, f(\{a, b\}) = f(\{a, c\}) = \{1, 2\}, f(\{b, c\}) = \{1\}, f(X) = \{1, 2\}$.



Definition 19. (Inverse image function) Given $f : X \to Y$, we define $f_{\mathcal{P}}^{-1} : \mathcal{P}(Y) \to \mathcal{P}(X)$ such that

$$f_{\mathcal{P}}^{-1}(B) = \{x \in X : f(x) \in B\}.$$

Again, this new function is often denoted by f^{-1}, not to be confused with the inverse function of a bijection (which will be defined later). The set $f^{-1}(B)$ is called the inverse image of B. In particular $f^{-1}(\{y\})$ is in general a subset of X.

Example 4.21. If $X = \{a, b, c\}$, $Y = \{1, 2, 3\}$ and $f(a) = 2, f(b) = f(c) = 1$, then $f^{-1}(\{1\}) = f^{-1}(\{1, 3\}) = \{b, c\}$, $f^{-1}(\{2\}) = f^{-1}(\{2, 3\}) = \{a\}$, $f^{-1}(\{3\}) = f^{-1}(\emptyset) = \emptyset$, $f^{-1}(\{1, 2\}) = f^{-1}(Y) = \{a, b, c\}$.

Theorem 4.22. *Let $f : X \to Y$ be a function, let $A, B \in \mathcal{P}(X)$, and let $C, D \in \mathcal{P}(Y)$. Then*

a. $f(A \cup B) = f(A) \cup f(B)$.

b. $f(A \cap B) \subseteq f(A) \cap f(B)$.

c. $f^{-1}(C') = (f^{-1}(C))'$.

d. $f^{-1}(C \cup D) = f^{-1}(C) \cup f^{-1}(D)$.

e. $f^{-1}(C \cap D) = f^{-1}(C) \cap f^{-1}(D)$.

Proof. a. Let $y \in f(A \cup B)$. Then there is $x \in A \cup B$ such that $f(x) = y$. If $x \in A$, then $f(x) \in f(A)$ and if $x \in B$ then $f(x) \in f(B)$. In any case $y = f(x) \in f(A) \cup f(B)$. We proved that $f(A \cup B) \subseteq f(A) \cup f(B)$.

Let $y \in f(A) \cup f(B)$. Then $y \in f(A)$ or $y \in f(B)$. There is $x \in A$ such that $f(x) = y$ or there is $x \in B$ such that $f(x) = y$. We found $x \in A \cup B$ such that $f(x) = y$, hence $y \in f(A \cup B)$. By double inclusion we get $f(A \cup B) = f(A) \cup f(B)$.

b. Let $y \in f(A \cap B)$. Then there is $x \in A \cap B$ with $f(x) = y$. It follows that $f(x) = y \in f(A) \cap f(B)$. Note that the inclusion may be strict. For $X = Y = \mathbb{R}$, $A = \{-1\}, B = \{1\}$ and $f(x) = x^2$ we have $f(A \cap B) = f(\emptyset) = \emptyset$ but $f(A) \cap f(B) = \{1\}$.

c. Let $x \in f^{-1}(C')$. Then $f(x) = y \in C'$, so for any $z \in C$ we have $f(x) \neq z$. This means that $x \notin f^{-1}(C)$ or $x \in (f^{-1}(C))'$.

Let $x \in (f^{-1}(C))'$. Since $x \notin f^{-1}(C)$, it follows that $f(x) \notin C$ or $f(x) \in C'$ and therefore $x \in f^{-1}(C')$. By double inclusion we get equality.

d. Let $x \in f^{-1}(C \cup D)$. Then $f(x) \in C \cup D$, so $f(x) \in C$ or $f(x) \in D$ which means that $x \in f^{-1}(C) \cup f^{-1}(D)$. For the other inclusion, let $x \in f^{-1}(C) \cup f^{-1}(D)$. It follows that $f(x) \in C$ or $f(x) \in D$, therefore $f(x) \in C \cup D$ or $x \in f^{-1}(C \cup D)$.

e. Exercise. □

Example 4.23. Let

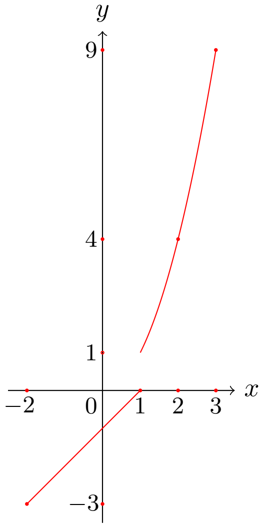
$$f : \mathbb{R} \to \mathbb{R}, f(x) = \left\{ \begin{array}{lll} x-1 & \text{if} & x \leq 1 \\ x^2 & \text{if} & x > 1 \end{array} \right.$$

Let's find $f([-2,3])$. We have $[-2,3] = [-2,1] \cup (1,3]$ and $f([-2,1]) = [-3,0]$, $f((1,3]) = (1,9]$, hence $f([-2,3]) = [-3,0] \cup (1,9]$.

Example 4.24. For

$$f : \mathbb{R} \to \mathbb{R}, f(x) = \left\{ \begin{array}{lll} x-1 & \text{if} & x \leq 1 \\ x^2 & \text{if} & x > 1 \end{array} \right.$$

let us find $f^{-1}([-3,4])$. We have $[-3,4] = [-3,0] \cup (0,4]$, $f^{-1}([-3,0]) = [-2,1]$ and $f^{-1}((0,4]) = (1,2]$, hence $f^{-1}([-3,4]) = [-2,2]$. A look at the following graph is helpful.



Exercise 4.25. Let $A = \{1,2,3,4\}$ and let $B = \{a,b,c,d,e\}$. For

$$f : A \to B, f = \{\langle 1,e\rangle, \langle 2,c\rangle, \langle 3,a\rangle, \langle 4,e\rangle\},$$

determine the sets

a. $f(\{1,3\})$

b. $f^{-1}(\{a,b,c\})$

c. $f^{-1}(f(\{2,4\}))$

d. $f(f^{-1}(\{b, d, e\}))$.

Exercise 4.26. Let $f : \mathbb{R} \to \mathbb{R}, f(x) = |x - 2| + 3$. Calculate

a. $f((-2, 5])$

b. $f((-2, -1) \cup (3, 6))$

c. $f^{-1}([0, 2))$

d. $f^{-1}([4, 7))$

e. $f^{-1}(f((-1, 3)))$

f. $f(f^{-1}([-1, 5]))$.

4.3. Restriction and extension of a function

Suppose $f : X \to Y$ and $g : Z \to W$ are two functions. Recall that they are equal and we write $f = g$ if and only if $X = Z$, $Y = W$ and $\forall x \in X$ we have $f(x) = g(x)$. In particular, if we change the codomain of a function, we obtain a new function.

Example 4.27. $f : [0, \infty) \to \mathbb{R}, f(x) = \sqrt{x}$ and $g : [0, \infty) \to [0, \infty), g(x) = \sqrt{x}$ are two different functions, even though they have the same domain and the same formula.

Example 4.28. Let $f : \{-1, 1, 2\} \to \mathbb{R}, f(x) = x^2 - 1, g : \{-1, 1, 2\} \to \mathbb{R}, g(x) = x^3 - x^2 - x + 1$. Then $f(-1) = g(-1) = 0, f(1) = g(1) = 0, f(2) = g(2) = 3$, hence $f = g$, even though their formulas are different. Notice that the domain has only three points. If the domain was $\mathbb{R}$, then they would be different functions.

Definition 20. Let $f : X \to Y$ be a function. A *restriction* of f is a function $g : A \to Y$ such that $A \subseteq X$ and $g(a) = f(a)$ for all $a \in A$. This function g is also denoted by $f|_A$. An *extension* of f is a function $h : Z \to Y$ such that $X \subseteq Z$ and $h(x) = f(x)$ for all $x \in X$. Sometimes an extension of f is denoted $\tilde{f}$. If g is a restriction of f, then f is an extension of g.

Example 4.29. Let $f : \mathbb{R} \to [-1, 1], f(x) = \sin x$. Then $g : [-\pi/2, \pi/2] \to [-1, 1]$ is a restriction of f. The function $h : [-\pi, \pi] \to [-1, 1], h(x) = \sin x$ is an extension of g.

Example 4.30. Consider $f : \mathbb{R} \setminus \{0\} \to \mathbb{R}, f(x) = \dfrac{\sin x}{x}$. We know from Calculus that $\lim\limits_{x \to 0} \dfrac{\sin x}{x} = 1$. We can define an extension of f by

$$\tilde{f} : \mathbb{R} \to \mathbb{R}, \tilde{f} = \begin{cases} \frac{\sin x}{x} & \text{for } x \neq 0 \\ 1 & \text{for } x = 0. \end{cases}$$

Exercise 4.31. Let $f : \{1, 2\} \to \mathbb{R}, f(1) = 2, f(2) = 4$. Find an extension $g : \mathbb{R} \to \mathbb{R}$ of f of the form $g(x) = ax + b$.

Exercise 4.32. Let $f : \{1, 3, 5\} \to \mathbb{R}$ such that $f(1) = 0, f(3) = 2, f(5) = 12$. Find an extension $g : \mathbb{R} \to \mathbb{R}$ of f of the form $g(x) = ax^2 + bx + c$.

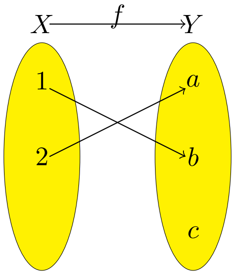
We may also shrink or enlarge the codomain of a function. The new functions are sometimes called *corestriction* and *coextension*, respectively. Some people use the name restriction or extension for the new function obtained by shrinking or enlarging either the domain or codomain (or both).

Example 4.33. Let $f : [0,\infty) \to \mathbb{R}, f(x) = \sqrt{x}$. Then $g : [0,\infty) \to [0,\infty), g(x) = \sqrt{x}$ is a corestriction of f.

4.4. One to one and onto functions. Composition and inverse functions

Definition 21. A function $f : X \to Y$ is *one-to-one* or *injective* if and only if for all $x, x' \in X$, $x \neq x' \Rightarrow f(x) \neq f(x')$.

Example 4.34. The function $f : \{1,2\} \to \{a,b,c\}, f(1) = b, f(2) = a$ is one-to-one.



Note that no two arrows arrive at the same spot.

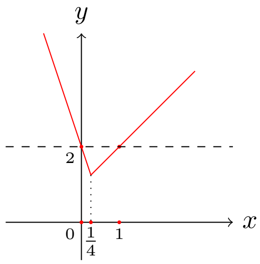
The function $g : \mathbb{R} \to \mathbb{R}, g(x) = x^2$ is not; in fact it is two-to-one because $g(-x) = g(x)$, except at zero. The restriction $g_1 : [0,\infty) \to \mathbb{R}, g_1(x) = x^2$ is one-to-one. Another one-to-one restriction is $g_2 : (-\infty, 0] \to \mathbb{R}, g_2(x) = x^2$.

Remark 4.35. A function f is one-to-one if and only if for all $x, x' \in X$, $f(x) = f(x') \Rightarrow x = x'$. Indeed, this is the contrapositive of the statement $x \neq x' \Rightarrow f(x) \neq f(x')$.

Example 4.36. Let's check if the function $f : \mathbb{R} \to \mathbb{R}, f(x) = \max(x+1, 2-3x)$ is one-to-one by looking at its graph. Since $x + 1 \geq 2 - 3x$ for $x \geq 1/4$ and $2 - 3x > x + 1$ for $x < 1/4$, we get

$$f(x) = \begin{cases} x+1 & \text{if} \quad x \geq 1/4 \\ 2-3x & \text{if} \quad x < 1/4, \end{cases}$$

which has the graph



Notice that a horizontal line may cut the graph in two different points, so f is not one-to-one. Indeed, there are $x_1 \neq x_2$ such that $f(x_1) = f(x_2)$, for example $x_1 = 0, x_2 = 1$.

Exercise 4.37. Which of the following functions are injective?

a. $g(x) = \min(-x, x), x \in \mathbb{R}$.

b. $h(x) = \max(x + 1, 2x - 1), x \in \mathbb{R}$.

c. $k(x) = \min(-2x, -x + 1), x \in \mathbb{R}$.

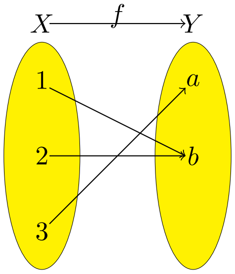
Exercise 4.38. Let $A \subset \mathbb{R}$ and let $f : A \to \mathbb{R}$ defined below. Determine two different sets A so that $f\,|_A$ is one-to-one. Choose them as large as possible.

a. $f(x) = \dfrac{2}{(x-3)^2}$

b. $f(x) = \cot x$.

Definition 22. A function $f : X \to Y$ is *onto* or *surjective* if for all $y \in Y$ there is $x \in X$ with $f(x) = y$. This is equivalent to $\text{ran}f = Y$ or $f(X) = Y$.

Example 4.39. Let $f : X = \{1, 2, 3\}, Y = \{a, b\}, f(1) = f(2) = b, f(3) = a$ with diagram



Note that at each point in the codomain arrives at least one arrow.

The function $g : \mathbb{R} \to \mathbb{R}, g(x) = x^2$ is not onto since it does not take negative values.

Remark 4.40. Given any function $f : X \to Y$, by shrinking the codomain to $\text{ran}(f)$, we can construct a surjective function $g : X \to \text{ran}(f)$ such that $g(x) = f(x)$ for all $x \in X$. We distinguish between the functions f and g if f is not onto.

Definition 23. Suppose f and g are functions. We define a new function $f \circ g$ called the *composition* of f and g with domain $\{x \in \text{dom}(g) : g(x) \in \text{dom}(f)\}$ such that $(f \circ g)(x) = f(g(x))$.

Example 4.41. Let $f : [0, 4] \to [0, 2], f(x) = \sqrt{x}$ and let $g : \mathbb{R} \to [-1, \infty), g(x) = x^2 - 1$. Then

$$f \circ g : [-\sqrt{5}, -1] \cup [1, \sqrt{5}] \to [0, 2], (f \circ g)(x) = \sqrt{x^2 - 1}$$

and

$$g \circ f : [0, 4] \to [-1, 3], (g \circ f)(x) = x - 1.$$

Remark 4.42. Sometimes the domain of $f \circ g$ may be the empty set, in which case $f \circ g$ is the empty function (not so interesting). To avoid this situation, many times we assume ran(g)=dom(f). Also, if $f : X \to X$ and $g : X \to X$, then both functions $f \circ g$ and $g \circ f$ may be defined. In general, $f \circ g \neq g \circ f$.

Example 4.43. Let

$$f : \mathbb{R} \to \mathbb{R}, f(x) = \begin{cases} x - 1 & \text{if} \quad x \leq 1 \\ x^2 & \text{if} \quad x > 1 \end{cases}, \quad g : \mathbb{R} \to \mathbb{R}, g(x) = \begin{cases} x/2 & \text{if} \quad x \geq 2 \\ x^3 & \text{if} \quad x < 2 \end{cases}.$$

Let us find $f \circ g$ and $g \circ f$. We have

$$(f \circ g)(x) = \begin{cases} g(x) - 1 & \text{if} \quad g(x) \leq 1 \\ (g(x))^2 & \text{if} \quad g(x) > 1 \end{cases}.$$

Notice that $g(x) \leq 1$ for $x \leq 1$ and for $x = 2$; otherwise $g(x) > 1$. It follows that

$$(f \circ g)(x) = \begin{cases} x^3 - 1 & \text{if} \quad x \leq 1 \\ x^6 & \text{if} \quad 1 < x < 2 \\ 0 & \text{if} \quad x = 2 \\ \dfrac{x^2}{4} & \text{if} \quad x > 2 \end{cases}.$$

On the other hand,

$$(g \circ f)(x) = \begin{cases} \dfrac{f(x)}{2} & \text{if} \quad f(x) \geq 2 \\ (f(x))^3 & \text{if} \quad f(x) < 2 \end{cases}.$$

We have $f(x) \geq 2$ for $x \geq \sqrt{2}$ and $f(x) < 2$ for $x < \sqrt{2}$, hence

$$(g \circ f)(x) = \begin{cases} \dfrac{x^2}{2} & \text{if} \quad x \geq \sqrt{2} \\ x^6 & \text{if} \quad 1 < x < \sqrt{2} \\ (x-1)^3 & \text{if} \quad x \leq 1 \end{cases}.$$

Theorem 4.44. *Let $f : Y \to Z$ and $g : X \to Y$. If f and g are one-to-one functions, then so is $f \circ g : X \to Z$. If f and g are onto, then $f \circ g : X \to Z$ is also onto.*

Proof. Assume $(f \circ g)(x) = (f \circ g)(x')$, so $f(g(x)) = f(g(x'))$ for $x, x' \in X$. Since f is one-to-one, we get $g(x) = g(x')$. Since g is one-to-one, we get $x = x'$, hence $f \circ g$ is one-to-one.

Assume now that $z \in Z$. Since f is onto, we can find $y \in Y$ with $f(y) = z$. Since g is onto, there is $x \in X$ with $g(x) = y$. We conclude that $(f \circ g)(x) = z$, hence $f \circ g$ is onto. □

Exercise 4.45. Prove by counterexample that the converse of each statement of the above theorem is false.

Exercise 4.46. Given three functions f, g, h, prove that $f \circ (g \circ h) = (f \circ g) \circ h$.

Definition 24. A function $f : X \to Y$ is called *bijective* if it is one-to-one and onto.

Exercise 4.47. Prove that the function $f : \mathbb{R} \to \mathbb{R}, f(x) = x^3$ is bijective.

Definition 25. We say that a function $f : X \to Y$ is *invertible* (or has an inverse) if there is $g : Y \to X$ such that $g \circ f = id_X$ and $f \circ g = id_Y$. The inverse of f is unique, is denoted f^{-1} and satisfies

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

Remark 4.48. Recall that we already used the notation $f^{-1} = f_{\mathcal{P}}^{-1} : \mathcal{P}(Y) \to \mathcal{P}(X)$ for any function $f : X \to Y$ and we called it the inverse image function. In the case f is a bijection, we have $f^{-1}(\{y\}) = f^{-1}(y)$. You must be careful to distinguish from the context between the two meanings of f^{-1}.

Theorem 4.49. *A function $f : X \to Y$ is invertible if and only if it is bijective.*

Proof. If $f : X \to Y$ is invertible, let $g : Y \to X$ its inverse. To prove that f is one-to-one, assume $f(x_1) = f(x_2)$. Applying g both sides, we get $(g \circ f)(x_1) = (g \circ f)(x_2)$, hence $x_1 = x_2$ since $g \circ f = id_X$. To prove that f is onto, let $y \in Y$. Then $f(g(y)) = y$, so we found $x = g(y) \in X$ such that $f(x) = y$.

Conversely, given $f : X \to Y$ bijective, define $g : Y \to X$ such that $g(y) = x \Leftrightarrow f(x) = y$. Then it is easy to verify that $g \circ f = id_X$ and $f \circ g = id_Y$, so g is the inverse of f. □

Example 4.50. Let $f : (2, \infty) \to (-1, \infty), f(x) = \dfrac{3 - x}{x - 2}$. Then f is one-to-one since $f(x_1) = f(x_2)$,

$$\frac{3 - x_1}{x_1 - 2} = \frac{3 - x_2}{x_2 - 2}$$

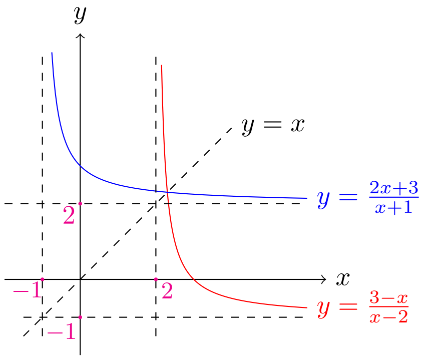
implies

$$3x_2 - x_1x_2 - 6 + 2x_1 = 3x_1 - 6 - x_1x_2 + 2x_2,$$

hence $x_1 = x_2$. It is onto since given $y \in (-1, \infty)$, the equation $y = \dfrac{3 - x}{x - 2}$ has solution $x = \dfrac{2y + 3}{y + 1}$ which belongs to $(2, \infty)$. Indeed, when $y \to -1$ we have $x \to \infty$ and when $y \to \infty$, $x \to 2$. The last computation gives the formula for the inverse

$$f^{-1} : (-1, \infty) \to (2, \infty), f^{-1}(y) = \frac{2y + 3}{y + 1}.$$

If we graph f and f^{-1} in the same system of coordinates, we notice that their graphs are symmetric with respect to the first quadrant bisector $y = x$.



Exercise 4.51. Let $f : [1/e, e] \to [-\sin 1, \sin 1], f(x) = \sin(\ln x)$. Prove that f is a bijection and find the formula for f^{-1}.

Remark 4.52. 1. If f, g are bijections, then $(f \circ g)^{-1} = g^{-1} \circ f^{-1}$.

2. For an invertible function $f : X \to Y$, we have $f^{-1}(\{y\}) = \{x\}$, where $f(x) = y$.

3. Recall that a function $f : X \to Y$ was defined as a set of ordered pairs $\langle x, f(x)\rangle$ in the Cartesian product $X \times Y$. If f is invertible, then f^{-1} is the set of ordered pairs $\langle f(x), x\rangle$ in the Cartesian product $Y \times X$.

Definition 26. Given $f : X \to Y$, a *retract* of f is a function $r : Y \to X$ such that $r \circ f = id_X$ (a left inverse). A *section* of f is a function $s : Y \to X$ such that $f \circ s = id_Y$ (a right inverse).

Example 4.53. Let $f : \{1, 2\} \to \{a, b, c\}, f(1) = b, f(2) = c$. Then $r : \{a, b, c\} \to \{1, 2\}, r(a) = 1, r(b) = 1, r(c) = 2$ is a retract for f. Notice that $r(a)$ can be any element of $\{1, 2\}$.

Let $g : \{1, 2, 3\} \to \{a, b\}, g(1) = g(2) = b, g(3) = a$ and $s : \{a, b\} \to \{1, 2, 3\}, s(a) = 3, s(b) = 2$. Then s is a section for g. Notice that to define $s(b)$, we may choose any element from the set $g^{-1}(\{b\})$.

Remark 4.54. Any injective function has a retract. Conversely, if f has a retract, then f is injective.

Proof. Given $f : X \to Y$ injective, define $r : Y \to X$ as follows. For $y \in f(X)$, say $y = f(x)$ define $r(y) = x$. This is well defined since there is a unique x such that $f(x) = y$. For $y \in Y \setminus f(X)$, define $r(y) = x_0$ for a fixed arbitrary element of X. Then we have $r \circ f = id_X$ since $r(f(x)) = x$ for all $x \in X$. Conversely, assume f has a retract $r : Y \to X$ and let's prove that f is one-to-one. Suppose $f(x) = f(x')$. By applying r we get $r(f(x)) = r(f(x'))$ or $x = x'$, hence f is one-to-one. □

Exercise 4.55. Which of the following subsets of $\{a, b, c, d\} \times \{a, b, c, d\}$ are functions? For those that fail, give a reason why.

a. $f = \{\langle a, b\rangle, \langle c, d\rangle\}$;

b. $g = \{\langle a, a\rangle, \langle b, c\rangle, \langle c, a\rangle, \langle d, b\rangle\}$;

c. $h = \{\langle a, b\rangle, \langle b, c\rangle, \langle c, d\rangle, \langle d, a\rangle, \langle a, c\rangle\}$;

d. $k = \{\langle a, b\rangle, \langle b, c\rangle, \langle c, d\rangle, \langle d, d\rangle\}$;

e. $\ell = \{\langle a, b\rangle, \langle b, c\rangle, \langle c, d\rangle, \langle d, a\rangle\}$.

Exercise 4.56. Which of the functions from $\{a, b, c, d\}$ to $\{a, b, c, d\}$ that you found above are onto? Which are one-to-one?

Exercise 4.57. If $f : X \to X$ is injective, prove by induction that the composition $f^n = f \circ f \circ \cdots \circ f$ is injective for all $n \geq 1$. Same for surjective.

Exercise 4.58. Let $f : \mathbb{R} \to \mathbb{R}$ be a function such that $f(2x + 1) = x^2 + x - 2$ for all x. Find $f(x)$.

Exercise 4.59. Prove that $g = \{\langle x, y\rangle \in \mathbb{R} \times \mathbb{R} : x^2 = y^2\}$ is not a function.

Exercise 4.60. Let $f : X \to Y$ be a function, let $A, B \in \mathcal{P}(X)$, and let $C, D \in \mathcal{P}(Y)$. Prove that

a. $f(A \cap B) = f(A) \cap f(B)$ for f one-to-one.

b. $f(A') \subseteq (f(A))'$ for f one-to-one.

c. $f(A') \supseteq (f(A))'$ for f onto.

In parts b and c find f and A such that the inclusions are strict.

Exercise 4.61. Show that if $g \circ f$ is injective, then f is injective. Show that if $f \circ g$ is surjective, then f is surjective. Prove that the converse statements are false.

Exercise 4.62. Find two injective restrictions of $f : \mathbb{R} \to \mathbb{R}, f(x) = x^2 - 3x + 1$.

Exercise 4.63. Determine which of the following functions is bijective and find its inverse:

a. $f : \mathbb{R} \to \mathbb{R}, f(x) = 7x + 1$;

b. $g : (-\infty, 0] \to [0, \infty), g(x) = x^2$;

c. $h : [2, \infty) \to (-\infty, 0], h(x) = -x^2 + 4x - 4$;

d. $k : [-3, 1] \to [-6, 3], k(x) = \max(2x, 3x)$.

Exercise 4.64. Show that $f : \mathbb{R} \to \mathbb{R}, f(x) = x^2 - 6x + 2$ has invertible restrictions defined on

a. $(-\infty, 3]$;

b. $[3, \infty)$;

c. $(-\infty, 0] \cup [3, 6)$.

Find these inverses and graph them.

Exercise 4.65. Let

$$f : \mathbb{R} \to [0, \infty), f(x) = x^2, \;\; g : \mathbb{R} \to [-1, 1], g(x) = \frac{2x}{1 + x^2}, \;\; h : [1, \infty) \to [0, \infty), h(x) = \sqrt{x - 1}.$$

Compute $f \circ g \circ h$ and specify its domain and range.

Exercise 4.66. Let

$$f : \mathbb{R} \to \mathbb{R}, f(x) = \begin{cases} x & \text{if} \quad x \leq 0 \\ x + 1 & \text{if} \quad x > 0 \end{cases}, \;\; g : \mathbb{R} \to [0, \infty), g(x) = \begin{cases} x^2 & \text{if} \quad x < 0 \\ x & \text{if} \quad x \geq 0 \end{cases}.$$

Find $f \circ g$ and $g \circ f$.

Exercise 4.67. Two functions $f, g : \mathbb{R} \to \mathbb{R}$ are such that for all $x \in \mathbb{R}$,

$$g(x) = x^2 + x + 3, \;\; (g \circ f)(x) = x^2 - 3x + 5.$$

Find all possibilities for f.

4.5. *Family of sets and the axiom of choice

Definition 27. Consider I, X arbitrary sets. A *family* of subsets of X is a function $f : I \to \mathcal{P}(X)$. We denote it by $\{X_i\}_{i \in I}$, where $X_i = f(i), i \in I$. The set I is called the index set.

Many times the set X is understood, so we just talk about the family of sets $\{X_i\}_{i\in I}$. There is an ambiguity in this notation, since in an arbitrary family $\{X_i\}_{i\in I}$ we may have $i_1 \neq i_2$ and still $X_{i_1} = X_{i_2}$. This ambiguity comes from the fact that for example if $A \subseteq X$ and $I = \{1,2\}$ the family with two elements $\{A_i\}_{i=1,2}$ where $A_1 = A_2 = A$, as a set is just $\{A\}$.

We define the union and the intersection of the family of sets $\{X_i\}_{i\in I}$ by

$$\bigcup_{i\in I} X_i = \{x \in X : \exists j \in I, x \in X_j\}, \quad \bigcap_{i\in I} X_i = \{x \in X : \forall j \in I, x \in X_j\}.$$

If $I = \{1,2,3,...,n\}$, then we will often use the more familiar notation

$$\bigcup_{i=1}^{n} X_i \text{ or } \bigcap_{i=1}^{n} X_i.$$

Example 4.68. Suppose, for each positive integer n, that $X_n = \{1,2,3,...,n\}$. The index set I in this case is the set of all positive integers. Then $\bigcup_{n\in I} X_n = I$ and $\bigcap_{n\in I} X_n = \{1\}$.

Example 4.69. Let $I = (0,\infty)$ and let $X_i = (-i,i)$ for each $i \in I$. In this case $\bigcup_{i\in I} X_i = (-\infty,\infty)$ and $\bigcap_{i\in I} X_i = \{0\}$.

Theorem 4.70. *We have*

1. $x \in \bigcup_{i\in I} X_i \Leftrightarrow \exists j \in I$ *such that* $x \in X_j$.
2. *If* $\{X_i\}_{i\in I}$ *and* $\{X_j\}_{j\in J}$ *are two family of sets, then* $\bigcup_{i\in I} X_i \cup \bigcup_{j\in J} X_j = \bigcup_{k\in I\cup J} X_k$.
3. $A \cap (\bigcup_{i\in I} X_i) = \bigcup_{i\in I}(A \cap X_i)$ *for any set* A.
4. $(\bigcup_{i\in I} X_i)' = \bigcap_{i\in I} X_i'$.

Proof. 1. By definition, if $x \in \bigcup_{i\in I} X_i$, we can find $j \in I$ with $x \in X_j$. Conversely, if $x \in X_j$, then $x \in \bigcup_{i\in I} X_i$ by the definition of the union.

2. Let $x \in \bigcup_{i\in I} X_i \cup \bigcup_{j\in J} X_j$. Then $x \in \bigcup_{i\in I} X_i$ or $x \in \bigcup_{j\in J} X_j$. By definition, there is $i_0 \in I$ such that $x \in X_{i_0}$ or there is $j_0 \in J$ with $x \in X_{j_0}$. In any case, there is $k_0 \in I \cup J$ (take $k_0 = i_0$ or $k_0 = j_0$) such that $x \in X_{k_0}$. We conclude that $x \in \bigcup_{k\in I\cup J} X_k$, hence $\bigcup_{i\in I} X_i \cup \bigcup_{j\in J} X_j \subseteq \bigcup_{k\in I\cup J} X_k$. The other inclusion is similar.

3. Let $x \in A \cap (\bigcup_{i\in I} X_i)$. Then $x \in A$ and $x \in \bigcup_{i\in I} X_i$, hence there is $j \in I$ with $x \in A$ and $x \in X_j$. This means $x \in A \cap X_j$, hence $x \in \bigcup_{i\in I}(A \cap X_i)$ and $A \cap (\bigcup_{i\in I} X_i) \subseteq \bigcup_{i\in I}(A \cap X_i)$ for any set A. The other inclusion is similar.

4. Let $x \in (\bigcup_{i\in I} X_i)'$. This means that for all $i \in I$ we have $x \notin X_i$, hence that for all $i \in I$ we have $x \in X_i'$. We conclude that $x \in \bigcap_{i\in I} X_i'$ and that $(\bigcup_{i\in I} X_i)' \subseteq \bigcap_{i\in I} X_i'$. Similarly, we can prove the other inclusion.

□

Exercise 4.71. a. Prove that $\bigcup_{i\in I} X_i$ is the smallest set containing all the sets X_i.

b. Show that $\bigcap_{i\in I} X_i$ is the largest set contained in all the sets X_i.

c. State and prove the dual statements of parts 2,3 and 4 of the above Theorem.

Exercise 4.72. Consider a family of sets $\{A_n\}_{n\geq 1}$. Prove that there is a family of disjoint sets $\{B_n\}_{n\geq 1}$ such that

$$\bigcup_{n=1}^{\infty} A_n = \bigcup_{n=1}^{\infty} B_n.$$

Hint. Take $B_1 = A_1, B_2 = A_2 \setminus A_1, B_3 = A_3 \setminus (A_1 \cup A_2)$ etc.

Exercise 4.73. Consider a family of sets $\{E_n\}_{n\geq 1}$ and define

$$\limsup E_n = \bigcap_{k=1}^{\infty} \bigcup_{n=k}^{\infty} E_n, \quad \liminf E_n = \bigcup_{k=1}^{\infty} \bigcap_{n=k}^{\infty} E_n.$$

Prove that

$$\limsup E_n = \{x : x \in E_n \text{ for infinitely many } n\},$$
$$\liminf E_n = \{x : x \in E_n \text{ for all but finitely many } n\}.$$

Exercise 4.74. Compute $\limsup E_n$ and $\liminf E_n$ for the following families of sets

a) $E_n = [n, n+1), n \geq 1$.

b) $E_n = \{1, 2, ..., n\}, n \geq 1$.

Definition 28. The Cartesian product of a family of sets $\{X_i : i \in I\}$ is

$$\prod_{i\in I} X_i = \{x : I \to \bigcup_{i\in I} X_i : x(j) \in X_j \text{ for all } j \in I\}.$$

Exercise 4.75. For $I = \{1, 2\}$, compare the new definition of $\prod_{i=1}^{2} X_i = X_1 \times X_2$ with the old one.

We are now in the position to add a new axiom to our set theory axioms:

Axiom 3 (*Axiom of choice*). Let $\mathcal{F}$ be any family of nonempty sets. Then there is a function f defined on $\mathcal{F}$ such that $f(A) \in A$ for all $A \in \mathcal{F}$. The function f is called a choice function, and its existence may be thought of as the result of choosing for each of the sets A in $\mathcal{F}$ an element in A.

There is, of course, no difficulty in constructing the function f if the family $\mathcal{F}$ is finite; also, if for example $\mathcal{F}$ is made of subsets of natural numbers, we can define $f(A)$ to be the minimum of A. For $\mathcal{F}$ infinite we may need the axiom of choice in general. (Recall that a set is finite if it is empty or it is in bijection with $\{1, 2, ..., n\}$ for some positive integer n. A set is infinite if it is not finite).

The Axiom of choice can be stated as: For each nonempty set X there is a function $c : \mathcal{P}(X) \setminus \{\emptyset\} \to X$ satisfying $c(A) \in A$ for every $A \in \mathcal{P}(X) \setminus \{\emptyset\}$.

Remark 4.76. The axiom of choice is equivalent to the fact that if none of the sets of a nonempty family $\{X_i : i \in I\}$ are empty, then the Cartesian product $\prod_{i\in I} X_i$ is not empty.

Proof. Indeed, assuming the axiom of choice, given $\{X_i\}_{i\in I}$, we can define a function $x : I \to \bigcup_{i\in I} X_i$ such that $x(i) \in X_i$. Conversely, given a family $\mathcal{F}$ of nonempty sets, the fact that the cartesian product of all members in $\mathcal{F}$ is nonempty means that we can choose for each $A \in \mathcal{F}$ an element in A. □

We will mention other equivalent statements with the Axiom of choice, like Zorn's Lemma and the Hausdorff maximal principle, in the next chapter. Many proofs in mathematics require the Axiom of choice. For example,

Theorem 4.77. *The function $f : X \to Y$ has a section iff f is surjective.*

Proof. If $f : X \to Y$ has a section $s : Y \to X$, then given $y \in Y$ we can take $s(y) \in X$ such that $f(s(y)) = y$, hence f is surjective. Conversely, if $f : X \to Y$ is surjective, we can construct a section $s : Y \to X$ as follows: for each $y \in Y$ choose an element x in the nonempty set $f^{-1}(y)$, and define $s(y) = x$. This is possible by the Axiom of choice. Moreover, $f(s(y)) = f(x) = y$, so s is a section for f. □

Notation 1. Given sets X, Y, the set of all functions from X to Y is denoted by Y^X.

This notation will be useful when we will discuss cardinalities and counting techniques.

Exercise 4.78. Find $\{a, b\}^{\{1,2,3\}}$. How many elements are in this set? How many are one-to-one? How many are onto?

Chapter 5

Relations

You already heard about relations like the order relation between real numbers or the relation of inclusion between sets. Since we will need other kinds of relations, in this chapter we will define this concept in general, using the theory of sets.

5.1. General relations and operations

Definition 29. Consider two sets X and Y. A *relation* R from X to Y is a subset of the Cartesian product $X \times Y$. If $X = Y$, we say that R is a relation on X.

We often write xRy to express the fact that $\langle x, y\rangle \in R$.

Example 5.1. Consider $X = \{1, 2, 3, 6\}$ and the relation xRy if x divides y. As a subset of $X \times X$,

$$R = \{\langle 1,1\rangle, \langle 1,2\rangle, \langle 1,3\rangle, \langle 1,6\rangle, \langle 2,2\rangle, \langle 2,6\rangle, \langle 3,3\rangle, \langle 3,6\rangle, \langle 6,6\rangle\}.$$

The *domain* of R, denoted by $\text{dom}(R)$, consists of all first components of pairs in R. Specifically,

$$\text{dom}(R) = \{x \in X : \exists y \in Y \text{ such that } \langle x, y\rangle \in R\}.$$

Note that the domain of R may be a proper subset of X.

The range of R, written $\text{ran}(R)$, is the set of all second components of pairs in R:

$$\text{ran}(R) = \{y \in Y : \exists x \in X \text{ such that } \langle x, y\rangle \in R\},$$

a subset of Y.

Remark 5.2. Given a relation R from X to Y, if we let $Z =\text{dom}(R) \cup \text{ran}(R)$, then $R \subseteq Z \times Z$, so R can be viewed as a relation on Z.

Definition 30. Consider a relation R from X to Y and subsets $A \subseteq X, B \subseteq Y$. The direct image $R(A)$ is defined as

$$R(A) = \{y \in Y : \exists a \in A \text{ with } \langle a, y \rangle \in R\},$$

and the inverse image $R^{-1}(B)$ is defined as

$$R^{-1}(B) = \{x \in X : \exists b \in B \text{ with } \langle x, b \rangle \in R\}.$$

Example 5.3. Consider $X = \{1, 2, 3, 6\}$ and the relation xRy if x divides y. Then $\mathrm{dom}(R) = \mathrm{ran}(R) = X$,

$$R(\{1, 3\}) = \{1, 2, 3, 6\}, \quad R^{-1}(\{2, 3\}) = \{1, 2, 3\}.$$

Example 5.4. Consider $X = \{1, 2, 3\}$ and $Y = \{a, b, c\}$. Then $S = \{\langle 1, b\rangle, \langle 2, a\rangle\}$ is a relation with domain $\{1, 2\}$ and range $\{a, b\}$. We have

$$S(\{2, 3\}) = \{a\}, \quad S^{-1}(\{b, c\}) = \{1\}.$$

Of course, $R(A)$ is a subset of Y, $R^{-1}(B)$ is a subset of X and $\mathrm{ran}(R) = R(X)$. This way, R defines a function $R : \mathcal{P}(X) \to \mathcal{P}(Y)$ and a function $R^{-1} : \mathcal{P}(Y) \to \mathcal{P}(X)$. Again we abuse the notation, since R has now two different meanings. Note that here R^{-1} denotes a set function; the inverse of a relation is defined below.

Example 5.5. Any function $f : X \to Y$ is a relation from X to Y, with domain X and range a subset of Y. But of course not every relation is a function. The direct image and the inverse image of a function viewed as a relation coincide with those from the previous chapter.

Definition 31. Let $P(x, y)$ be a property depending on $x \in X$ and $y \in Y$. We can form

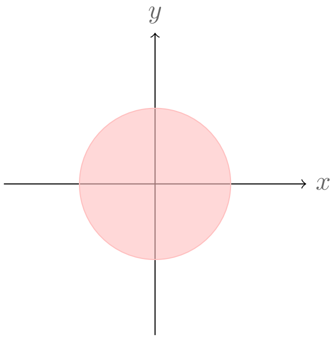
$$\{\langle x, y\rangle \in X \times Y : P(x, y) \text{ is true}\}$$

as the set of ordered pairs satisfying the property.

Example 5.6. Let $P(x, y)$ be $x^2 + y^2 \leq 1$ for $x, y \in \mathbb{R}$. Then

$$T = \{\langle x, y\rangle \in \mathbb{R} \times \mathbb{R} : x^2 + y^2 \leq 1\}$$

is a relation on $\mathbb{R}$. Note that $\mathrm{dom}(T) = \mathrm{ran}(T) = [-1, 1]$. We can visulize T as a disc in the plane



Remark 5.7. Given a relation $R \subseteq X \times X$ and a set Y such that $X \subset Y$, R can be considered as a relation on Y. Notice that even though we may have the same set of ordered pairs, we are dealing with a different concept. For example, suppose R is the relation

$$\{\langle x, y\rangle : x \leq y \text{ and } x, y \text{ are integers}\},$$

X is the set of integers, and Y is the set of rational numbers. If R is considered as a relation on X, we can properly infer that for all $x \in X$, $\langle x, x\rangle \in R$. However if we assume that R is a relation on Y, then for example $\langle \frac{1}{2}, \frac{1}{2}\rangle \notin R$.

Remark 5.8. Given relations R_i from X_i to Y_i, $i = 1, 2$, we can take their union $R_1 \cup R_2$, intersection $R_1 \cap R_2$ or differences $R_1 \setminus R_2$, $R_2 \setminus R_1$, and we get new relations as subsets of $(X_1 \cup X_2) \times (Y_1 \cup Y_2)$. Also, given a relation R from X to Y, we may consider its complement $R' \subseteq X \times Y$, which is another relation from X to Y.

Example 5.9. Consider $R_1 = \{\langle u, u\rangle, \langle v, v\rangle, \langle u, v\rangle\}$ as a relation on $\{u, v\}$ and $R_2 = \{\langle v, v\rangle, \langle w, w\rangle, \langle v, w\rangle, \langle w, v\rangle\}$ as a relation on $\{v, w\}$. Then

$$R_1 \cup R_2 = \{\langle u, u\rangle, \langle v, v\rangle, \langle u, v\rangle, \langle v, v\rangle, \langle w, w\rangle, \langle v, w\rangle, \langle w, v\rangle\},$$

$$R_1 \cap R_2 = \{\langle v, v\rangle\}, \quad R_1 \setminus R_2 = \{\langle u, u\rangle, \langle u, v\rangle\}, \quad R_2 \setminus R_1 = \{\langle w, w\rangle, \langle v, w\rangle, \langle w, v\rangle\}$$

as relations on $\{u, v, w\}$. Moreover, $R_1' = \{\langle v, u\rangle\}$ and $R_2' = \emptyset$.

Definition 32. The *inverse* of a relation $R \subseteq X \times Y$ is the relation

$$R^{-1} = \{\langle y, x\rangle \in Y \times X : \langle x, y\rangle \in R\},$$

a subset of $Y \times X$.

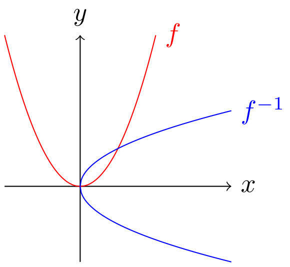
Remark 5.10. If R is a relation from X to Y, then R^{-1} is a relation from Y to X and $yR^{-1}x \Leftrightarrow xRy$. In particular, the inverse of a relation is defined always. For example, given any function f, we can form f^{-1} as a relation. This relation is a function only in the case that f is bijective.

Example 5.11. For the relation $R_1 = \{\langle 1, b\rangle, \langle 2, a\rangle\}$ we have $R_1^{-1} = \{\langle b, 1\rangle, \langle a, 2\rangle\}$ and for the relation $R_2 = \{\langle v, v\rangle, \langle w, w\rangle, \langle v, w\rangle, \langle w, v\rangle\}$ we have $R_2^{-1} = R_2$.

Example 5.12. Let $f : \mathbb{R} \to \mathbb{R}, f(x) = x^2$. We know that f is not one-to-one, in particular is not an invertible function. Then the relation f^{-1} is

$$f^{-1} = \{\langle x^2, x\rangle : x \in \mathbb{R}\}.$$

We can visualize f, f^{-1} as subsets of $\mathbb{R}^2$:



Note that f^{-1} is the reflection of f into the line $y = x$.

Theorem 5.13. *If R and S are relations from X to Y, then:*

1. $(R^{-1})^{-1} = R$.
2. $(R \cup S)^{-1} = R^{-1} \cup S^{-1}$.
3. $(R \cap S)^{-1} = R^{-1} \cap S^{-1}$.
4. $(R \setminus S)^{-1} = R^{-1} \setminus S^{-1}$.

Proof. 1. follows from the definition of the inverse: $\langle x, y\rangle \in (R^{-1})^{-1}$ iff $\langle y, x\rangle \in R^{-1}$ iff $\langle x, y\rangle \in R$.

For 2,3,4 recall that $R \cup S, R \cap S, R \setminus S$ are also relations from X to Y and by taking the inverses we reverse the ordered pairs. □

Definition 33. If R and S are relations, the composition of R and S is the relation

$$\{\langle x, y\rangle : \exists z \text{ such that } \langle x, z\rangle \in S \text{ and } \langle z, y\rangle \in R\}.$$

We denote the composition by $R \circ S$.

Remark 5.14. Some people prefer the notation $S \circ R$, but this clashes with the notation for composition of functions, introduced in the previous chapter. Indeed, $\langle x, y\rangle \in f \circ g$ if there is $\langle x, z\rangle \in g$ and $\langle z, y\rangle \in f$, hence we have $z = g(x)$ and $y = f(g(x))$. Notice that $\text{dom}(R \circ S) \subseteq \text{dom}(S)$ and $\text{ran}(R \circ S) \subseteq \text{ran}(R)$. In general $R \circ S \neq S \circ R$.

Example 5.15. With $R_1 = \{\langle 1, b\rangle, \langle 2, a\rangle\}$ and $R_2 = \{\langle x, y\rangle \in \mathbb{R} \times \mathbb{R} : x^2 + y^2 = 1\}$, $R_1 \circ R_1 = \emptyset$, $R_2 \circ R_2 = R_2$. In particular notice that the composition of two relations may be empty.

Example 5.16. Let xPy if x is a parent of y, and xSy if x is a sister of y. Then $P \circ P = G$ where xGy if x is a grandparent of y and $P \circ S = A$, where xAy if x is an aunt of y.

Theorem 5.17. *If R and S are relations, then:*

1. $(R \circ S) \circ T = R \circ (S \circ T)$.
2. $(R \circ S)^{-1} = S^{-1} \circ R^{-1}$.
3. $R \circ (S \cap T) \subseteq (R \circ S) \cap (R \circ T)$.
4. $R \circ (S \cup T) = (R \circ S) \cup (R \circ T)$.

Proof. 1. Let $\langle x, y\rangle \in (R \circ S) \circ T$. Then there is z such that $\langle x, z\rangle \in T$ and $\langle z, y\rangle \in R \circ S$. We can find $w \in \text{dom}(R) \cap \text{ran}(S)$ such that $\langle z, w\rangle \in S$ and $\langle w, y\rangle \in R$. It follows that $\langle x, w\rangle \in S \circ T$, and we conclude that $\langle x, y\rangle \in R \circ (S \circ T)$. The other inclusion is proved similarly.

2. Let $\langle x, y\rangle \in (R \circ S)^{-1}$. Then $\langle y, x\rangle \in R \circ S$, so there is z with $\langle y, z\rangle \in S$ and $\langle z, x\rangle \in R$. But then $\langle x, z\rangle \in R^{-1}$ and $\langle z, y\rangle \in S^{-1}$, so $\langle x, y\rangle \in S^{-1} \circ R^{-1}$. The other inclusion is similar.

3. Let $\langle x, y\rangle \in R \circ (S \cap T)$. We can find z with $\langle x, z\rangle \in S \cap T$ and $\langle z, y\rangle \in R$. It follows that $\langle x, y\rangle \in R \circ S$ and $\langle x, y\rangle \in R \circ T$, hence $\langle x, y\rangle \in (R \circ S) \cap (R \circ T)$. Note that the reversed inclusion may be false. Where does the proof break down?

4. We leave this for the reader. □

Theorem 5.18. *If R and S are relations, then:*

1. $dom(R \cap S) \subseteq dom(R) \cap dom(S)$.
2. $ran(R \cap S) \subseteq ran(R) \cap ran(S)$.
3. $dom(R \cup S) = dom(R) \cup dom(S)$.
4. $ran(R \cup S) = ran(R) \cup ran(S)$.
5. $dom(R) = ran(R^{-1})$.

Proof. 1. Let $x \in \mathrm{dom}(R \cap S)$. Then there is y such that $\langle x, y\rangle \in R \cap S$. This means that $\langle x, y\rangle \in R$ and $\langle x, y\rangle \in S$, hence $x \in \mathrm{dom}(R) \cap \mathrm{dom}(S)$. The reversed inclusion is false. Here is a counterexample: let $R = \{\langle a, b\rangle, \langle b, a\rangle\}, S = \{\langle a, b\rangle, \langle b, c\rangle\}$. Then $R \cap S = \{\langle a, b\rangle\}, \mathrm{dom}(R \cap S) = \{a\}$ and $\mathrm{dom}(R) \cap \mathrm{dom}(S) = \{a, b\}$.

We leave the others for the reader. □

Exercise 5.19. Consider two relations R and S.

a. What can you say about $\mathrm{dom}(R \cap S)^{-1}$?

b. What can you say about $\mathrm{dom}(R \cup S)^{-1}$?

c. What can you say about $\mathrm{dom}(R \circ S)^{-1}$?

Exercise 5.20. Let $A = \{2, 3, 4\}$ and let $B = \{2, 6, 12, 17\}$. List the elements of

$$R = \{\langle x, y\rangle \in A \times B : x \text{ divides } y\}.$$

Find R^{-1}, $\mathrm{dom}(R)$ and $\mathrm{ran}(R)$.

Exercise 5.21. Let $A = \{1, 2, 3, 4\}$ and consider

$$R = \{\langle x, y\rangle \in A \times A : y - x \text{ is an even natural number}\}.$$

Find the elements of R and find $R \circ R$.

Exercise 5.22. Let S be the relation from $\{a, b, c, 2, 3\}$ to $\{a, b, e, f, 3, 6\}$,

$$S = \{\langle c, a\rangle, \langle b, 3\rangle, \langle 3, e\rangle, \langle 2, b\rangle, \langle a, f\rangle, \langle b, 6\rangle\}.$$

Find $\mathrm{dom}(S)$, $\mathrm{ran}(S)$ and S^{-1}.

Exercise 5.23. Find the domain and range for the following relations on $\mathbb{R}$ and then graph them:

a. $R_1 = \{\langle x, y\rangle \in \mathbb{R} \times \mathbb{R} : x = -2y^2 + 3\}$

b. $R_2 = \{\langle x, y\rangle \in \mathbb{R} \times \mathbb{R} : x = \sqrt{1 - y^2}\}$

c. $R_3 = \{\langle x, y\rangle \in \mathbb{R} \times \mathbb{R} : x = -3 \vee |y| < 4\}$

d. $R_4 = \{\langle x, y\rangle \in \mathbb{R} \times \mathbb{R} : x = -3 \wedge |y| < 4\}$

e. $R_5 = \{\langle x, y\rangle \in \mathbb{R} \times \mathbb{R} : x^2 + y^2 < 9\}$

f. $R_6 = \{\langle x, y\rangle \in \mathbb{R} \times \mathbb{R} : |x| + |y| \leq 9\}$.

Exercise 5.24. Find the inverse of the following relations

a. $R = \{\langle a, 1\rangle, \langle 2, b\rangle, \langle 3, 4\rangle, \langle x, y\rangle\}$

b. $S = \{\langle x, y\rangle \in \mathbb{Z} \times \mathbb{Z} : x^2 + y^2 = 1\}$

c. $T = \{\langle x, y\rangle \in \mathbb{R} \times \mathbb{R} : 3x^2 - 4y^2 = 9\}$

d. $V = \{\langle x, y\rangle \in \mathbb{R} \times \mathbb{R} : y < 2x - 5\}$

e. $W = \{\langle x, y\rangle \in \mathbb{R} \times \mathbb{R} : y(x+3) = x\}$.

Exercise 5.25. Let $R = \{\langle 1,4\rangle, \langle 2,3\rangle, \langle 5,4\rangle, \langle 3,2\rangle\}$, let $S = \{\langle 5,1\rangle, \langle 2,4\rangle, \langle 3,3\rangle\}$ and let $T = \{\langle 1,2\rangle, \langle 2,1\rangle\}$. Compute $R \circ S, S \circ T, R \circ R, T \circ T, R \circ (S \circ T), (R \circ S) \circ T, (R \circ S)^{-1}, R^{-1} \circ S^{-1}$.

Exercise 5.26. Use set-builder notation to describe $S \circ R$ for the given relations

a. $R = \{\langle x, y\rangle \in \mathbb{R} \times \mathbb{R} : y = 2x - 1\}, S = \{\langle x, y\rangle \in \mathbb{R} \times \mathbb{R} : 2x^2 + 3y^2 = 5\}$

b. $R = \{\langle x, y\rangle \in \mathbb{R} \times \mathbb{R} : y = \sqrt{x}\}, S = \{\langle x, y\rangle \in \mathbb{R} \times \mathbb{R} : y = \sin x\}$.

Exercise 5.27. Let P be the set of all living people, and consider the relations

$$B = \{\langle x, y\rangle \in P \times P : y \text{ is a brother of } x\},$$

$$F = \{\langle x, y\rangle \in P \times P : y \text{ is the father of } x\},$$

$$M = \{\langle x, y\rangle \in P \times P : y \text{ is the mother of } x\}$$

and

$$S = \{\langle x, y\rangle \in P \times P : y \text{ is a sister of } x\}.$$

Describe the relations $F \circ F, M \circ F, F \circ M, M \circ B, B \circ M, F \circ S, S \circ M, M \circ S$.

Exercise 5.28. Let R, S be relations on A. Provide counterexamples to the statements

a. $\mathrm{dom}(R) \subseteq \mathrm{dom}(S \circ R)$

b. $\mathrm{ran}(S) \subseteq \mathrm{ran}(S \circ R)$.

Exercise 5.29. Consider R, S, T relations on X. Does $R \circ S = R \circ T$ imply that $S = T$? Does $R \circ (T \cap T) = (R \circ S) \cap (R \circ T)$?

Exercise 5.30. Specify the inverse relations for the functions

a. $\{\langle x, x^2 + 1\rangle : x \in \mathbb{R}\}$,

b. $\{\langle x, e^{e^x}\rangle : x \in \mathbb{R}\}$.

5.2. Equivalence relations

Definition 34. Suppose R is a relation on X. We say:

1. R is *reflexive* iff $\forall x \in X$ we have xRx.
2. R is *symmetric* iff $\forall x, y \in X$ we have $xRy \Rightarrow yRx$.
3. R is *transitive* iff $\forall x, y, z \in X$ we have $xRy \wedge yRz \Rightarrow xRz$.
4. R is an *equivalence relation* if and only if R is reflexive, symmetric, and transitive.

Example 5.31. Let $X = \{a, b, c\}$ and let

$$R = \{\langle a, a\rangle, \langle a, b\rangle, \langle b, a\rangle, \langle b, b\rangle, \langle c, c\rangle\}.$$

Then R is an equivalence relation on X. Indeed, it is reflexive since $\langle a, a\rangle, \langle b, b\rangle, \langle c, c\rangle \in R$. It is symmetric since $\langle a, b\rangle \in R$ implies $\langle b, a\rangle \in R$. Transitivity follows easily by inspection.

Example 5.32. Let X be a nonempty set, and consider the equality relation on X: xRy iff $x = y$. Then R is obviously reflexive, symmetric and transitive, so equality is an equivalence relation.

Example 5.33. Let $X = \{a, b, c\}$ and let $S = \{\langle a, a\rangle, \langle a, b\rangle, \langle b, c\rangle\}$. Then S is not reflexive, since $\langle b, b\rangle \notin S$, is not symmetric since $\langle a, b\rangle \in S$ but $\langle b, a\rangle \notin S$, and it is not transitive since $\langle a, b\rangle, \langle b, c\rangle \in S$, but $\langle a, c\rangle \notin S$.

Exercise 5.34. Consider R a relation on X. Fill in the blank and prove the resulting statement:

a) We have $R \circ R \subseteq R$ iff ___________.

b) R is symmetric iff the complement R' ___________.

Example 5.35. Let $X = \mathbb{Z} \setminus \{0\}$ and $D = \{\langle x, y\rangle \in X \times X : x \text{ divides } y\}$. Then D is reflexive and transitive, but not symmetric because $\langle 2, 4\rangle \in D$ but $\langle 4, 2\rangle \notin D$.

Exercise 5.36. Find two relations on $\{1, 2, 3\}$ which are not reflexive, but their composition is reflexive.

Exercise 5.37. Let $S = \{1, 2, 3, 4\}$, and suppose that $\sim$ is an equivalence relation on S. You know that $1 \sim 2$ and $2 \sim 3$. Describe all possibilities for $\sim$.

Example 5.38. For $X = \mathbb{Z}$ and n a positive integer, let xRy if and only if n divides $x - y$. Then R is an equivalence relation on X, called congruence modulo n. Another notation for this relation is $x \equiv y (\text{mod } n)$.

Indeed, R is reflexive since for all $x \in X$, n divides $x - x = 0$. If n divides $x - y$, then n divides $y - x$, so R is symmetric. If n divides $x - y$ and n divides $y - z$, then n divides $x - y + y - z = x - z$, hence R is transitive.

Exercise 5.39. Let $A \neq \emptyset$ and let R be an equivalence relation on A which is also a function on A. Describe the relation R.

Definition 35. Suppose X is a set and $\mathcal{P}$ is a family of subsets of X. We say that $\mathcal{P}$ is a partition of X if and only if:

1. $A \in \mathcal{P} \Rightarrow A \neq \emptyset$,

2. $\mathcal{P}$ is disjointed (any two different members of $\mathcal{P}$ have empty intersection), and

3. $\displaystyle\bigcup_{A \in \mathcal{P}} A = X$.

Example 5.40. The family of sets $\{\{1, 2, 3\}, \{4, 5\}, \{6\}\}$ is a partition of the set $\{1, 2, 3, 4, 5, 6\}$, but not of the set $\{1, 2, 3, 4, 5\}$.

Example 5.41. The family $\{\{1, 2, 3\}, \{4, 5, 6\}, \{6\}\}$ is not a partition of the set $\{1, 2, 3, 4, 5, 6\}$; in fact, it is not a partition of any set, since $\{4, 5, 6\} \cap \{6\} = \{6\} \neq \emptyset$.

Theorem 5.42. *Suppose $\mathcal{P} = \{X_i\}_{i \in I}$ is a partition of X. Then there is an equivalence relation R on X such that:*

$$xRy \Leftrightarrow \exists i \in I \textit{ such that } x, y \in X_i.$$

Proof. Let $x \in X$. Since $X = \bigcup_{i \in I} X_i$, there is an $i_0 \in I$ with $x \in X_{i_0}$. Hence xRx, and R is reflexive. Obviously R is symmetric by definition. Let $x, y, z \in X$ with xRy and yRz. There is $i \in I$ with $x, y \in X_i$ and there is $j \in I$ with $y, z \in X_j$. Since $y \in X_i \cap X_j$ and $\mathcal{P}$ is a partition, we have $i = j$ and $X_i = X_j$, so $x, z \in X_i$ and xRz, hence R is transitive. □

Definition 36. Suppose X is a set and R is an equivalence relation on X. The equivalence class of $x \in X$, denoted $[x]$, is the set

$$[x] = \{y \in X : xRy\}.$$

An element $a \in [x]$ is called a representative of the class of x. The set of (distinct) equivalence classes is denoted by X/R, and it is called the quotient set.

Theorem 5.43. *Consider an equivalence relation R on X. Then the family of equivalence classes*

$$X/R = \{[x] \mid x \in X\}$$

forms a partition of X.

Proof. Notice that each $[x]$ is a nonempty subset of X, since $x \in [x]$. Moreover, $X = \bigcup_{x \in X} [x]$.

We want to show that two equivalence classes are either equal or disjoint. If xRy, then for any $x' \in [x]$ we have xRx', and by transitivity we get $x'Ry$, hence $x' \in [y]$ and $[x] \subseteq [y]$. Similarly we get the other inclusion, hence for xRy we have $[x] = [y]$.

Suppose $\langle x, y \rangle \notin R$. If there is $z \in [x] \cap [y]$, from zRx and zRy we get xRy, contradiction. Hence $[x] \cap [y] = \emptyset$, and we are done.

□

Example 5.44. Consider $R = \{\langle a, a \rangle, \langle a, b \rangle, \langle b, a \rangle, \langle b, b \rangle, \langle c, c \rangle\}$ the equivalence relation on $X = \{a, b, c\}$. Then $[a] = [b] = \{a, b\}, [c] = \{c\}$ and the corresponding partition of X is $\{\{a, b\}, \{c\}\}$. The quotient set X/R is $\{[a], [c]\} = \{\{a, b\}, \{c\}\}$.

Example 5.45. Consider R the congruence modulo n on $\mathbb{Z}$, where $n \geq 2$. Then $\mathbb{Z}/R$ has n elements, denoted $[0], [1], [2], ..., [n-1]$. The set of equivalence classes is denoted $\mathbb{Z}_n$. When we want to emphasize n we write $[x]_n$ for the congruence class of x modulo n.

Example 5.46. Given a function $f : X \to Y$, consider the relation R_f on X defined by

$$aR_f b \Leftrightarrow f(a) = f(b).$$

Then R_f is an equivalence relation. Indeed, since $f(x) = f(x)$ for all $x \in X$, R_f is reflexive. For $xR_f y$ we have $f(x) = f(y)$ which is the same as $f(y) = f(x)$, therefore R_f is symmetric. Transitivity follows since $f(x) = f(y)$ and $f(y) = f(z)$ implies $f(x) = f(z)$.

In particular, let $f(x) = x^2, x \in [-1, 1]$. Let's describe the equivalence classes for R_f and let's identify the quotient set. Since $f(-x) = f(x)$ it follow that $[x] = \{-x, x\}$ and $[-1, 1]/R_f$ can be identified with $[0, 1]$.

Exercise 5.47. For $x, y \in \mathbb{Z}$ define xRy if 4 divides $x + 3y$. Prove that R is an equivalence relation and describe its quotient set $\mathbb{Z}/R$.

Exercise 5.48. For $g(x) = \sin x, x \in [0, 2\pi]$, determine R_g and $[0, 2\pi]/R_g$.

Remark 5.49. Given an equivalence relation R on X, there is a canonical surjection $\pi : X \to X/R, \pi(x) = [x]$. In order to define functions on X/R, usually we start with a function on X, say $f : X \to Y$ and check if f does not depend on representatives, i.e. if $x_1 R x_2$ implies $f(x_1) = f(x_2)$. If this is the case for all $x_1, x_2 \in X$, then f induces a well defined function $\bar{f} : X/R \to Y$ such that $\bar{f} \circ \pi = f$. If the values of f depend on representatives, we say that $\bar{f}$ is not well defined.

Example 5.50. For $X = \{a, b, c\}$ and $R = \{\langle a, a\rangle, \langle a, b\rangle, \langle b, a\rangle, \langle b, b\rangle, \langle c, c\rangle\}$, let $f : X \to \{1, 2, 3\}, f(a) = f(b) = 2, f(c) = 1$. Since $f(a) = f(b)$, we get a well defined function $\bar{f} : X/R \to \{1, 2, 3\}, \bar{f}([a]) = 2, \bar{f}([c]) = 1$.

Exercise 5.51. Prove that $f : \mathbb{Z}_4 \to \mathbb{Z}_2, f([x]_4) = [x]_2$ is a well defined function.

Exercise 5.52. Prove that $f : \mathbb{Z}_3 \to \mathbb{Z}_5, f([x]_3) = [x]_5$ is not a well defined function.

Exercise 5.53. Let $f : \mathbb{Z}_5 \to \mathbb{Z}_5, f([x]) = [2x + 3]$. Prove that f is well defined and determine whether f is one-to-one and onto.

Definition 37. Let R be an equivalence relation on X. A subset $A \subseteq X$ is called saturated if it is the union of some equivalence classes, in other words $(a \in A \wedge aRb) \Rightarrow b \in A$.

Exercise 5.54. Given an equivalence relation on X and $B \subseteq X$ an arbitrary subset, prove that there is $A \subseteq X$ saturated such that $B \subseteq A$.

Example 5.55. For the congruence modulo 5 on $\mathbb{Z}$, the set $A = \{5k : k \in \mathbb{Z}\}$ is saturated, since $A = [0]$, but $B = \{0, 1, 2\}$ is not. The smallest saturated set containing B is $[0] \cup [1] \cup [2]$.

Exercise 5.56. Let D be the set of differentiable functions on $\mathbb{R}$. Define $f \sim g$ iff $f' = g'$. Prove that $\sim$ is an equivalence relation and describe $D/\sim$.

Exercise 5.57. Construct all quotient sets of $\{1, 2, 3\}$.

Exercise 5.58. Let $\mathcal{T}$ be the set of triangles in the plane and define the relation $\sim$ on $\mathcal{T}$ by $t_1 \sim t_2$ if t_1, t_2 are similar. Prove that $\sim$ is an equivalence relation and describe $\mathcal{T}/\sim$.

Exercise 5.59. Let X be the unit circle $\{\langle x, y\rangle \in \mathbb{R}^2 : x^2 + y^2 = 1\}$ and define R on X by $\langle x_1, y_1\rangle R\langle x_2, y_2\rangle$ if $\langle x_1, y_1\rangle = \pm\langle x_2, y_2\rangle$. Prove that R is an equivalence relation and describe X/R. Answer the same question if X is the unit sphere $\{\langle x, y, z\rangle \in \mathbb{R}^3 : x^2 + y^2 + z^2 = 1\}$ and $\langle x_1, y_1, z_1\rangle R\langle x_2, y_2, z_3\rangle$ if $\langle x_1, y_1, z_1\rangle = \pm\langle x_2, y_2, z_3\rangle$.

5.3. Order relations

Definition 38. A relation R on X is called *antisymmetric* if $\forall x, y \in X,\ xRy \wedge yRx \Rightarrow x = y$. A relation R is an *order relation* if it is reflexive, antisymmetric and transitive. An order relation R on X is called a *total order* if for all $x, y \in X$ we have xRy or yRx. In this case we also say that x, y are comparable elements. If neither xRy or tRx are true, then x, y are incomparable.

Remark 5.60. Since not every order is total, a general order relation R on X is also called a partial order. The pair (X, R) is called a *partially ordered set* (to keep in mind that it may not be a totally ordered set) or a *p.o. set* for short. Many times a partial order is denoted $\preceq$ or $\leq$.

Example 5.61. In Calculus we already used the usual order $\leq$ on the set of real numbers $\mathbb{R}$. This is a total order relation on $\mathbb{R}$. Unless specified otherwise, when we talk about real numbers, $\leq$ denotes the usual order relation. Warning: the notation $\leq$ may have a different meaning in a different context.

Example 5.62. Let X be a set, and let $\mathcal{R}$ be the relation on $\mathcal{P}(X)$ such that $A\mathcal{R}B$ iff $A \subseteq B$. Then $\mathcal{R}$ is reflexive, antisymmetric and transitive, hence a partial order. Therefore, $(\mathcal{P}(X), \subseteq)$ is a p.o. set.

In general, $\subseteq$ is not a total order, since for $X = \{a, b, c\}$, $\{a, b\}$ and $\{a, c\}$ are incomparable: neither $\{a, b\} \subseteq \{a, c\}$ nor $\{a, c\} \subseteq \{a, b\}$ is true.

Example 5.63. Let $X = \mathbb{R}$ and define xRy iff $x < y$. Then R is neither reflexive or symmetric, but R is transitive. Such a relation is called a strict order. It can be shown that $\subset$ is also a strict order on $\mathcal{P}(X)$.

Example 5.64. Consider $X = \mathbb{R} \cup \{-\infty, \infty\}$ with the usual ordering on $\mathbb{R}$ and such that by definition $-\infty < x < \infty$ for all $x \in \mathbb{R}$. Then X with this order relation becomes a totally ordered set. The set X is denoted sometimes by $\bar{\mathbb{R}}$.

Exercise 5.65. Given an order relation R, we can define a new relation S such that xSy if xRy and $x \neq y$. Prove that the relation S is transitive. It is called the strict order associated to R.

Remark 5.66. Consider P a relation on X which is reflexive and transitive (such a relation is called a preorder relation). Consider R defined by $xRy \Leftrightarrow xPy$ and yPx. Then R is an equivalence relation.

Define now the relation S on the quotient set X/R such that $[x]S[y] \Leftrightarrow \exists x' \in [x]\ \exists y' \in [y]$ such that $x'Py'$. Then S is an order relation on X/R.

Proof. It is easy to check using the definition that R is reflexive, symmetric and transitive, so R is an equivalence relation.

Let's prove now that S is an order relation. We have $[x]S[x]$ since xPx, so S is reflexive. Assume $[x]S[y]$ and $[y]S[x]$. By definition, there are $x' \in [x], y' \in [y]$ such that $x'Py'$ and there are $y'' \in [y], x'' \in [x]$ such that $y''Px''$. By definition of R, we have $y'Py'', y''Py', x'Px''$ and $x''Px'$. In particular, $y'Py'', y''Px''$ and $x''Px'$. By transitivity of P, it follows that $y'Px'$, hence since also $x'Py'$, we get $x'Ry'$ and $[x] = [y]$. This proves that S is antisymmetric. Transitivity of S is left as an exercise.

□

Example 5.67. Let $\mid$ be the divisibility relation on $\mathbb{Z} \setminus \{0\}$, i.e. $x \mid y$ if there is $z \in \mathbb{Z} \setminus \{0\}$ such that $y = xz$. Then $\mid$ is a preorder relation. The associated equivalence relation has classes $[x] = \{-x, x\}$, and $\mathbb{Z}/R$ can be identified with the set of positive integers, denoted $\mathbb{P}$. The associated partial order is divisibility on $\mathbb{P}$.

Remark 5.68. Given an order relation R on X, we can define a new order relation by taking R^{-1}. This is called the opposite order. For example, if $\leq$ is the usual order on $\mathbb{R}$, then $\leq^{-1}$ is the same as $\geq$.

Exercise 5.69. Which of the following relations on $\mathbb{R}$ are reflexive? Which are symmetric? Which are transitive?

a) xRy iff $x - y \in \mathbb{Q}$.

b) xRy iff $x - y \in \mathbb{R} \setminus \mathbb{Q}$.

c) xRy iff $|x - y| \leq 2$.

Exercise 5.70. On a set of your choice, give examples of relations that possess exactly one or exactly two of the properties: reflexivity, symmetry, transitivity.

Exercise 5.71. Let U be a nonempty set. Describe the properties (reflexivity, symmetry, transitivity) of the following relations on $\mathcal{P}(U)$

a) $A\mathcal{R}B$ iff $A \cap B = \emptyset$.

b) $A\mathcal{R}B$ iff $A \cap B \neq \emptyset$.

c) $A\mathcal{R}B$ iff $A \Delta B = \emptyset$

d) $A\mathcal{R}B$ iff $A \setminus B$ is finite.

e) $A\mathcal{R}B$ iff $A \Delta B$ is finite.

Exercise 5.72. Let R and S be relations on X. Prove or disprove:

a) If R and S are reflexive, then $R \cap S, R \cup S$ are reflexive.

b) If R and S are symmetric, then $R \cap S, R \cup S$ are symmetric.

c) If R and S are antisymmetric, then $R \cap S, R \cup S$ are antisymmetric.

d) If R and S are transitive, then $R \cap S, R \cup S$ are transitive.

Exercise 5.73. Let R and S be partial orderings on X. Prove or disprove

a) $R \circ S$ is a partial ordering on X.

b) $R \cup S$ is a partial ordering on X.

c) $R \cap S$ is a partial ordering on X.

Exercise 5.74. On $\mathbb{R}$ define xRy to mean $x \leq y$ (usual order) and xSy to mean $y = x^2$. Find $S \circ R$ and $R \circ S$ and graph them.

Exercise 5.75. On $\mathbb{R}^2$ we define the relation R such that $\langle x, y\rangle R\langle x', y'\rangle$ if $x \leq x'$ or $y \leq y'$. Is R an order relation?

Exercise 5.76. How many total order relations can be defined on $\{1, 2, 3, 4\}$?

Exercise 5.77. Let $(X, \leq)$ be a p.o. set and let Y be an arbitrary set. On X^Y (the set of all functions $f : Y \to X$) we define $\preceq$ by $f_1 \preceq f_2$ iff $f_1(y) \leq f_2(y)$ for all $y \in Y$. Prove that $(X^Y, \preceq)$ is a p.o. set.

5.4. *More on ordered sets and Zorn's lemma

In this section, unless otherwise specified, $\preceq$ denotes an order relation, and $\prec$ is the corresponding strict order.

Definition 39. Let $(X, \preceq)$ be a p.o. set.

A *least element* or *minimum* is $y \in X$ such that $y \preceq x$ for all $x \in X$.

A *minimal element* is $y \in X$ such that there is no $z \in X$ with $z \prec y$.

A *greatest element* or *maximum* is $y \in X$ such that $x \preceq y$ for all $x \in X$.

A *maximal element* is $y \in X$ such that there is no $z \in X$ with $y \prec z$.

An *upper bound* for $A \subseteq X$ is $x \in X$ with $a \preceq x$ for all $a \in A$.

A *lower bound* for $A \subseteq X$ is $x \in X$ with $x \preceq a$ for all $a \in A$.

The *least upper bound* or *supremum* of set $A \subseteq X$ is $x \in X$ such that $a \preceq x$ for all $a \in A$ and if $a \preceq y$ for all $a \in A$, then $x \preceq y$. The *greatest lower bound* or *infimum* is defined similarly.

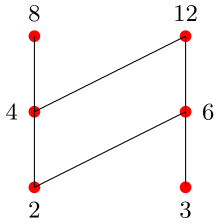
Remark 5.78. The minimum and the maximum in a p.o. set $(X, \preceq)$ (if they exist) are unique. In that case the minimum is the only minimal element, and the maximum is the only maximal element. A p.o. set $(X, \preceq)$ may have several minimal and maximal elements. One can define the minimum, the maximum, minimal and maximal elements of an arbitrary subset $A \subseteq X$. A subset $A \subseteq X$ may have several upper bounds and several lower bounds (if any). The least upper bound of A (if it exists) is unique and is denoted lub A or $\sup A$. The greatest lower bound is also unique (if it exists) and is denoted glb A or $\inf A$.

Example 5.79. $(\mathcal{P}(\{1,2,3\}) \setminus \{\emptyset\}, \subseteq)$ is a p.o. set. There is no minimum, and $\{1\}, \{2\}, \{3\}$ are minimal elements. The maximum is $\{1,2,3\}$. The upper bounds of $A = \{\{1\}, \{2\}\}$ are $\{1,2\}, \{1,2,3\}$ and the supremum of A is $\{1,2\}$. The set A has no lower bounds and no infimum.

Example 5.80. Let $X = \{2,3,4,6,8,12\}$ with the divisibility relation $|$. Find the minimal elements and the maximal elements in the p.o. set $(X, |)$. Find the lower bounds and the upper bounds of $A = \{3,4\} \subseteq X$ (if any). Does $(X, |)$ have a minimum or a maximum?

Solution. The minimal elements are $2, 3$ because there is no $x \in X$ with $x \mid 2$ or $x \mid 3$ and $x \neq 2, x \neq 3$. The maximal elements are $8, 12$ since there is no $y \in X$ other than 8 and 12 such that $8 \mid y$ or $12 \mid y$. The set $A = \{3,4\}$ has no lower bound since there is no $a \in X$ with $a \mid 3$ and $a \mid 4$. The only upper bound of A is 12. There is no minimum or maximum.

A good way to visualize $(X, |)$ is the graph:



Note the position of the minimal elements and of the maximal elements.

Exercise 5.81. Consider the relation $\preceq$ on $\mathbb{N}^2$, where $(x, y) \preceq (x', y')$ iff $x \leq x'$ and $y \leq y'$. Prove that $\preceq$ is a partial order. Find minimal elements. Find a set $A \subseteq \mathbb{N}^2$ such that any two elements of A are incomparable.

Definition 40. Let $(X, \preceq)$ be a p.o. set. If $\{x, y\} \subseteq X$ has a least upper bound, this element is denoted $x \vee y$ (not to be confused with the logic disjunction symbol). Similarly, $x \wedge y$ denotes the greatest lower bound of $\{x, y\}$. We say that a p.o. set $(X, \preceq)$ is a *lattice* if $x \vee y$ and $x \wedge y$ exist for all $x, y \in X$.

Example 5.82. The p.o. set $(\mathcal{P}(X), \subseteq)$ is a lattice with $A \vee B = A \cup B, A \wedge B = A \cap B$ for $A, B \in \mathcal{P}(X)$. The set $(\mathbb{N}, |)$ is a lattice with $a \vee b =$lcm$(a, b), a \wedge b =$gcd(a, b), where lcm denotes the least common multiple, and gcd denotes the greatest common divisor (more about lcm and gcd in the chapter about integers).

Exercise 5.83. Show that $X = \{1, 2, 3, 4, 6, 8, 12, 24\}$ with the divisibility relation is a lattice. How about $(Y, |)$ where $Y = \{2, 3, 4\}$?

Exercise 5.84. Prove that the sets $\mathbb{Z} \times \mathbb{Z}$ and $\mathbb{R} \times \mathbb{R}$ with product order

$$(x_1, x_2) \preceq (y_1, y_2) \text{ whenever } x_1 \leq y_1 \text{ and } x_2 \leq y_2$$

are lattices, but $\mathbb{Z} \times \mathbb{Z}$ and $\mathbb{R} \times \mathbb{R}$ are not totally ordered. If instead we use the *lexicographic* or *dictionary order*,

$$(x_1, x_2) \preceq (y_1, y_2) \text{ if either } x_1 < y_1 \text{ or } x_1 = y_1 \text{ and } x_2 \leq y_2,$$

prove that $\mathbb{Z} \times \mathbb{Z}$ and $\mathbb{R} \times \mathbb{R}$ become totally ordered.

Definition 41. Consider $(X, \preceq)$ and $(X', \preceq')$ two p.o. sets. A function $f : X \to X'$ is called increasing if $x_1 \preceq x_1$ implies $f(x_1) \preceq' f(x_2)$ for all $x_1, x_2 \in X$. An isomorphism of p.o. sets is a function $f : X \to X'$ which has an increasing inverse $f^{-1} : X' \to X$.

Example 5.85. The function $f : \mathbb{R} \to \mathbb{R}, f(x) = x^3$ is increasing. In fact f is an isomorphism of ordered sets, since its inverse $f^{-1} : \mathbb{R} \to \mathbb{R}, f^{-1}(y) = \sqrt[3]{y}$ is also increasing. The function $g : \mathbb{R} \to \mathbb{R}, g(x) = x^2$ is not increasing, but it has an increasing restriction $g_1 : [0, \infty) \to [0, \infty)$.

Example 5.86. Consider the p.o. sets $(\mathcal{P}(\{a, b\}), \subseteq)$ and $(\{1, 2, 3, 6\}, |)$. Then $f : \mathcal{P}(\{a, b\}) \to \{1, 2, 3, 6\}, f(\emptyset) = 1, f(\{a\}) = 2, f(\{b\}) = 3, f(\{a, b\}) = 6$ is an isomorphism of p.o. sets.

Example 5.87. We have seen that $\bar{\mathbb{R}} = \mathbb{R} \cup \{-\infty, \infty\}$, where $\mathbb{R}$ has the usual order and $-\infty < x < \infty$ for all $x \in \mathbb{R}$ is a totally ordered set. In this set, every subset has an upper bound and a lower bound. Indeed, $-\infty$ is a minimum, and ∞ is a maximum. As a consequence, the totally ordered sets $\mathbb{R}$ and $\bar{\mathbb{R}}$ are not isomorphic, since for example $[0, \infty)$ has no upper bound in $\mathbb{R}$.

Definition 42. We say that $(X, \preceq)$ is *well-ordered* if every nonempty subset A of X has a minimum (a lower bound for A belonging to A). This element is also called the first element of A or the smallest element of A.

Remark 5.88. It is easy to see that a well-ordered set $(X, \preceq)$ is totally ordered. Indeed, given $x, y \in X$, the set $\{x, y\}$ has a smallest element, say x. Then $x \preceq y$.

Example 5.89. Any subset of $\mathbb{N}$ (including $\mathbb{N}$ itself) with the natural order is well ordered. We will prove this in the chapter about positive integers, using an axiomatic theory.

Example 5.90. The sets $\mathbb{Z}$ and $\mathbb{R}$ with the usual order are totally ordered, but not well-ordered, since for example $\{..., -3, -2, -1, 0\}$ has no smallest element. Also $\bar{\mathbb{R}}$ is not well ordered.

Example 5.91. Consider $X = \mathbb{N} \cup \{\omega\}$, where $\omega \notin \mathbb{N}$. Consider the natural order on $\mathbb{N}$ and let $n < \omega$ for all $n \in \mathbb{N}$. Then X becomes a well ordered set, not isomorphic to $\mathbb{N}$, since X has a maximum.

Exercise 5.92. Prove that $\mathbb{N} \times \mathbb{N}$ with the lexicographic order,

$$(x_1, x_2) \preceq (y_1, y_2) \text{ if either } x_1 < y_1 \text{ or } x_1 = y_1 \text{ and } x_2 \leq y_2,$$

is well ordered.

Theorem 5.93. *(Principle of induction for well ordered sets) Let $(X, \preceq)$ be well ordered and let $A \subseteq X$ such that for all $x \in X$, whenever $a \prec x$ for all $a \in A$, we have $x \in A$. Then $A = X$.*

Proof. Assume $A \neq X$ and let $B = X \setminus A \neq \emptyset$. Then B has a smallest element, call it b_0. It follows that $a \prec b_0$ for all $a \in A$, so by hypothesis $b_0 \in A$, contradiction. □

Exercise 5.94. Prove that the sets $\mathbb{Z} \times \mathbb{Z}$ and $\mathbb{R} \times \mathbb{R}$ with the *lexicographic order*,

$$(x_1, x_2) \preceq (y_1, y_2) \text{ if either } x_1 < y_1 \text{ or } x_1 = y_1 \text{ and } x_2 \leq y_2,$$

are not well-ordered.

We state without proof

Theorem 5.95. *(Zermelo's well-ordering theorem). Every nonempty set X has an order $\preceq$ such that $(X, \preceq)$ is well-ordered.*

This seems very reasonable for finite sets and even for some countable sets (we already mentioned that $\mathbb{N}$ is well-ordered), but for sets like the interval $(1, \infty)$, it seems entirely unreasonable, and can be proved only using the Axiom of Choice. We know that with the usual order, there is no smallest element in $(1, \infty)$.

Definition 43. A p.o. set $(X, \preceq)$ is *inductively ordered* if every totally ordered subset of X has an upper bound in X.

Example 5.96. Consider X a nonempty set. Then $(\mathcal{P}(X), \subseteq)$ is inductively ordered. Indeed, given a totally ordered family $\{C_i\}_{i\in I}$ of $\mathcal{P}(X)$, we can take the union $C = \bigcup_{i\in I} C_i$, which is an upper bound for $\{C_i\}_{i\in I}$.

Theorem 5.97. *(The Hausdorff maximal principle) Every p.o. set $(X, \preceq)$ has a maximal totally ordered subset.*

A consequence of the Hausdorff maximal principle is

Theorem 5.98. *(Zorn's lemma). Every inductively ordered set X has a maximal element.*

Proof. Indeed, an upper bound for a maximal totally ordered subset of X is a maximal element of X. □

Remark 5.99. In fact, the two results are equivalent. Applying Zorn's lemma to the collection of totally ordered subsets of X, which is partially ordered by inclusion, we can prove the Hausdorff maximal principle.

Zorn's lemma is a very important tool in various parts of Mathematics. For example, it is used to prove the existence of maximal ideals in a commutative ring with identity, the existence of a basis in an arbitrary vector space and the existence of a spanning tree in a graph.

In fact, we have

Theorem 5.100. *The following are equivalent*

(i) The Axiom of choice(in the form: if $\{X_i\}_{i\in I}$ is a nonempty collection of nonempty sets, then $\prod_{i\in I} X_i$ is nonempty).

(ii) Zermelo's well-ordering theorem.

(iii) The Hausdorff maximal principle.

(iv) Zorn's Lemma.

Proof. (partial) We have seen already that (iii) and (iv) are equivalent. We prove now the implication $(iv) \Rightarrow (ii)$. Let $\mathcal{W}$ be the collection of well orderings of subsets of X, and define a partial ordering $\preceq$ on $\mathcal{W}$ as follows. If R_1 and R_2 are well orderings on the subsets $E_1, E_2 \subseteq X$, then $R_1 \preceq R_2$ if $E_1 \subseteq E_2$, R_2 restricted to E_1 agrees with R_1, and if $y \in E_2 \setminus E_1$, then xR_2y for all $x \in E_1$. It is easy to see that $\mathcal{W}$ is not empty and that $(\mathcal{W}, \preceq)$ satisfies the hypotheses of Zorn's lemma. Indeed, if $\mathcal{T} \subseteq \mathcal{W}$ is totally ordered, by taking the union of all sets in $\mathcal{T}$ with the appropriate well ordering, we get an upper bound for $\mathcal{T}$. We deduce that $\mathcal{W}$ has a maximal element (E, R). We must have $E = X$, since if $x_0 \in X \setminus E$, then R can be extended to a well order $\tilde{R}$ on $E \cup \{x_0\}$ by taking $\tilde{R} = R$ on E and $x\tilde{R}x_0$ for all $x \in E$.

For $(ii) \Rightarrow (i)$, let $X = \bigcup_{i\in I} X_i$ and choose a well ordering on X. For $i \in I$, let $f : I \to X$ such that $f(i)$ is the minimal element of X_i. Then $f \in \prod_{i\in I} X_i$.

□

Remark 5.101. We have now in our toolbox these equivalent statements from the previous theorem. We can use either one of them when we need. Not all mathematicians assume the Axiom of choice, but this would limit drastically our horizons in Mathematics.

Definition 44. A directed set (or filtered set) is a preordered set $(X, \preceq)$ (recall that $\preceq$ is reflexive and transitive) such that for any $a, b \in X$ there is $c \in X$ with $a \preceq c$ and $b \preceq c$.

Example 5.102. The ordered set $(\mathbb{N}, |)$ is directed, since given $a, b \in \mathbb{N}$ we can take $c =$lcm(a, b). Let $X = \{-2, 2, 3, 4\}$. Then the preordered set $(X, |)$ is not directed, since the elements $-2, 3$ have no upper bound in X.

Example 5.103. Given a set X, $(\mathcal{P}(X), \subseteq)$ is a directed set, since given $A, B \in \mathcal{P}(X)$, we can take $C = A \cup B$.

Remark 5.104. Note that in a directed set $(X, \preceq)$, any finite subset has an upper bound.

Proof. Let $A \subseteq X$ with n elements. We use induction. For $n = 2$, we have an upper bound by definition. Assume that this is true for subsets with k elements, and let us prove it for $\{x_1, x_2, ..., x_k, x_{k+1}\}$. Consider y an upper bound for $\{x_1, x_2, ..., x_k\}$. By definition, the set $\{y, x_{k+1}\}$ has un upper bound z. By transitivity, we get that z is an upper bound for $\{x_1, x_2, ..., x_k, x_{k+1}\}$. □

Definition 45. A net (or generalized sequence) in a set Y is given by a function $x : (I, \preceq) \to Y$, where $(I, \preceq)$ is a directed set. If $I = \mathbb{N}$ with the usual order, then x is called a sequence in Y. We denote a net by $(x_i)_{i \in I}$, where $x_i = x(i)$ for all $i \in I$. When $I = \mathbb{N}$, we also write $(x_n)_{n \geq 0}$ or just (x_n).

Example 5.105. Let $I = \mathbb{R}$ with the usual order and for $i \in I$ let $x_i = [i - 1, i)$. Then $(x_i)_{i \in I}$ is a generalized sequence in $\mathcal{P}(\mathbb{R})$.

Example 5.106. A constant sequence is $x : I \to Y$ such that $x_i = y_0$ for all $i \in I$ for some fixed element $y_0 \in Y$. Note that we distinguish the constant sequence $(y_0)_{i \in I}$ from the set $\{y_0\}$.

Generalized sequences are used in general topology and in functional analysis.

Chapter 6

Axiomatic theory of positive integers

6.1. Peano axioms and addition

The Positive Integers $1, 2, 3, \ldots$, sometimes called the Counting Numbers or the (nonzero) Natural Numbers, are undoubtedly the oldest numbers known to us. They are the first numbers we learn about in elementary school and their properties and the ways in which we calculate with them are among the most familiar of mathematical notions. Even so, if pressed to actually define them, most of us would find it difficult to come up with an adequate description without resorting to handwaving or merely giving examples. We will say enough about the positive integers through the axioms such that all their basic properties can be proved as theorems. In fact, as you will see, even though the axioms involve no explicit operation, we will be able to define and prove theorems about addition, subtraction, multiplication, division, etc. In the process, you should learn more about what constitutes a valid proof, some useful techniques in theorem proving, and some things to think about when attempting to prove something yourself.

The objects $1, 2, 3, \ldots$ called positive integers relate to the notion of cardinality, a notion defined in a separate chapter. To get a flavor of this, some people associate 1 with the set $\{\emptyset\}$, 2 with the set $\{\emptyset, \{\emptyset\}\}$, 3 with the set $\{\emptyset, \{\emptyset, \{\emptyset\}\}\}$, and in general $n + 1$ with the set $n \cup \{n\}$. The idea is that n represents all sets containing exactly n elements.

We denote here the set of positive integers by $\mathbb{P}$. Some people prefer the notation $\mathbb{N}$, but we will reserve this for $\mathbb{P} \cup \{0\}$. The set of positive integers satisfy the following five axioms, known as the Peano axioms.

Axiom 1. There exists $1 \in \mathbb{P}$.

Axiom 2. For each $n \in \mathbb{P}$, there is an element $s(n) \in \mathbb{P}$, called the successor of n.

Axiom 3. For each $n \in \mathbb{P}$, $s(n) \neq 1$

Axiom 4. If $m, n \in \mathbb{P}$ and $s(m) = s(n)$, then $m = n$.

Axiom 5. If Q is a subset of $\mathbb{P}$ such that $1 \in Q$ and $s(n) \in Q$ whenever $n \in Q$, then $Q = \mathbb{P}$.

The first axiom implies that $\mathbb{P}$ is not empty. Axioms 2,3,4 say that there is a function $s : \mathbb{P} \to \mathbb{P}$ which is one-to-one and 1 is not in the range of s. In fact 1 is the only element not belonging to the range of s. We define 2 as $s(1)$, 3 as $s(2)$, in general $n + 1$ as $s(n)$. We get that $\mathbb{P} = \{1, s(1), s(s(1)), ...\} = \{1, 2, 3, ...\}$. Indeed, $\mathbb{P}$ has no other elements by axiom 5. Later we will add the number 0 to $\mathbb{P}$ to get the set of natural numbers, denoted by $\mathbb{N}$.

Axiom 5 is also called the *Principle of Mathematical Induction.* As we already mentioned in the chapter about proofs, it gives us a method to prove many statements of the form $\forall n\ S(n)$. The basic idea behind its use is as follows. First, realize that whether or not an open sentence $S(n)$ is true always, sometimes, or never, it makes sense to discuss the set of all values of n for which it is true; this "truth set" of the open sentence may consist of all, some, or no integers at all, but it is at least a definite mathematical object which can be investigated. Second, if $Q = \{n : S(n)\}$, then the statements $Q = \mathbb{P}$ and $\forall n \in \mathbb{P}\ S(n)$ are equivalent. Thus, to prove that $S(x)$ is true for all positive integers x, form the set Q of all x for which it is true, establish that the hypotheses of axiom 5 are valid, and conclude that $Q = \mathbb{P}$.

Remark 6.1. There are other sets satisfying the Peano axioms, for example the set $\{1, 3, 5, 7, ...\}$ of odd positive integers with $s(1) = 3, s(3) = 5, s(5) = 7, ...$ It can be proved that any two sets satisfying the Peano axioms are in bijection, and we view them as the same object (we call them isomorphic models).

You may wonder what happens if we drop some of the axioms. Do we still deal with the set of positive integers? For example, if we drop Axiom 3 and allow 1 to be in the range of s, we can take the finite set $\{1, 2, ..., n\}$ such that $s(1) = 2, s(2) = 3, ..., s(n) = 1$. For example, on a usual clock, 12 is followed by 1. This set with this successor function satisfies the other four axioms. It can be proved that Axiom 3 forces $\mathbb{P}$ to be infinite. More about infinite sets in a separate chapter.

How do we know that $\mathbb{P}$ is not too big? If we drop the last axiom, we may consider $A = \mathbb{P} \cup \{\omega\}$, where $\omega \notin \mathbb{P}$ is a new element and we can extend s to A such that $s(\omega) = \omega$. The new set A satisfies the first four axioms, but not the last one (take $Q = \mathbb{P}$ which is a proper subset of A).

Definition 46. We define the operation $+$ on $\mathbb{P}$ called *addition* such that

$$m + 1 = s(m), \quad m + s(k) = s(m + k).$$

In other words, for a fixed m, we need to know how to define $m + 1$, and, once we know $m + k$, we define $m + s(k)$ as $s(m + k)$. Since any positive integer other than 1 is of the form $s(k)$ for some k, we are done. We say that we defined the addition inductively. This way, for each $m, n \in \mathbb{P}$ there is a unique $m + n \in \mathbb{P}$.

Example 6.2. Let us show that $2 + 2 = 4$.

Proof. We give a direct proof. Indeed, $2+2 = 2+s(1)$ (definition of 2) $= s(2+1) = s(s(2))$ (definition of addition) $= s(3)$ (definition of 3) $= 4$ (definition of 4). □

Theorem 6.3. *The addition of positive integers has the properties*

1. $\forall n\ (n+1 \neq n)$.

2. $\forall n\ (n=1) \vee (\exists m(n=m+1))$.

3. $\forall m \forall n \forall p\ [(m+n)+p = m+(n+p)]$ *(addition is associative).*

Proof. 1. This says that for all n, $s(n) \neq n$. This is true for $n=1$, since $1+1=2=s(1)$ can not be equal to 1 by axiom 3. Consider a k such that $s(k) \neq k$. Since the successor function is one-to-one (axiom 4), we get $s(s(k)) \neq s(k)$, or $s(k+1) \neq k+1$. We proved by induction that for all $n \in \mathbb{P}$ we have $s(n) \neq n$.

2. Given $n \in \mathbb{P} \setminus \{1\}$, we know that there is $m \in \mathbb{P}$ with $s(m)=n$, in other words such that $n=m+1$.

3. We fix $m, n \in \mathbb{P}$ and use induction on p. For $p=1$,

$$(m+n)+1 = s(m+n) = m+s(n) = m+(n+1).$$

Assume that $(m+n)+q = m+(n+q)$, and let's prove associativity for $p=s(q)$. We have

$$(m+n)+p = (m+n)+s(q) = s((m+n)+q) = s(m+(n+q)) =$$

$$= m+s(n+q) = m+((n+q)+1) = m+(n+(q+1)) = m+(n+p).$$

□

Lemma 1. $\forall n\ (n+1 = 1+n)$.

Proof. For $n=1$ this is clear. Assume $k+1=1+k$ for a fixed k, and let $n=s(k)$. We have

$$1+n = 1+s(k) = s(1+k) = s(k+1) =$$

$$= k+s(1) = k+(1+1) = (k+1)+1 = s(k)+1 = n+1.$$

□

Theorem 6.4. *The addition is commutative, more precisely* $\forall m \forall n\ (m+n = n+m)$.

Proof. We know this to be true for $n=1$ by the lemma. Assume $m+k=k+m$, and let's prove it for $n=s(k)$. We have

$$m+s(k) = s(m+k) = s(k+m) = k+s(m) =$$

$$= k+(m+1) = k+(1+m) = (k+1)+m = s(k)+m = n+m,$$

using the associativity of addition. □

Theorem 6.5. *The addition of positive integers satisfies the cancellation law.* $\forall m \forall n \forall p\ (m+p = n+p \Rightarrow m=n)$.

Proof. For $p=1$, assuming $m+1=n+1$, we get $s(m)=s(n)$, which implies $m=n$ since s is one-to-one. Assume that $m+k=n+k$ implies $m=n$ for some k, and let's prove that $m+s(k)=n+s(k) \Rightarrow m=n$. Since $m+s(k)=s(m+k)$ and $n+s(k)=s(n+k)$, from $s(m+k)=s(n+k)$ we obtain $m+k=n+k$, hence $m=n$. □

6.2. The natural order relation and subtraction

Definition 47. For $x, y \in \mathbb{P}$, we say that $x < y$ if and only if there exists a positive integer u such that $x + u = y$. Other ways of expressing the relation $x < y$ are: x is less than y, x is smaller than y, or y is greater than x.

Recall that $\mathbb{P} = \{1, s(1), s(s(1)), s(s(s(1))), ...\}$. The relation $x < y$ can be understood like this: in the sequence $1, s(1), s(s(1)), ...$ the number x appears first, and y later. That is, y is obtained by applying s or s composed to s a number of times to x. As a consequence, $1 < 2 < 3 < ...$ and there is no positive integer m such that $x < m$ for all $x \in \mathbb{P}$.

Theorem 6.6. *The relation $<$ is transitive: $(x < y) \wedge (y < z) \Rightarrow x < z$.*

Proof. Since $x < y$ and $y < z$, there are u, v with $y = x + u$ and $z = y + v$. Then

$$z = y + v = (x + u) + v = x + (u + v),$$

hence $x < z$. □

Lemma 2. For $x, y \in \mathbb{P}$, we have

1. $x = 1$ or $1 < x$.
2. $x = y$ or $x < y$ or $y < x$.
3. $\neg(x < x)$.

Proof. 1. If $x \neq 1$, we have seen that $x = s(k)$ for some k, hence $x = k + 1 = 1 + k$ and $1 < x$.

2. If $x \neq y$, suppose that in the sequence $1, s(1), s(s(1)), ...$ the number x appears first. This means that there is u such that $y = x + u$ and $x < y$. If y appears first, then $y < x$.

3. If $x < x$, we get that $x = x + u$ for some $u \in \mathbb{P}$, contradiction. □

Corollary 1. (law of trichotomy) For all positive integers x and y, exactly one of the following three statements is true:

a. $x = y$

b. $x < y$,

c. $y < x$.

Remark 6.7. We proved above that the relation$<$ is transitive, hence it is a strict order relation. If we define $x \leq y$ if $x < y$ or $x = y$, then it is easy to prove that $\leq$ is reflexive, antisymmetric and transitive, hence an order relation.

Theorem 6.8. *For $x, y, z \in \mathbb{P}$ we have $x < y \Leftrightarrow x + z < y + z$.*

Proof. If $x < y$, there is u with $x + u = y$. Adding z we get $(x + u) + z = y + z$ or $(x + z) + u = y + z$, hence $x + z < y + z$. The converse uses cancellation. □

Theorem 6.9. *For $x, y, z \in \mathbb{P}$ we have $x + y < z \Rightarrow (x < z) \wedge (y < z)$.*

Proof. Since $x + y < z$, we get $z = x + y + u$ for some u. In particular, $z = x + (y + u)$, hence $x < z$ and $z = y + (x + u)$, hence $y < z$. □

Theorem 6.10. *For $x, y, z, u \in \mathbb{P}$ we have $(x < z) \wedge (y < u) \Rightarrow x + y < z + u$.*

Proof. Since $x < z$ and $y < u$ we get $z = x + v$ and $u = y + w$ for some v, w. Then $z + u = x + v + y + w = (x + y) + (v + w)$, therefore $x + y < z + u$. □

Theorem 6.11. *For $x, y, z, u \in \mathbb{P}$ we have $x + y < z + u \Rightarrow (x < z) \vee (y < u)$.*

Proof. From $x + y < z + u$ we get $z + u = x + y + v$ for some v. If $x < z$, we are done. Assume $z \leq x$. Then $x = z$ or $x = z + w$ for some w. In the first case, by cancellation $u = y + v$, so $y < u$. In the second case, $z + u = z + w + y + v$ and $u = y + (v + w)$, so $y < u$ as well. □

Exercise 6.12. Prove the following properties of the relation $\leq$ for $x, y, z \in \mathbb{P}$.

a) $x \leq y \Leftrightarrow x + z \leq y + z$.

b) $(x \leq y) \vee (y \leq x)$.

c) $y \leq x \Leftrightarrow y < x + 1$.

It is sometimes convenient to use the opposite of $<$, the greater than relation, denoted $>$. This is defined symbolically by $x > y \Leftrightarrow y < x$. Clearly, any statement using $<$ has a natural counterpart using $>$ and all the theorems about *less than* can be converted into theorems about *greater than*. We can also define $x \geq y$ if $x = y$ or $x > y$. The relation $\geq$ is also reflexive, antisymmetric and transitive, so it is an order relation on $\mathbb{P}$.

Theorem 6.13. *(Archimedean property): For all $m, n \in \mathbb{P}$ $\exists\, k \in \mathbb{P}$ with $m < kn$.*

Proof. If $m < n$, we can take $k = 1$. For $m = n$, $k = 2$ works. For $n < m$ we can take $k = m + 1$ since $m < mn + n$. □

Theorem 6.14. *(Well-ordering Principle) If A is a non-empty subset of $\mathbb{P}$, then A has a smallest element. More specifically, there is an element $x \in A$ such that $x \leq y$ for all $y \in A$. The smallest element is unique.*

Proof. Suppose there is a subset $A \neq \emptyset$ with no smallest element. We shall prove by induction on n that $x \in A \Rightarrow x \geq n$. For $n = 1$ this is obvious. Assume that the property holds for some $k \geq 1$. Then we can not have $k \in A$, since this would be the smallest element. Hence $k \notin A$ and every $x \in A$ has the property that $x \geq k + 1$. By induction we got $x \in A \Rightarrow x \geq n$ for all $n \geq 1$. Since A is not empty, let $m \in A$ be some element. Using the inequality for $n = m + 1$ we get $m \geq m + 1$, contradiction. It remains that all nonempty subsets have a smallest element.

Uniqueness follows from the fact that if $a, b \in A$ are both smallest elements, then $a \leq b$ and $b \leq a$ implies $a = b$. □

Remark 6.15. The well-ordering Principle says that $\mathbb{P}$ with the natural order is a well-ordered set. This is not to be confused with Zermelo's well-ordering Theorem, equivalent with the Axiom of choice and with Zorn's Lemma discussed in the previous chapter. Warning: some authors call Zermelo's theorem the well-ordering Principle.

Theorem 6.16. *The well-ordering Principle implies the Principle of Mathematical induction.*

Proof. Indeed, assume that for each positive integer n, a statement $P(n)$ is given. We assume that $P(1)$ is true, and that $P(k) \Rightarrow P(k+1)$. Let's prove that $P(n)$ is true for all n. If not, let $Q \neq \emptyset$ be the subset of $\mathbb{P}$ consisting of those m for which $P(m)$ is false. By the Well-ordering Principle, Q contains a smallest element d. Since $P(1)$ is true, we must have $d > 1$. But then there is e with $d = s(e) = e+1$ and e cannot be in Q, so $P(e)$ must be true. From hypothesis, we get $P(e+1) = P(d)$ true, contradiction. Therefore Q must be empty and $P(n)$ is true for all n. □

Remark 6.17. For any $x, y \in \mathbb{P}$ with $x < y$ there exists a unique $z \in \mathbb{P}$ such that $x + z = y$.

Proof. Recall that since $x < y$, there is z with $x + z = y$. If z' also satisfies $x + z' = y$, we get $x + z = x + z'$, so $z = z'$ by cancellation. □

Definition 48. Suppose that $x, y \in \mathbb{P}$ with $x < y$. We define the subtraction operation and write $y - x$ to denote the unique $z \in \mathbb{P}$ such that $x + z = y$. We say that we have subtracted x from y. In other words, $y - x$ stands for the positive integer such that $x + (y - x) = y$.

Example 6.18. Let's prove that

a. $4 - 2 = 2$.

b. $(x + y) - x = y$.

c. $[x + (y + z)] - z = x + y$.

d. $x + y < z \Rightarrow y < z - x$.

e. $(x < y) \wedge (y < z) \Rightarrow y - x < z$.

Proof. Indeed, for a we have seen that $2+2 = 4$. Equation b follows since $x+y > x$ and $x + y = x + y$. Part c is using associativity of addition. For d, notice that $z = x + y + u$ and therefore $z - x = y + u$. For e, let $y = x + u, z = y + v$ for some $u, v \in \mathbb{P}$. Then $u = y - x$ and $z = x + u + v$, in particular $u < z$. □

Theorem 6.19. *For $x, y, z \in \mathbb{P}$ we have*

1. $z < y \Rightarrow (x + y) - z = x + (y - z)$.

2. $x + y < z \Rightarrow z - (x + y) = (z - x) - y$.

3. $(x < y) \wedge (y < z) \Rightarrow z - (y - x) = (z - y) + x$.

4. $(x < y) \wedge (z < x) \Rightarrow x - z < y - z$.

5. $(x < y) \wedge (y < z) \Rightarrow z - y < z - x$.

Proof. 1. Since $z < y$, we have $z + (y - z) = y$. Adding x we get $(z + (y - z)) + x = y + x$ or $((y - z) + x) + z = x + y$, hence $(y - z) + x = (x + y) - z$.

2. Note that $x + y < z$ implies $x < z$ and $y < z - x$. Using part 1 and the fact that $(x+y) - x = y$, we get $(x+y) + [(z-x) - y] = (x+y+z-x) - y = (y+z) - y = z$.

3. We have $[(z - y) + x] + (y - x) = (z - y) + [x + (y - x)] = (z - y) + y = z$, so $(z - y) + x = z - (y - x)$.

4. Since $z < x < y$, we get $z < y$. We have $y - z = (y - x) + (x - z)$, hence $x - z < y - z$.

5. Again $x < z$, and $z - x = (z - y) + (y - x)$, so $z - y < z - x$. □

6.3. Multiplication and divisibility

Definition 49. We define inductively the operation of *multiplication* (denoted by a dot $\cdot$, which sometimes is omitted) on $\mathbb{P}$ as follows:

$x \cdot 1 = x$ and $x \cdot s(y) = x \cdot (y+1) = x \cdot y + x$.

Theorem 6.20. *Multiplication on $\mathbb{P}$ has properties*

1. $x \cdot (y+z) = x \cdot y + x \cdot z$ *and* $(x+y) \cdot z = x \cdot z + y \cdot z$ *(distributivity).*
2. $x \cdot y = y \cdot x$ *(commutativity).*
3. $x \cdot (y \cdot z) = (x \cdot y) \cdot z$ *(associativity).*
4. $x < y \Rightarrow x \cdot z < y \cdot z$.
5. $x \cdot z = y \cdot z \Rightarrow x = y$ *(cancellation).*
6. $x \cdot z < y \cdot z \Rightarrow x < y$.
7. $x < y \Rightarrow z \cdot (x - y) = z \cdot y - z \cdot x$.
8. $x < y \wedge u < v \Rightarrow x \cdot u < y \cdot v$.
9. $y \neq 1 \Rightarrow x < x \cdot y$.
10. $x \leq x \cdot y$.

Proof. 1. By induction on z. For $z = 1$,

$$x \cdot (y+1) = x \cdot y + x = x \cdot y + x \cdot 1.$$

Assume $x \cdot (y+k) = x \cdot y + x \cdot k$. Then

$$x \cdot (y + (k+1)) = x \cdot [(y+k)+1] = x \cdot (y+k) + x =$$
$$= x \cdot y + x \cdot k + x \cdot 1 = x \cdot y + x \cdot (k+1).$$

The other equality is proved similarly.

2. First we prove by induction on x that $1 \cdot x = x$. This is certainly true for $x = 1$. Assume $1 \cdot k = k$. Then

$$1 \cdot (k+1) = 1 \cdot k + 1 \cdot 1 = k + 1.$$

Now we use induction on y to show that $x \cdot y = y \cdot x$. This is true for $y = 1$ since $x \cdot 1 = x = 1 \cdot x$. Assume $x \cdot k = k \cdot x$. Then

$$x \cdot (k+1) = x \cdot k + x = k \cdot x + x = (k+1) \cdot x.$$

3. By induction on z. We have

$$x \cdot (y \cdot 1) = x \cdot y = (x \cdot y) \cdot 1.$$

Assume $x \cdot (y \cdot k) = (x \cdot y) \cdot k$. Then

$$x \cdot (y \cdot (k+1)) = x \cdot (y \cdot k + y) = x \cdot (y \cdot k) + x \cdot y =$$
$$= (x \cdot y) \cdot k + x \cdot y = (x \cdot y) \cdot (k+1).$$

4. For $z = 1$ it is true: $x < y \Rightarrow x < y$. Assume that $x < y \Rightarrow x \cdot k < y \cdot k$ for some k, and let's prove it for $k+1$. By adding the inequalities $x < y$ and $x \cdot k < y \cdot k$ we get $x \cdot (k+1) < y \cdot (k+1)$.

5. We prove the contrapositive: $x \neq y \Rightarrow x \cdot z \neq y \cdot z$. By trichotomy, if $x \neq y$, there are two possibilities: $x < y$ or $x > y$. In the first case we get $x \cdot z < y \cdot z$ and in the second case $x \cdot z > y \cdot z$, hence $x \cdot z \neq y \cdot z$.

We leave the other properties as exercise. □

Definition 50. Given $x, y \in \mathbb{P}$, we say that x *divides* y, x is a *factor* or *divisor* of y or y is a *multiple* of x if and only if $\exists u$ such that $x \cdot u = y$. We write this symbolically as $x \mid y$, and we obtain the *divisibility* relation on $\mathbb{P}$.

Theorem 6.21. *We have*

1. $(x \mid y) \wedge (y \mid z) \Rightarrow x \mid z$ *(transitivity).*
2. $(x \mid y) \wedge (y \mid x) \Rightarrow x = y$ *(antisymmetry).*
3. $x \mid y \Rightarrow x \leq y$.
4. $(1 \mid x) \wedge (x \mid x)$.
5. $x \mid y \Leftrightarrow x \cdot z \mid y \cdot z$.
6. $(x \mid y) \wedge (x \mid z) \Rightarrow x \mid (y + z)$.
7. $(x \mid y) \wedge (x \mid z) \wedge (y < z) \Rightarrow x \mid (z - y)$.

Proof. 1. We have $y = x \cdot u$ and $z = y \cdot v$ for some u, v. It follows that $z = x \cdot (uv)$, hence $x \mid z$.

2. We have $y = x \cdot u$ and $x = y \cdot v$, hence $y = y \cdot (uv)$. It follows that $uv = 1$, so $u = v = 1$ and $x = y$.

3. Since $y = x \cdot u$ for some u and $x \leq x \cdot u$, we get $x \leq y$.

4. We have $x = 1 \cdot x = x \cdot 1$.

5. "$\Rightarrow$" Suppose $x \mid y$. Then there exists a positive integer u such that $x \cdot u = y$. Multiplying by z we get $(x \cdot u) \cdot z = y \cdot z$. Using associativity and commutativity on the left side, we can write the equation in the form $(x \cdot z) \cdot u = y \cdot z$. Thus by Definition 50, $x \cdot z \mid y \cdot z$.

"$\Leftarrow$" If $x \cdot z \mid y \cdot z$, then for some u, $(x \cdot z) \cdot u = y \cdot z$. As above, this can be rewritten as $(x \cdot u) \cdot z = y \cdot z$, and by multiplicative cancellation, $x \cdot u = y$. Thus $x \mid y$.

We leave parts 6 and 7 as exercises. □

Corollary 2. Divisibility is an order relation on $\mathbb{P}$.

Proof. Indeed, it is reflexive, antisymmetric and transitive. □

Remark 6.22. Unlike the relation $\leq$, the order relation $\mid$ is not a total order. For example $2 \nmid 3$ and $3 \nmid 2$, so not any two elements are comparable.

Recall that given $x, y \in \mathbb{P}$ with $y \mid x$, there exists a unique $u \in \mathbb{P}$ such that $x = y \cdot u$. Indeed, if $x = y \cdot u = y \cdot v$, we get $u = v$ by part 4 in theorem 6.20.

Definition 51. If $y \mid x$, then the unique u such that $y \cdot u = x$ is denoted by $x \div y$ and is called the *quotient* of x by y. This defines the *division* operation for selected positive integers. Later we will also use x/y or $\dfrac{x}{y}$ for $x \div y$. Note that:

$y \mid x \Rightarrow y \cdot (x \div y) = x$ and $y \cdot u = x \Rightarrow u = x \div y$.

Theorem 6.23. *The division operation has properties*

1. $(y \mid x) \wedge (z \mid y) \Rightarrow (y \div z) \mid (x \div z)$.
2. $z \mid y \Rightarrow (x \cdot y) \div z = x \cdot (y \div z)$.
3. $(y \mid x) \wedge (x \mid z) \Rightarrow (z \div x) \mid (z \div y)$.
4. $x \cdot y \mid z \Rightarrow z \div (x \cdot y) = (z \div x) \div y$.
5. $(x \mid y) \wedge (x \mid z) \Rightarrow (y + z) \div x = (y \div x) + (z \div x)$.
6. $(x \mid y) \wedge (x \mid z) \wedge (z < y) \Rightarrow (y - z) \div x = (y \div x) - (z \div x)$.

Proof. 1. We have $x = y \cdot u$ and $y = z \cdot v$ for some u, v, so $x = z \cdot uv$. Moreover, $y \div z = v$ and $x \div z = uv$, hence $(y \div z) \mid (x \div z)$.

2. Since $z \mid y$, we have $y = zu$ for some u, hence $y \div z = u$. We get $xy = xzu$ and $(x \cdot y) \div z = x \cdot u$.

We leave the other parts as exercise. □

6.4. Natural numbers

The set $\mathbb{N} = \mathbb{P} \cup \{0\}$ of natural numbers satisfies the following axioms:

Axiom 1. There exists an element $0 \in \mathbb{N}$.

Axiom 2. For each $n \in \mathbb{N}$, there is an element $s(n) \in \mathbb{N}$, called the successor of n.

Axiom 3. For each $n \in \mathbb{N}$ we have $s(n) \neq 0$.

Axiom 4. If $m, n \in \mathbb{N}$ and $s(m) = s(n)$, then $m = n$.

Axiom 5. If A is a subset of $\mathbb{N}$ such that $0 \in A$ and $s(n) \in A$ whenever $n \in A$, then $A = \mathbb{N}$.

The number 0 was discovered later, and it could be thought as the number of elements in the empty set. Axiom 5 implies the Principle of Mathematical Induction for $\mathbb{N}$: If $P(n)$ is a statement for each $n \in \mathbb{N}$ and we prove

1. $P(0)$ true
2. $P(k)$ true implies $P(k+1)$ true for all $k \geq 0$,

then $P(n)$ is true for all $n \in \mathbb{N}$.

Example 6.24. Let us prove by induction that a set with n elements has 2^n subsets.

Proof. The empty set $\emptyset$ has only one subset, namely itself. So the property holds for $n = 0$ since $2^0 = 1$. Assume that any set X with k elements has 2^k subsets. Let Y be a set with $k+1$ elements. We can write $Y = X \cup \{y\}$ where X has k elements and $y \notin X$. The subsets of Y are of two kinds: subsets which are included in X (there are 2^k of these) and subsets which contain y. The last type of subsets are of the form $A \cup \{y\}$ where $A \subseteq X$, hence a total of another 2^k. All together there are $2^k + 2^k = 2^{k+1}$ subsets of Y and we are done. □

Exercise 6.25. Prove that the set $\{0, 2, 4, 6, ...\}$ of even natural numbers is another set satisfying the Peano axioms for $\mathbb{N}$, defining an appropriate successor function.

Exercise 6.26. For $n \in \mathbb{N}$, define the set of descendants $D(n)$ as the smallest subset of $\mathbb{N}$ such that $n \in D(n)$ and it is closed under the successor function: $m \in D(n) \Rightarrow s(m) \in D(n)$. Prove the following properties:

1. $D(n) = \{n\} \cup D(s(n))$.

2. $D(s(n)) \subseteq s(D(n))$.

3. $n \notin D(s(n))$.

4. $D(m) = D(n) \Rightarrow m = n$.

5. If $\emptyset \neq A \subseteq \mathbb{N}$ and A is closed under s, in the sense that $s(A) \subseteq A$, then there is a unique $k \in \mathbb{N}$ such that $A = D(k)$.

6. For $m, n \in \mathbb{N}, m \leq n \Leftrightarrow n \in D(m)$.

We can extend the addition and multiplication operations to the set of natural numbers, with the new rules $x + 0 = x$, $x \cdot 0 = 0$. When we define divisibility, we exclude 0 as a divisor.

We list the major properties of the natural numbers, especially those that we will use later when we study the integers. All the proofs are similar to the ones for positive integers.

Theorem 6.27. *For the set $\mathbb{N}$ of natural numbers*

1) Addition and multiplication are commutative and associative.

2) Multiplication is distributive with respect with addition.

3) We have cancelation properties: $x+y = x+z \Rightarrow y = z$ and $(x \cdot y = x \cdot z \wedge x \neq 0) \Rightarrow y = z$.

4) There is a natural order defined by $x < y \Leftrightarrow \exists u \in \mathbb{N} \setminus \{0\}$ such that $x+u = y$ and we define $x \leq y \Leftrightarrow (x < y) \vee (x = y)$.

5) The trichotomy property holds: $\forall x, y \in \mathbb{N}$, exactly one of the following is true: $x < y$, $x = y$, or $y < x$.

6) We have the Archimedean property: $\forall m, n \in \mathbb{N}$ with $n \neq 0$ there exists $k \in \mathbb{P}$ with $m < kn$.

7) We have $x < y \Leftrightarrow x + z < y + z$ for all $z \in \mathbb{N}$ and if $z \neq 0$, then $x < y \Leftrightarrow xz < yz$.

8) The well-ordering Principle is: If $A \subseteq \mathbb{N}$, $A \neq \emptyset$, then A contains a unique smallest element.

Definition 52. For $x \in \mathbb{P}$ and $y \in \mathbb{N}$ we define the *power* x^y inductively by: $x^0 = 1$, $x^{y+1} = x^y \cdot x$. The number x is called the *base* and y is called the *exponent.*

Exercise 6.28. Prove that for $x \in \mathbb{P}$ and $y, z \in \mathbb{N}$,

a. $x^{y+z} = x^y \cdot x^z$.

b. $x^{yz} = (x^y)^z$.

Definition 53. For $n \in \mathbb{N}$, the factorial function $n!$ is defined by $0! = 1$ and $(n+1)! = (n+1) \cdot n!$.

Note that $1! = 1, 2! = 2, 3! = 6, 4! = 24$, etc. and for $m \geq 1$ we have $m \leq n \Rightarrow m \mid n!$.

Example 6.29. Show by induction that the sum of the cubes of three consecutive natural numbers is divisible by 9.

Proof. Indeed, $0^3 + 1^3 + 2^3 = 9$ which is divisible by 9. Assume

$$(k-1)^3 + k^3 + (k+1)^3 = 9m$$

for some $k, m \geq 1$ and let us prove that $k^3 + (k+1)^3 + (k+2)^3$ is a multiple of 9. Since

$$(k-1)^3 = k^3 - 3k^2 + 3k - 1 \text{ and } (k+2)^3 = k^3 + 6k^2 + 12k + 8,$$

we get

$$k^3 + (k+1)^3 + (k+2)^3 = 9m + 9k^2 + 3k + 9,$$

which is a multiple of 9. □

Example 6.30. For $n \geq 1$ prove that

$$1 + \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{3}} + \cdots + \frac{1}{\sqrt{n}} < 2\sqrt{n}.$$

Proof. For $n = 1$ the inequality becomes $1 < 2$, which is true. Assume

$$1 + \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{3}} + \cdots + \frac{1}{\sqrt{k}} < 2\sqrt{k}$$

for some $k \geq 1$ and let's prove the inequality for $k+1$. We have

$$1 + \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{3}} + \cdots + \frac{1}{\sqrt{k}} + \frac{1}{\sqrt{k+1}} < 2\sqrt{k} + \frac{1}{\sqrt{k+1}} = \frac{2\sqrt{k^2+k}+1}{\sqrt{k+1}} < 2\sqrt{k+1}$$

because $2\sqrt{k^2+k} < 2k+1$ and we are done. □

Exercise 6.31. Prove by induction that for $n \geq 1$

$$2 \cdot 6 \cdot 10 \cdot \ldots \cdot (4n-2) = \frac{(2n)!}{n!}.$$

6.5. Other forms of induction

Remark 6.32. (Generalized induction) Consider $k_0 \in \mathbb{N}$ and for each $n \geq k_0$ a statement $P(n)$. To prove that $P(n)$ is true for all $n \geq k_0$ it suffices to check two steps

1. $P(k_0)$ is true
2. For each integer $k \geq k_0$, $P(k)$ true implies $P(k+1)$ true.

Example 6.33. For any $n \geq 2$ prove that

$$\frac{1}{n+1} + \frac{1}{n+2} + \cdots + \frac{1}{2n} \geq \frac{7}{12}.$$

Proof. For $n = k_0 = 2$ we have $\frac{1}{3} + \frac{1}{4} = \frac{7}{12}$, so the statement is true. It is easy to check that the inequality fails for $n = 1$. Assume

$$\frac{1}{k+1} + \frac{1}{k+2} + \cdots + \frac{1}{2k} \geq \frac{7}{12}$$

for some $k \geq 2$ and let's prove the inequality for its successor $k+1$. We have

$$\frac{1}{k+1+1} + \frac{1}{k+1+2} + \cdots + \frac{1}{2k} + \frac{1}{2k+1} + \frac{1}{2k+2} =$$

$$= \left(\frac{1}{k+1} + \frac{1}{k+2} + \cdots + \frac{1}{2k}\right) - \frac{1}{k+1} + \frac{1}{2k+1} + \frac{1}{2k+2}$$

and it suffices to notice that

$$-\frac{1}{k+1} + \frac{1}{2k+1} + \frac{1}{2k+2} = \frac{-2(2k+1)+(2k+2)+(2k+1)}{(2k+1)(2k+2)} =$$

$$= \frac{1}{(2k+1)(2k+2)} > 0.$$

□

Example 6.34. Show that $n^2 \leq 2^n$ for all $n \geq 4$.

Proof. Here $k_0 = 4$. Note that $3^2 = 9 > 2^3 = 8$, so there is a good reason to take $k_0 = 4$. For $n = 4$ the inequality becomes $4^2 = 16 \leq 2^4$ and the statement is true. Assume $k^2 \leq 2^k$ for some $k \geq 4$. We want to show that $(k+1)^2 \leq 2^{k+1}$. Since $2^{k+1} = 2 \cdot 2^k$, we multiply the inequality $k^2 \leq 2^k$ by 2 and we get $2k^2 \leq 2^{k+1}$. This is not yet what we wanted, but if we show that $(k+1)^2 \leq 2k^2$ for $k \geq 4$, we are done by transitivity. This last inequality is equivalent to $k^2 + 2k + 1 \leq 2k^2$ or $k^2 - 2k \geq 1$. If we write this as $k(k-2) \geq 1$, we see that it is true, since $k \geq 4$. It follows that $n^2 \leq 2^n$ for all $n \geq 4$. □

Exercise 6.35. For $n \geq 10$ prove by generalized induction that $2^n \geq n^3$.

Theorem 6.36. *(Strong induction or Complete induction) If A is a subset of $\mathbb{N}$ such that*

1. *$0 \in A$ and*
2. *$\forall n \geq 1$, $\{0,1,2,...,n\} \subseteq A \Rightarrow n+1 \in A$.*

Then $A = \mathbb{N}$.

Proof. Consider the statement $0,1,2,...,n \in A$, denoted $P(n)$. Since $0 \in A$, $P(0)$ is true. Assume $P(k)$ to be true, so $0,1,2,...,k \in A$. From part 2. we get that $k+1 \in A$, hence $P(k+1)$ is true. By induction, it follows that $P(n)$ is true for all n, in particular $A = \mathbb{N}$. □

Note that in fact the strong induction implies the usual induction, hence they are equivalent. Using strong induction and generalized induction, we get

Corollary 3. If A is a subset of $\mathbb{N}$ such that $k_0 \in A$ and $(m \leq n \Rightarrow m \in A) \Rightarrow n+1 \in A$, then $A = \{k_0, k_0+1, ...\}$.

Definition 54. A positive integer x is a prime if and only if $x \neq 1$ and $y \mid x$ implies $(y = 1) \vee (y = x)$.

Theorem 6.37. *1. A positive integer x is prime if and only if $x \neq 1$ and*

$$\forall r \forall s (x = r \cdot s \Rightarrow (r = 1) \vee (r = x)).$$

2. If $y \neq 1$, then there is a prime p such that $p \mid y$.

Proof. The first part follows directly from the definition. For part 2 we use complete induction. If $y = 2$, then 2 is a prime and $2 \mid y$. Assume the statement to be true for $2, 3, ..., y$ and let's prove it for $y + 1$. If $y + 1$ is prime, we are done. If not, then it has a divisor $2 \leq d \leq y$. Since d has a prime divisor, it follows that $y + 1$ also has a prime divisor.

□

It is worth noting that, in the set of positive integers, a prime is a number which has exactly two divisors: 1 and itself. However, in the larger set $\mathbb{Z}$ consisting of all integers, we will see that a prime is a number with exactly four divisors.

Theorem 6.38. *(Fundamental theorem of arithmetic) Each positive integer $n \geq 2$ is either a prime or is a product of primes.*

Proof. The basis step is true, since 2 is a prime. Suppose that the integers $2, 3, ..., k$ are either primes or product of primes, and let's prove that $k + 1$ also has this property. If it happens that $k+1$ is a prime, we are done. If not, then $k+1 = a \cdot b$, where $2 \leq a, b \leq k$. By hypothesis, both a and b are either primes or product of primes. It follows that $k + 1 = a \cdot b$ is a product of primes as well, and we are done. □

Exercise 6.39. Suppose $u_0 = 2, u_1 = 3$ and $u_{n+1} = 3u_n - 2u_{n-1}$ for all $n \geq 1$. Prove by strong induction that $u_n = 2^n + 1$.

Exercise 6.40. Prove that any positive integer can be written as a product of an odd integer and a power of 2.

Exercise 6.41. Let B be a set with $n \geq 3$ elements. Prove that the number of subsets with three elements is $n(n-1)(n-2)/3!$.

Theorem 6.42. **(Induction with bigger steps) Consider a statement $P(n)$ for each $n \geq k_0$. Suppose*

1. $P(k_0), P(k_0 + 1), ...P(k_0 + k_1 - 1)$ are true for a fixed integer $k_1 \geq 1$ called step;

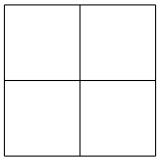
2. $P(k)$ true implies $P(k + k_1)$ true for all $k \geq k_0$.

Then $P(n)$ is true for all $n \geq k_0$.

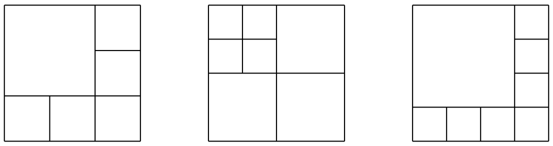
Proof. Indeed, by the division algorithm (see next chapter for a proof), any integer $n \geq k_1$ is of the form $n = qk_1 + r$ where $q \geq 1$ and $0 \leq r \leq k_1 - 1$. □

Example 6.43. For $n \geq 6$, any square can be partitioned into n squares using segments parallel with its sides.

Proof. Obviously a square can be partitioned into 4 equal squares using segments through the midpoints of the sides.



We prove now that we can partitioned a square into $6, 7$ or 8 squares, and then we will prove the induction step from k to $k+3$. Here $k_0 = 6$ and $k_1 = 3$. Indeed, the following picture illustrates the cases $n = 6, 7$ and 8:



Suppose we know how to divide a square into k squares for $k \geq 6$. Take one of the small squares and divide it into four squares. This way, we get a partition of the initial square into $k+3$ squares. □

Exercise 6.44. *Prove that any cube can be partitioned into $n \geq 58$ cubes using planes parallel with its faces. (Hint: use the fact that a cube can be partitioned into 8 cubes and into 27 cubes to verify the statement for $58, 59, ..., 64$ and then use induction with step 7).

Chapter 7

The construction of integers

The invention or discovery of the set of integers $\mathbb{Z} = \{-3, -2, -1, 0, 1, 2, 3, ...\}$ was based on pragmatic concerns. Specifically, there were equations, such as $x + 6 = 2$, which mathematicians could not solve using the natural numbers, but which cried out for solution. As a result, a new set of numbers was developed. This set, referred to as the set of integers, was initially considered by many as, at best, a necessary evil. Negative integers were relegated to second class status and used only when absolutely necessary. Ultimately, however, their usefulness could not be denied and they gradually gained acceptance over the course of the years.

In these more enlightened times, there are lots of ways to model the idea of a negative integer, so that most people can tie the concept down to something more or less concrete. For example, a football buff's attention can be directed towards the idea of a fullback gaining or losing yardage; the accountant type can think in terms of owing money or being owed; the game player can consider the difference between having points or being in the hole (negative numbers often make an appearance on Jeopardy!); and the geometrically inclined individual can perceive the difference between motion to the right and motion to the left. Also, the weather man uses positive and negative temperatures.

It is possible to introduce the concept of integer by announcing that we are inventing a new kind of number, denoted by ^{-}n, and specifying how such a number will interact with the already known natural numbers. This can be a bit unwieldy, so we prefer a different approach.

Our introduction to the theory of integers is based on the idea of using pairs of natural numbers to represent integers. Intuitively, the first component of a pair will describe how much plus stuff is involved, while the second component will count the number of minuses. Thus, when we write the pair $\langle 5, 2\rangle$, we will think of the net result of combining 5 pluses with 2 minuses, which of course is 3 pluses. Likewise $\langle 3, 8\rangle$ will be thought of as 3 pluses and 8 minuses together, which is equivalent to

5 minuses. Notice that these thoughts entail our regarding of the pairs $\langle 7,9\rangle$, $\langle 0,2\rangle$, and $\langle 37,39\rangle$ as representing the same integer.

To make all this precise, we will introduce an equivalence relation on the set $\mathbb{N}\times\mathbb{N}$ of ordered pairs of natural numbers and define an integer to be one of the equivalence classes determined by this relation. In addition, we will define the addition, multiplication, subtraction and division operations. We will extend the usual order relation $\leq$ from $\mathbb{N}$ to $\mathbb{Z}$. We will then proceed to prove divisibility properties of integers from the new definitions.

7.1. Definition and operations

We begin by defining the basic relation between ordered pairs of natural numbers that will in effect determine when the pairs really represent the same integer. In contrast with our previous practice, we will not use a letter to stand for the relation, but will denote it by the symbol $\sim$.

Definition 7.1. If $\langle a,b\rangle, \langle c,d\rangle \in \mathbb{N}\times\mathbb{N}$, then $\langle a,b\rangle \sim \langle c,d\rangle$ iff $a+d=b+c$.

Notice that the objects that are related are themselves ordered pairs. The elements of the actual relation are thus pairs whose components are also ordered pairs. An actual element of the relation $\sim$ on $\mathbb{N}\times\mathbb{N}$ will have the form $\langle\langle a,b\rangle,\langle c,d\rangle\rangle$, but since we will generally utilize the xRy notation, this symbolic complexity will not be troublesome.

As usual, the definition can be used in two distinct ways. First, if we know that $\langle a,b\rangle \sim \langle c,d\rangle$, then we can immediately assert that $a+d=b+c$. If the hypothesis of a theorem is $\langle 6,b\rangle \sim \langle c,12\rangle$, then an immediate conclusion is $6+12=b+c$. If you know that $\langle 4a,a\rangle \sim \langle 10,4\rangle$, then you also have $4a+4=a+10$, so $a=2$.

Second, whenever you see the expression $a+d=b+c$, you may immediately write the equivalent statement $\langle a,b\rangle \sim \langle c,d\rangle$. Thus, since $5+4=2+7$, we have $\langle 5,2\rangle \sim \langle 7,4\rangle$. Also, if $2a+1=4b+3$, then $\langle 2a,3\rangle \sim \langle 4b,1\rangle$. These ideas figure prominently in the proofs of the next few theorems.

Theorem 7.2. *The relation $\sim$ is an equivalence relation on $\mathbb{N}\times\mathbb{N}$.*

Proof. We must separately verify each of the three conditions that appear in the definition of equivalence relation.

1) Suppose $\langle a,b\rangle \in \mathbb{N}\times\mathbb{N}$. Since $a+b=b+a$, it follows that $\langle a,b\rangle \sim \langle a,b\rangle$. Thus $\sim$ is reflexive.

2) Suppose $\langle a,b\rangle \sim \langle c,d\rangle$. Then $a+d=b+c$. Hence, by the commutative property of addition in $\mathbb{N}$, together with the symmetry property of equality, we get $c+b=d+a$. Thus, by definition, $\langle c,d\rangle \sim \langle a,b\rangle$ and $\sim$ is symmetric.

3) Suppose $\langle a,b\rangle \sim \langle c,d\rangle$ and $\langle c,d\rangle \sim \langle e,f\rangle$. Then $a+d=b+c$ and $c+f=d+e$.

Adding these equations produces $a+d+c+f=b+c+d+e$. Clearly c and d cancel, so $a+f=b+e$. We get $\langle a,b\rangle \sim \langle e,f\rangle$, hence $\sim$ is transitive. □

The equivalence class $[\langle a,b\rangle]$ containing the pair $\langle a,b\rangle$ is denoted simply by $[a,b]$. In other words,

$$[a,b]=\{\langle e,f\rangle : \langle e,f\rangle \sim \langle a,b\rangle\}.$$

Definition 7.3. Each equivalence class $[a, b]$ will be called an *integer*. The set of all integers will be called $\mathbb{Z}$ (in case you wonder, the letter Z comes from the German word *Zahl*). Thus:

$$\mathbb{Z} = \{[a, b] : a, b \in \mathbb{N}\}.$$

Note that each integer has infinitely many representations, in the sense that we can choose different representatives; we can write $[13, 15] = [8, 10] = [259, 261] = [a, a + 2]$, among many others.

Exercise 7.4. a. Show that $\langle 6, 12\rangle \in [8, 14]$.

b. Prove: if $\langle c, c\rangle \in [a, b]$, then $a = b$.

c. Prove: if $\langle c, c + 5\rangle \in [4, b]$, then $b = 9$.

Theorem 7.5. *If* $[a, b] = [a', b']$ *and* $[c, d] = [c', d']$*, then* $[a+c, b+d] = [a'+c', b'+d']$ *and* $[ac + bd, ad + bc] = [a'c' + b'd', a'd' + b'c']$.

Proof. Since $a+b' = b+a'$ and $c+d' = d+c'$, we get $a+b'+c+d' = b+a'+d+c'$, hence $[a + c, b + d] = [a' + c', b' + d']$. In order to prove $[ac + bd, ad + bc] = [a'c'+b'd', a'd'+b'c']$, we need to show that $ac+bd+a'd'+b'c' = ad+bc+a'c'+b'd'$. Multiplying the equality $a + b' = b + a'$ by c and d, using distributivity and adding together we get

$$(1)\ ac + bd + b'c + a'd = ad + bc + a'c + b'd.$$

Similarly, multiplying the equality $c + d' = d + c'$ by a' and b', we get

$$(2)\ a'd' + b'c' + a'c + b'd = a'c' + b'd' + a'd + b'c.$$

Adding (1) and (2) we get

$$ac+bd+b'c+a'd+a'd'+b'c'+a'c+b'd = ad+bc+a'c+b'd+a'c'+b'd'+a'd+b'c,$$

and by cancellation, $ac + bd + a'd' + b'c' = ad + bc + a'c' + b'd'$. □

Definition 7.6. We define the addition and multiplication operations on $\mathbb{Z}$ denoted $\oplus$ and $\odot$ (to distinguish from the old operations $+, \cdot$ on $\mathbb{N}$) by

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

$$[a, b] \odot [c, d] = [ac + bd, ad + bc],$$

which by the previous theorem do not depend on representatives. After we get used to the new operations, we will of course go back to the usual $+$ and $\cdot$.

Using the definitions we can easily prove

Theorem 7.7. *We have*

1. $[a, b] = [0, 0] \Leftrightarrow a = b$.
2. $[a, b] \oplus [0, 0] = [0, 0] \oplus [a, b] = [a, b]$.
3. $[0, 0] \odot [a, b] = [0, 0]$.
4. $[1, 0] \odot [a, b] = [a, b]$.

Theorem 7.8. *The operations $\oplus$ and $\odot$ on $\mathbb{Z}$ have the following properties (here a, b, c, d, e, f are natural numbers):*

1. $[a, b] \oplus [c, d] = [c, d] \oplus [a, b]$ *(commutativity).*

2. $([a, b] \oplus [c, d]) \oplus [e, f] = [a, b] \oplus ([c, d] \oplus [e, f])$ *(associativity).*

3. $[a, b] \odot [c, d] = [c, d] \odot [a, b]$ *(commutativity).*

4. $([a, b] \odot [c, d]) \odot [e, f] = [a, b] \odot ([c, d] \odot [e, f])$ *(associativity).*

5. $[a, b] \odot ([c, d] \oplus [e, f]) = [a, b] \odot [c, d] \oplus [a, b] \odot [e, f]$ *(distributivity).*

6. $[a, b] \oplus [c, d] = [a, b] \oplus [e, f] \Rightarrow [c, d] = [e, f]$ *(cancellation).*

7. If $[a, b] \neq [0, 0]$ *and* $[a, b] \odot [c, d] = [a, b] \odot [e, f]$*, then* $[c, d] = [e, f]$ *(cancellation). (Note that the first hypothesis could be written in the form* $a \neq b$*).*

Proof. 1. This follows from the commutativity of the addition of natural numbers.

2. This follows from the associativity of the addition of natural numbers.

3. Indeed, $[ac + bd, ad + bc] = [ca + db, cb + da]$.

4. We compute $([a, b] \odot [c, d]) \odot [e, f] = [ac + bd, ad + bc] \odot [e, f] = [ace + bde + adf + bcf, acf + bdf + ade + bcf]$ and $[a, b] \odot ([c, d] \odot [e, f]) = [a, b] \odot [ce + df, cf + de] = [ace + adf + bcf + bde, acf + ade + bce + bdf]$.

5. We have $[a, b] \odot ([c, d] \oplus [e, f]) = [a, b] \odot [c + e, d + f] = [ac + ae + bd + bf, ad + af + bc + be]$, $[a, b] \odot [c, d] \oplus [a, b] \odot [e, f] = [ac + bd, ad + bc] \oplus [ae + bf, af + be] = [ac + bd + ae + bf, ad + bc + af + be]$.

6. From $[a, b] \oplus [c, d] = [a, b] \oplus [e, f]$ we get $[a + c, b + d] = [a + e, b + f]$, hence $a + c + b + f = b + d + a + e$. Using cancellation for natural numbers, we get $c + f = d + e$ and therefore $[c, d] = [e, f]$.

7. Indeed, $[a, b] \neq [0, 0] \Leftrightarrow a + 0 \neq b + 0 \Leftrightarrow a \neq b$. Assuming $a \neq b$, there are two cases: either $a < b$ or $b < a$. From $[a, b] \odot [c, d] = [a, b] \odot [e, f]$ we get $[ac + bd, ad + bc] = [ae + bf, af + be]$, hence $ac + bd + af + be = ad + bc + ae + bf$ and $a(c + f) + b(d + e) = a(d + e) + b(c + f)$. Assuming $a < b$, $b - a \in \mathbb{P}$ and the last equality could be put in the form $(b - a)(d + e) = (b - a)(c + f)$. Using the cancellation for multiplication of natural numbers, we get $d + e = c + f$ and therefore $[c, d] = [e, f]$. The case $b < a$ is similar. □

7.2. Order

Definition 7.9. We define the relations $\prec$ and $\succ$ on $\mathbb{Z}$ by

1. $[a, b] \prec [c, d] \Leftrightarrow a + d < b + c$.

2. $[a, b] \succ [c, d] \Leftrightarrow [c, d] \prec [a, b]$. We use this notation to distinguish form the old $<$ and $>$ for natural numbers. Again, eventually we will also use $<$ and $>$ for integers.

Exercise 7.10. a. Show that $\prec$ is well defined, in other words prove that if $\langle a, b\rangle \sim \langle a', b'\rangle$, $\langle c, d\rangle \sim \langle c', d'\rangle$, and $a + d < b + c$, then $a' + d' < b' + c'$.

b. Suppose we defined $[a, b] \prec [c, d]$ to mean $a < c$. Would this be well-defined? Why or why not?

Theorem 7.11. *(Trichotomy) For all natural numbers a, b, c, d, exactly one of the following is true in $\mathbb{Z}$: $[a, b] \prec [c, d]$ or $[a, b] = [c, d]$ or $[c, d] \prec [a, b]$.*

Proof. This follows from trichotomy in $\mathbb{N}$. □

Theorem 7.12. *(Transitivity) $[a, b] \prec [c, d] \wedge [c, d] \prec [e, f] \Rightarrow [a, b] \prec [e, f]$.*

Proof. We have $a + d < b + c$ and $c + f < d + e$. Adding together, $a + d + c + f < b + c + d + e$. Canceling $c + d$, we get $a + f < b + e$, hence $[a, b] \prec [e, f]$. □

From now on, when we wish to refer to an integer without mentioning an equivalence class, we will use lower case letters near the end of the alphabet. Sometimes we will be able to prove theorems without having to bring equivalence classes into the picture at all, but when we can't, we are always able to fall back on the definition of an integer.

Theorem 7.13. *For all integers x, y, z we have*

1. $(x \succ y) \wedge (y \succ z) \Rightarrow x \succ z$.
2. $x \prec y \Leftrightarrow x \oplus z \prec y \oplus z$.
3. $(x \prec y) \wedge ([0, 0] \prec z) \Rightarrow x \odot z \prec y \odot z$.
4. $(x \prec y) \wedge ([0, 0] \succ z) \Rightarrow x \odot z \succ y \odot z$.

Proof. 1. This follows from transitivity of $<$ on $\mathbb{N}$.

2. We need to work with representatives: let $x = [a, b], y = [c, d], z = [e, f]$. Then $x \oplus z = [a + e, b + f], y \oplus z = [c + e, d + f]$. We have $a + d < b + c$ and adding $e + f$ both sides, $a + d + e + f < b + c + e + f$, hence $x \oplus z \prec y \oplus z$.

3. Let $x = [a, b], y = [c, d], z = [e, f]$ with $e > f$. We have $[e, f] = [e - f, 0]$. Without loss of generality we may assume $z = [e, 0]$ with $e > 0$. In this case $x \odot z = [ae, be]$ and $y \odot z = [ce, de]$. From $a + d < b + c$, multiplying both sides be e we get $ae + de < be + ce$, hence $x \odot z \prec y \odot z$.

4. Let $x = [a, b], y = [c, d], z = [e, f]$. Since $z \prec [0, 0]$, we may assume $z = [0, f]$ with $f > 0$. In this case $x \odot z = [bf, af]$ and $y \odot z = [df, cf]$. From $a + d < b + c$, we get $af + df < bf + cf$, hence $y \odot z \prec x \odot z$. □

Definition 7.14. An integer x is called *positive* if and only if $x \succ [0, 0]$. An integer x is called *negative* if and only if $x \prec [0, 0]$.

Corollary 7.15. If x is any integer, then exactly one of the following is true: x is positive, x is negative, or $x = [0, 0]$.

Proof. Indeed, if $x = [a, b]$, then either $a < b$, $b < a$, or $a = b$. □

Theorem 7.16. *If x and y are positive integers, then $x \oplus y$ and $x \odot y$ are positive integers. For any $x \in \mathbb{Z}$ there is a unique $y \in \mathbb{Z}$ such that $x \oplus y = [0, 0]$. In fact $[a, b] \oplus [b, a] = [0, 0]$ for all $a, b \in \mathbb{N}$.*

Proof. If $x = [a, 0]$ and $y = [c, 0]$ with $a > 0$ and $c > 0$, then $x \oplus y = [a + c, 0]$ and $x \odot y = [ac, 0]$, hence $x \oplus y$ and $x \odot y$ are positive.

For $x = [a, b]$, we can take $y = [b, a]$ and $x \oplus y = [a + b, a + b] = [0, 0]$. If y' is another integer with $x \oplus y' = [0, 0] = x \oplus y$, by cancellation we get $y = y'$. □

Definition 7.17. The class $[b, a]$ is called the additive inverse or *opposite* of $[a, b]$ and is denoted by $\ominus[a, b]$. We define the subtraction operation on $\mathbb{Z}$ by $x \ominus y = x \oplus (\ominus y)$.

Remark 7.18. We have

1. $\forall x, y \in \mathbb{Z}\ \exists! z \in \mathbb{Z}$ such that $x = y \oplus z$, namely $z = x \ominus y$.
2. For all $x \in \mathbb{Z}$, $\ominus(\ominus x) = x$.

Exercise 7.19. Prove that for $x, y, z \in \mathbb{Z}$

a. $\ominus(x \oplus y) = (\ominus x) \oplus (\ominus y)$.

b. $\ominus(x \ominus y) = y \ominus x$.

c. $x \odot (\ominus y) = (\ominus x) \odot y = \ominus(x \odot y)$.

d. $(\ominus x) \odot (\ominus y) = x \odot y$.

e. $[0, 1] \odot x = \ominus x$.

f. $x \odot y = [0, 0] \Rightarrow (x = [0, 0]) \vee (y = [0, 0])$.

g. $x \odot (y \ominus z) = (x \odot y) \ominus (x \odot z)$.

Theorem 7.20. *For $a, b \in \mathbb{N}$ we have*

1. $a > b \Rightarrow \exists! n \in \mathbb{P}$ *such that* $[a, b] = [n, 0]$.

2. $a < b \Rightarrow \exists! m \in \mathbb{P}$ *such that* $[a, b] = [0, m]$.

Proof. We can take $n = a - b$ in the first case, and $m = b - a$ in the second. □

Definition 7.21. If A is a subset of $\mathbb{Z}$, we say that $\mathbb{N}$ is *isomorphic* with A if and only if there exists a one-to-one function f with domain $\mathbb{N}$ and range A such that for all $a, b \in \mathbb{N}$ we have

$$f(a + b) = f(a) \oplus f(b), \quad f(a \cdot b) = f(a) \odot f(b), \quad \text{and } a < b \Rightarrow f(a) \prec f(b).$$

Such a function f is called an *isomorphism* between $\mathbb{N}$ and A.

Theorem 7.22. *If $A = \{[a, 0] : a \in \mathbb{N}\}$, then $\mathbb{N}$ is isomorphic with A.*

Proof. Define $f : \mathbb{N} \to A, f(n) = [n, 0]$. Then f is a bijection and preserves the addition, multiplication and the strict order. □

Exercise 7.23. For each of the following functions $f : \mathbb{N} \to \mathbb{Z}$, determine which, if any, of the properties of an isomorphism are valid. In each case, assume that A is the range $f(\mathbb{N}) \subseteq \mathbb{Z}$.

a. $f(a) = [a, a]$.

b. $f(a) = [a, a + 1]$.

c. $f(a) = [a, 2a]$.

d. $f(a) = [0, a]$.

e. $f(a) = [a + 1, 2]$.

f. $f(a) = [2a, a]$.

g. $f(a) = [5a, 0]$.

Because there is an isomorphism between $\mathbb{N}$ and the set of nonnegative integers, we will henceforth consider the class $[a, 0]$ to be the same as the natural number a unless there is something to be gained by making a distinction between them. In addition, if x, y are integers, from now on we will ordinarily write: $x + y$ for $x \oplus y$, $x \cdot y$ or xy for $x \odot y$, $x < y$ for $x \prec y$, $-x$ for $\ominus x$, etc.

Remark 7.24. If we repeat the construction of integers as above using pairs of integers instead of pairs of positive integers, we don't get anything new.

Definition 7.25. The set of all positive integers will be denoted by $\mathbb{Z}^+$ or $\mathbb{P}$. The set of all negative integers will be denoted by $\mathbb{Z}^-$.

Using the properties of $\mathbb{P}$ and $\mathbb{N}$, we obtain

Corollary 7.26. 1. If $A \subseteq \mathbb{Z}^+$, $1 \in A$, and $x \in A \Rightarrow x + 1 \in A$, then $G = \mathbb{Z}^+$.

2. If $A \subseteq \mathbb{Z}^+$ and $A \neq \emptyset$, then A contains a unique smallest member.

In part 1, the conclusion remains valid if $\mathbb{Z}^+$ is replaced by the set of all nonnegative integers $\mathbb{Z}^+ \cup \{0\} = \mathbb{N}$ and the hypothesis $1 \in A$ is changed to $0 \in A$.

7.3. Absolute value and divisibility

Definition 7.27. If x is any integer, then the absolute value of x is the natural number defined by:

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

Theorem 7.28. *We have the following properties of the absolute value*

1. $|-x| = |x|$.
2. $x \leq |x|$ *and* $-x \leq |x|$.
3. $|x| = |y| \Leftrightarrow (x = y) \vee (x = -y)$.
4. $|xy| = |x| \cdot |y|$.
5. $a > 0 \Rightarrow (|x| \leq a \Leftrightarrow -a \leq x \leq a)$.
6. $|x| < |y| \Leftrightarrow -|y| < x < |y|$.
7. $|x + y| \leq |x| + |y|$ *(triangle inequality).*
8. $|x - y| \leq |x| + |y|$.
9. $|x| - |y| \leq |x - y|$.

Proof. 1 and 2 follow from the definition, considering the cases $x \geq 0$ and $x < 0$.

3. There are four cases to consider: $x \geq 0$ and $y \geq 0$, $x \geq 0$ and $y < 0$, $x < 0$ and $y \geq 0$, $x < 0$ and $y < 0$. In each case we get: $x = y, x = -y, -x = y$ and $-x = -y$, respectively.

4. We consider the four cases as in 3 and compute.

5. For $x \geq 0$ we get $x \leq a$. For $x < 0$ we get $-x \leq a$, hence $x \geq -a$.

6. We take $a = |y|$ and use 5.

7. If $x \geq 0$ and $y \geq 0$ this is clear. If $x \geq 0$ and $y < 0$, there are two subcases $x + y \geq 0$ and $x + y < 0$. In the first subcase, $x + y \leq x - y$ is true since $y < -y$.

In the second subcase, $-x-y \leq x-y$ is true since $-x \leq x$. If $x<0$ and $y \geq 0$, we treat similarly the subcases $x+y \geq 0$ and $x+y<0$. If $x<0$ and $y<0$, then $-x-y \leq -x-y$ is clearly true.

8. We write $x-y=x+(-y)$, use 7 and 1.

9. We have $|x|=|x-y+y| \leq |x-y|+|y|$, hence $|x|-|y| \leq |x-y|$. □

Exercise 7.29. Prove that

a. $|x|=\max(x,-x)$.

b. $\big||x|-|y|\big| \leq |x-y|$.

c. $a \geq 0 \Rightarrow (|x|>a \Leftrightarrow (x>a) \vee (x<-a))$

Definition 7.30. Let x, y be integers. We say that y is divisible by x, x divides y, or x is a factor of y if and only if $x \neq 0$ and there exists an integer z such that $x \cdot z = y$. We will write $x \mid y$ when x divides y. The integer z is also denoted by y/x or $\dfrac{y}{x}$.

Theorem 7.31. *If x and y are nonzero integers, then:*

1. $x \mid y \Rightarrow |x| \leq |y|$.

2. $x \mid y \Rightarrow |x|\big||y|$.

3. $x \mid 1 \Rightarrow x = \pm 1$.

4. $(x \mid y) \wedge (y \mid x) \Rightarrow x = \pm y$.

5. $(x \mid y) \wedge (y \mid z) \Rightarrow x \mid z$ *(transitivity).*

6. $(x \mid y) \wedge (x \mid z) \Rightarrow x \mid (y \pm z)$.

Proof. 1. If $x \mid y$, then $y = xa$ for $a \in \mathbb{Z} \setminus \{0\}$ and $|y|=|xa|=|a||x| \geq |x|$ since $a| \geq 1$.

2. As above, if $x \mid y$, then $|y|=|a||x|$, hence $|x|\big||y|$.

3. If $1=ax$, then $a=x=1$ or $a=x=-1$.

4. Assuming $x \mid y \wedge y \mid x$, we get $y=ax$ and $x=by$ for some integers a, b. It follows that $y=aby$, hence $ab=1$ and therefore $a=b=1$ or $a=b=-1$. In the first case $y=x$, and in the second $y=-x$.

5. Assuming $x \mid y \wedge y \mid z$, we get $y=ax$ and $z=by$, hence $z=abx$ and $x \mid z$.

6. Assuming $x \mid y \wedge x \mid z$, let $y=ax$ and $z=bx$. Then $y \pm z = ax \pm bx = (a \pm b)x$, hence $x \mid y \pm z$. □

Remark 7.32. The divisibility relation $\mid$ on $\mathbb{Z} \setminus \{0\}$ is reflexive and transitive, but not symmetric because $-2 \mid 4$ and $4 \nmid -2$ or antisymmetric because $-2 \mid 2$ and $-2 \neq 2$.

Theorem 7.33. *(Division Algorithm) For any integer y and any nonzero integer x there exist unique integers q and r such that $y=qx+r$ and $0 \leq r < |x|$.*

Proof. Assume first that $x>0$. Consider the set S of natural numbers of the form $y-kx$ where $k \in \mathbb{Z}$. Notice that S is not empty: for example $y+|y|x \in S$. Indeed, since $x \geq 1$ and $|y| \geq -y$, we get $y+|y|x \geq 0$ and we can take $k=-|y|$. By the well-ordering Principle, S contains a smallest element of the form $r = y - qx$. We found integers q and r with $y = qx + r$ and we know that $r \geq 0$. To show that $r < x$, by way of contradiction assume that $r \geq x$. Then $r - x \geq 0$ and $r - x = y - qx - x = y - (q+1)x \in S$. We found an element in S, namely $r - x$ such that $r - x < r$, which contradicts the fact that r was the smallest. Hence $r < x$.

To show uniqueness, suppose that q' and r' are some integers such that $y = q'x + r'$ and $0 \leq r' < x$. We will show that $q' = q$ and $r' = r$. From $qx + r = q'x + r'$ we get $(q - q')x = r' - r$. By adding the inequalities $-x < -r \leq 0$ and $0 \leq r' < x$, we obtain $-x < r' - r < x$, so using $r' - r = (q - q')x$ we get $-x < (q - q')x < x$. Canceling x, we obtain $-1 < q - q' < 1$, which means that $q - q' = 0$ or $q = q'$. Substituting $q = q'$ in the equation $r' - r = (q - q')x$, we get $r = r'$.

It remains to prove the theorem for $x < 0$. Let $x' = |x| = -x > 0$. Applying the division algorithm for y and x', we find unique q_1 and r such that $y = q_1 x' + r$ and $0 \leq r < x'$. Take $q = -q_1$. We conclude that $y = qx + r$ with $0 \leq r < |x|$, and q, r are unique. □

Exercise 7.34. Suppose it is now 8 a.m. in Boston. What time will be in 6538 hours ?

7.4. Greatest common divisor and least common multiple

Definition 7.35. An integer $z \neq 0$ is a *common divisor* of x and y if and only if $z \mid x$ and $z \mid y$.

An integer z is a *common multiple* of x and y if and only if $x \mid z$ and $y \mid z$.

Definition 7.36. We say that z is a *greatest common divisor* of x and y if and only if z is a common divisor of x and y and for all t such that $t \mid x$ and $t \mid y$, it follows that $t \mid z$. For $x, y \neq 0$, the positive greatest common divisor of x and y is denoted by $\gcd(x, y)$. Of course, $\gcd(0, 0)$ is undefined, and for nonzero x, $\gcd(x, 0) = \gcd(0, x) = |x|$.

We say that z is a *least common multiple* of x and y if and only if z is a common multiple of x and y and for all t such that $x \mid t$ and $y \mid t$ it follows that $z \mid t$. The positive least common multiple of x and y is denoted by $\operatorname{lcm}(x, y)$. If one of x and y is zero, then $\operatorname{lcm}(x, y)$ is undefined.

Example 7.37. $\gcd(4, 6) = 2$, $\operatorname{lcm}(4, 6) = 12$, $\gcd(30, -45) = 15$, $\operatorname{lcm}(30, -45) = 90$, $\gcd(-4, -33) = 1$, $\operatorname{lcm}(-4, -33) = 132$.

Exercise 7.38. Prove that for nonzero integers x, y, z, t we have

a) 1 is a common divisor of x and 1.

b) x is a common divisor of x and x.

c) 1 is a common divisor of x and y.

d) If z is a common divisor of x and y and $t \mid z$, then t is a common divisor of x and y.

e) If z is a common divisor of x and y and $t \mid z$, then z/t is a common divisor of x/t and y/t.

Exercise 7.39. Prove that for nonzero integers x, y, z, t we have

a) x is a common multiple of x and 1.

b) x is a common multiple of x and x.

c) $x \cdot y$ is a common multiple of x and y.

d) If z is a common multiple of x and y and $z \mid t$, then t is a common multiple of x and y.

e) If z is a common multiple of x and y, $t \mid x$, $t \mid y$, and $t \mid z$, then z/t is a common multiple of x/t and y/t.

Theorem 7.40. *If $\emptyset \neq G \subseteq \mathbb{Z}$ and G is closed under subtraction, then there exists an element $d \in G$ such that $G = \{x \cdot d : x \in \mathbb{Z}\}$.*

Proof. If $G = \{0\}$, we can take $d = 0$. Assume that G has nonzero elements. Consider $S = \{|x| : x \in G, x \neq 0\}$. Then $S \subseteq \mathbb{P}$ is not empty, therefore has a least element $a > 0$. For any $x \in G$ there are q, r such that $x = qa + r$ and $0 \leq r < a$. Since $r = x - qa$ and G is closed under subtraction, it follows that $r \in G$. It must be that $r = 0$ and $x = qa$, since a was the smallest element and $r < a$. We can take $d = a$ and we conclude $G = \{q \cdot d : q \in \mathbb{Z}\}$. □

Theorem 7.41. *If x and y are nonzero integers, then gcd(x, y) and lcm(x, y) exist. Moreover, there are $a, b \in \mathbb{Z}$ such that gcd$(x, y) = ax + by$.*

Proof. Consider the set $S = \{xm + yn : m, n \in \mathbb{Z}\}$. Note that $1 \leq x \cdot x + y \cdot y \in S$, hence $S \cap \mathbb{P} \neq \emptyset$. By the well-ordering Principle, $S \cap \mathbb{P}$ contains a smallest element $t \geq 1$. We claim that $t =$gcd(x, y). Let's show first that $t \mid x$.

By the Division Algorithm, there are $q, r \in \mathbb{Z}$ such that $x = tq + r$ with $0 \leq r < t$. We know that $t \in S$ and that there are $a, b \in \mathbb{Z}$ such that $t = ax + by$. By an easy computation, it follows that

$$r = x - tq = x - (ax + by)q = (1 - aq)x + (-bq)y,$$

hence $r \in S$. Since $r < t$, the only possibility is $r = 0$, hence $x = tq$ and $t \mid x$.

A similar argument shows $t \mid y$, hence t is a common divisor. Let z be another common divisor, and let $x = zu, y = zv$. Then $t = ax + by = auz + bvz = (au + bv)z$, hence $z \mid t$. It follows that $t =$gcd(x, y).

Since there is at least one positive common multiple for each pair of nonzero integers x, y (for example $|xy|$), by the well-ordering Principle the set of positive common multiples has a smallest element. This proves that lcm(x, y) exists. □

Lemma 7.42. *Let a, b, c be integers such that $a \mid bc$ and gcd$(a, b) = 1$. Then $a \mid c$.*

Proof. Let $bc = ad$. Since gcd$(a, b) = 1$, there are integers u, v such that $1 = au + bv$. Therefore $c = c \cdot 1 = cau + cbv = cau + adv = a(cu + dv)$ and $a \mid c$. □

Remark 7.43. Let x, y be nonzero integers. If gcd$(x, y) = 1$, then lcm$(x, y) = |xy|$.

Proof. Let $m = |xy|$. It is clear that $x \mid m$ and $y \mid m$, so m is a common multiple. Suppose $x \mid k$ and $y \mid k$. Then $k = xk'$ for some integer k'. Since $y \mid xk'$ and gcd$(x, y) = 1$, by Lemma 7.42 we get $y \mid k'$. It follows that $|xy| = m \mid k$, hence lcm$(x, y) = |xy|$. □

Corollary 7.44. For nonzero integers x, y we have $\mathrm{lcm}(x, y)\cdot\mathrm{gcd}(x, y) = |xy|$.

Proof. Let $d = \mathrm{gcd}(x, y)$. Then $x = dx', y = dy'$ for some integers x', y' and $\mathrm{gcd}(x', y) = 1$. We will prove that $\mathrm{lcm}(x, y) = \frac{|xy|}{d}$. Let $m = \frac{|xy|}{d} = \pm x'y = \pm xy'$. It is clear that $x \mid m$ and $y \mid m$, so m is a common multiple. Assume $x \mid k$ and $y \mid k$. Then $x' \mid k$ and $y \mid k$, so as in the above Remark we conclude that $x'y \mid k$, so $m \mid k$. It follows that $m = \mathrm{lcm}(x, y)$. □

Exercise 7.45. Prove that $\mathrm{gcd}(6n + 8, 4n + 5) = 1$.

Exercise 7.46. Prove by induction that it is possible to pay without requiring change any whole number of roubles greater than 7 with banknotes of value 3 roubles and 5 roubles.

Theorem 7.47. *We have the properties*

1. $(x \mid z) \wedge (y \mid z) \Rightarrow lcm(x, y) \mid z$.
2. $lcm(lcm(x, y), z) = lcm(x, lcm(y, z))$ *(associativity).*
3. $z \mid x \wedge z \mid y \Rightarrow z \mid gcd(x, y)$.
4. $gcd(gcd(x, y), z) = gcd(x, gcd(y, z))$ *(associativity).*
5. $x \mid y \Rightarrow gcd(x, y) = |x|$.
6. $y = q \cdot x + r \Rightarrow gcd(x, y) = gcd(r, x)$.

Proof. Parts 1 and 3 follow from the definition.

2. Both are equal to $\mathrm{lcm}(x, y, z)$, the least common multiple of x, y, z, defined as the smallest positive integer divisible by x, y, z.

4. Both sides are equal to $\mathrm{gcd}(x, y, z)$, the largest positive integer that divides x, y, z.

5. Since $|x| \mid x$ and $|x| \mid y$, we get $|x| \leq \mathrm{gcd}(x, y)$. Since also $\mathrm{gcd}(x, y) \leq |x|$, we get equality.

6. If d divides x and y, then $d \mid y - q \cdot x = r$, hence $d \mid \mathrm{gcd}(r, x)$. Conversely, if $d \mid r$ and $d \mid x$, then $d \mid q \cdot x + r = y$, hence $d \mid \mathrm{gcd}(x, y)$. By double inequality, we get $\mathrm{gcd}(x, y) = \mathrm{gcd}(r, x)$.

□

Theorem 7.48. *(Euclidean Algorithm) Let a, b be positive integers with $a \geq b$. If $b \mid a$, then $gcd(a, b) = b$. If $b \nmid a$, apply the division algorithm repeatedly as follows:*

$$a = bq_0 + r_0, \;\; 0 < r_0 < b$$

$$b = r_0q_1 + r_1, \;\; 0 \leq r_1 < r_0$$

$$r_0 = r_1q_2 + r_2, \;\; 0 \leq r_2 < r_1$$

$$\vdots$$

This process ends when we get a zero remainder, say $r_{n-1} = r_nq_{n+1} + 0$. Then r_n, the last nonzero remainder is the greatest common divisor of a, b. Moreover, using these equations backwards, we may express r_n in the form of a linear combination $au + bv$ for some integers u, v.

Proof. The case $b \mid a$ is clear. For $b \nmid a$, the process ends since $r_0 > r_1 > r_2 \cdots \geq 0$. The fact that the last nonzero remainder r_n is the greatest common divisor follows from part 6 in Theorem 7.47. Putting r_n in the form $au + bv$ is a straightforward computation. □

Example 7.49. Let's find gcd(306, 657). We have

$$\begin{aligned} 657 &= 306 \cdot 2 + 45 \\ 306 &= 45 \cdot 6 + 36 \\ 45 &= 36 \cdot 1 + 9 \\ 36 &= 9 \cdot 4 + 0, \end{aligned}$$

hence $\gcd(306, 657) = 9$. Moreover,

$$\begin{aligned} 9 &= 45 - 36 = 45 - (306 - 45 \cdot 6) = 306 + 45 \cdot 7 = \\ &= 306 + (657 - 306 \cdot 2) \cdot 7 = (-13) \cdot 306 + 7 \cdot 657. \end{aligned}$$

Corollary 7.50. The algorithm may be used to find the greatest common divisor of any two nonzero integers a, b.

Proof. Indeed, we may reduce to the case of positive integers since

$$\gcd(a, b) = \gcd(a, -b) = \gcd(-a, b) = \gcd(-a, -b).$$

□

Definition 7.51. An integer p is prime if and only if p has exactly four divisors.

For example, $\pm 2, \pm 13, \pm 19$ are primes; 0, ± 1, ± 6 are not. An integer other than 0 or ± 1 that is not prime is called composite. For example, $45 = 3 \cdot 3 \cdot 5$ is composite.

Remark 7.52. If p is prime and $p \mid xy$, then $(p \mid x) \vee (p \mid y)$.

Proof. Assume p is prime and $p \mid xy$. Let $d = \gcd(p, x)$. Since p is prime, there are two possibilities: $d = |p|$ or $d = 1$. In the first case $p \mid x$. In the second case, by Lemma 7.42, $p \mid y$. □

Theorem 7.53. *(Fundamental Theorem of Arithmetic) Each integer except* 0 *and* ± 1 *is either a prime, or it can be written in a unique way as a product of primes if we disregard signs and order of factors.*

Proof. We proved part of this theorem by complete induction for positive integers, see Theorem 6.38 in the previous chapter. If n is negative, then $-n$ is prime or $-n = p_1 p_2 \cdots p_k$ with p_j primes $j = 1, ..., k$. Then n is prime or $n = (-p_1) p_2 \cdots p_k$.

For the uniqueness part, assume that $n = p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_m$ with p_i, q_j primes for $i = 1, ..., k, j = 1, ..., m$. We want to show that $k = m$ and that, after reordering and relabeling, if necessary, $p_1 = \pm q_1, p_2 = \pm q_2, ..., p_k = \pm q_k$. We have that $p_1 \mid q_1 q_2 \cdots q_m$. By Remark 7.52, p_1 must divide one of the q_j. By reordering and relabeling, we may assume $p_1 \mid q_1$. It follows that $p_1 = \pm q_1$. Canceling p_1, we get $p_2 p_3 \cdots p_k = \pm q_2 q_3 \cdots q_m$ (assuming $k \geq 2$), hence $p_2 \mid q_2 q_3 \cdots q_m$. Repeating the argument, we eliminate one prime on each side at a time. If $k < m$, then after k steps, we get $1 = \pm q_{k+1} \cdots q_m$, which is impossible, since q_j are primes. A similar argument shows that $k > m$ does not work either. It remains that $k = m$ and $p_i = \pm q_i$ for all $i = 1, ..., k$. □

Corollary 7.54. Consider two integers a, b with $|a|, |b| \geq 2$ and decompose them into a product of primes. Then $\gcd(a, b)$ is the absolute value of the product of the common primes from the decomposition with the least exponent, and $\mathrm{lcm}(a, b)$ is the absolute value of the product of all primes from the decomposition with the largest exponent.

Example 7.55. Let $a = -10140, b = 2600$. We have

$$-10140 = -2^2 \cdot 3 \cdot 5 \cdot 13^2 \quad \text{and} \quad 2600 = 2^3 \cdot 5^2 \cdot 13.$$

Then $\gcd(-10140, 2600) = 2^2 \cdot 5 \cdot 13 = 260$ and $\mathrm{lcm}(-10140, 2600) = 2^3 \cdot 3 \cdot 5^2 \cdot 13^2 = 101400$.

Exercise 7.56. Prove that for each integer x, there exists a prime p such that $x < p$.

Exercise 7.57. Find the greatest common divisor of the following pairs of numbers and express it as a linear combination $au + bv$: $a = 56, b = 72$; $a = 24, b = 138$; $a = 143, b = 227$; $a = 272, b = 1479$.

Exercise 7.58. Prove or disprove: If $a \mid (b + c)$, then $a \mid b$ or $a \mid c$.

Exercise 7.59. Prove that $\gcd(n, n + 1) = 1$ for any integer n.

Exercise 7.60. What are the possible values for $\gcd(n, n + 6)$?

Exercise 7.61. Use induction to show that if $\gcd(a, b) = 1$, then $\gcd(a, b^n) = 1$ for all $n \geq 1$.

Exercise 7.62. For $a, b, c \in \mathbb{Z} \setminus \{0\}$ we defined $\gcd(a, b, c)$ to be the largest positive integer which divides a, b, c. Prove that there are integers s, t, u such that

$$\gcd(a, b, c) = sa + tb + uc.$$

Example 7.63. Find all integer solutions to the (Diophantine) equations

$$a)\ x^2 = y^3, \quad b)\ x^2 = y^4 - 77.$$

Solution. a) Notice that $y \geq 0$ since $x^2 \geq 0$. The obvious solutions are $x = y = 0$, $x = y = 1$, $x = -1, y = 1$. To find all solutions, assume $y \geq 2$, therefore $|x| \geq 2$. Since x and y have the same prime factors and in x^2 each prime has exponent a multiple of 2 and in y^3 each prime has exponent a multiple of 3, it follows that each exponent is a multiple of 6. Hence $x^2 = n^6 = y^3$ and all solutions are of the form $x = \pm n^3, y = n^2$ for $n \in \mathbb{Z}$.

b) The equation is equivalent to $y^4 - x^2 = 77$ or $(y^2 - x)(y^2 + x) = 77$. Since the only divisors of 77 are $\pm 1, \pm 7, \pm 11$ and ± 77 there are the following possibilities

1) $y^2 - x = 1, y^2 + x = 77$, which gives $y^2 = 39$, no solution;

2) $y^2 - x = -1, y^2 + x = -77$, no solution;

3) $y^2 - x = 7, y^2 + x = 11$, which gives $y = \pm 3, x = 2$;

4) $y^2 - x = -7, y^2 + x = -11$, no solution;

5) $y^2 - x = 11, y^2 + x = 7$, which gives $y = \pm 3, x = -2$;

6) $y^2 - x = -11, y^2 + x = -7$, no solution;

7) $y^2 - x = 77, y^2 + x = 1$, no solution;

8) $y^2 - x = -77, y^2 + x = -1$, no solution.

Exercise 7.64. Find the integer solutions of $x^4 = 4y^2 + 4y - 23$.

Exercise 7.65. Verify that $x^2 + x + 41$ is prime for all integers $-40 \leq x \leq 40$, but for $x = 41$ it is not prime.

Example 7.66. Prove that for all $n \geq 0$, $5^{2n} - 3^n$ is divisible by 11.

Proof. This is true for $n = 0$ since $11 \mid 0$. Assume $11 \mid 5^{2k} - 3^k$ for some $k \geq 0$ and let's prove that $11 \mid 5^{2k+2} - 3^{k+1}$. We have

$$5^{2k+2} - 3^{k+1} = 25 \cdot 5^{2k} - 3 \cdot 3^k = 25(5^{2k} - 3^k) + 22 \cdot 3^k.$$

Since $11 \mid 5^{2k} - 3^k$ and $11 \mid 22$ it follows that $11 \mid 5^{2k+2} - 3^{k+1}$. □

Exercise 7.67. *Suppose n is a positive integer such that both $2n + 1$ and $3n + 1$ are perfect squares. Prove that n is divisible by 40.

7.5. Decimal representation and divisibility tests

We are used to the decimal notation, i.e. to write numbers in base 10. When we write 4712, we mean $4 \cdot 10^3 + 7 \cdot 10^2 + 1 \cdot 10^1 + 2 \cdot 10^0$. Any positive integer n has a decimal representation

$$n = a_k a_{k-1} \cdots a_0 = a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + \cdots + a_1 \cdot 10 + a_0,$$

where each a_i is a digit from 0 to 9 and we omit the leading zeros. This representation extends easily to all integers, by adding the number 0 and by using a minus sign for negative integers.

Fix n a positive integer. Recall that two integers a, b are congruent modulo n if n divides $a - b$. We write $a \equiv b (\text{mod } n)$. We proved in Example 5.38 that this is an equivalence relation on $\mathbb{Z}$.

Theorem 7.68. *If $a \equiv b(mod\, n)$ and $c \equiv d(mod\, n)$, then $a + c \equiv b + d(mod\, n)$ and $ac \equiv bd(mod\, n)$.*

Proof. Exercise. □

Theorem 7.69. *Every positive integer $a_k a_{k-1} \cdots a_0$ written in base 10 is congruent modulo 9 to the sum of its digits $a_k + \cdots + a_0$.*

Proof. Since $10 \equiv 1 (\text{mod } 9)$, we get $10^i \equiv 1 (\text{mod } 9)$, hence $a_i \cdot 10^i \equiv a_i (\text{mod } 9)$ for all $0 \leq i \leq k$. We get $\sum_{i=0}^{k} a_i \cdot 10^i \equiv \sum_{i=0}^{k} a_i (\text{mod } 9)$. □

Corollary 7.70. An integer is a multiple of 9 iff the sum of its digits is a multiple of 9.

Exercise 7.71. An integer is a multiple of 3 iff the sum of its digits is a multiple of 3.

Theorem 7.72. *An integer with decimal representation $a_ka_{k-1}\cdots a_0$ is divisible by* 11 *iff the alternating sum of the digits* $\sum_{i=0}^{k}(-1)^ia_i$ *is divisible by* 11*.*

Proof. We use the congruence $10 \equiv -1 (\text{mod } 11)$ to get $a_i \cdot 10^i \equiv (-1)^ia_i (\text{mod } 11)$ and $\sum_{i=0}^{k} a_i \cdot 10^i \equiv \sum_{i=0}^{k}(-1)^ia_i (\text{mod } 11)$. □

Remark 7.73. It is easy to state divisibility tests by $2, 4, 5, 6, 8, 10$:

A number $n = a_ka_{k-1}\cdots a_0$ is divisible by 2 iff the last digit a_0 is even;

$n = a_ka_{k-1}\cdots a_0$ is divisible by 4 iff the number formed by the last two digits a_1a_0 is divisible by 4;

$n = a_ka_{k-1}\cdots a_0$ is divisible by 5 iff the last digit a_0 is 0 or 5;

$n = a_ka_{k-1}\cdots a_0$ is divisible by 6 iff it is divisible by 2 and 3;

$n = a_ka_{k-1}\cdots a_0$ is divisible by 8 iff the number formed by the last three digits $a_2a_1a_0$ is divisible by 8;

$n = a_ka_{k-1}\cdots a_0$ is divisible by 10 iff the last digit a_0 is 0.

Proof. For example, $n = a_ka_{k-1}\cdots a_2 \cdot 10^2 + a_1a_0$ and $4 \mid 100$. Also, $n = a_ka_{k-1}\cdots a_3 \cdot 10^3 + a_2a_1a_0$ and $8 \mid 1000$. We leave the other cases as exercise. □

Remark 7.74. There are different ways of representing integers, using a base other than 10. For example, in base 2 we use only the digits 0 and 1 and the number 7 is binary represented as 111. An integer with binary representation $a_ka_{k-1}\cdots a_0$ is divisible by 2 iff the last digit a_0 is 0. It is divisible by 4 iff the last two digits a_1, a_0 are 0.

It would be interesting to state some divisibility tests for positive integers represented in a base other than 10.

Exercise 7.75. Prove that if n is odd, then $n^2 \equiv 1 (\text{mod } 8)$.

Exercise 7.76. Prove that for any integer n we have $n^3 \equiv n (\text{mod } 6)$.

Exercise 7.77. For the following congruence equations, either find a solution $x \in \mathbb{Z}$ or show that no solution exists:

$$99x \equiv 18 \ (\text{mod } 30), \ \ 91x \equiv 84 \ (\text{mod } 143), \ \ x^2 \equiv 2 \ (\text{mod } 5),$$
$$x^2 + x + 1 \equiv 0 \ (\text{mod } 5), \ \ x^2 + x + 1 \equiv 0 \ (\text{mod } 7).$$

Chapter 8

Cardinality. Finite sets, infinite sets

Learning how to count the elements of a set is a great achievement. Of course, this is easy for (small) finite sets like $\{a, b, c\}$ or $\{1, 3, 5, 7\}$. What if the sets are infinite? We will see that there are different flavors of infinity, something that puzzled people for many years. The correct way to compare infinite sets is a notion called cardinality and is based on the existence of bijective functions.

8.1. Equipotent sets

Definition 8.1. Fix a universe U. Two sets $A, B \subseteq U$ have the same cardinality or are equipotent, written $A \approx B$ if there is a bijection $f : A \to B$.

Remark 8.2. Using the empty bijection, we have $\emptyset \approx \emptyset$.

Example 8.3. Let X be a set with ten elements, let S be the set of all six-element subsets of X, and let T be the set of all four-element subsets of X. Then $S \approx T$. Indeed, define $f : S \to T, f(A) = X \setminus A$. Then f is one-to-one and onto. Its inverse is $f^{-1} : T \to S, f^{-1}(B) = X \setminus B$. We will see later how many elements are in the sets S and T.

Example 8.4. Let E denote the set of even integers, and define $f : \mathbb{Z} \to E, f(n) = 2n$. Then f is a bijection, hence $E \approx \mathbb{Z}$. This example illustrates the fact that $\mathbb{Z}$ is equipotent with a proper subset.

Example 8.5. Let $a, b \in \mathbb{R}$ with $a < b$. Then $f : (a, b) \to (0, 1), f(x) = \dfrac{x - a}{b - a}$ is a bijection and hence $(a, b) \approx (0, 1)$.

Example 8.6. The function $\arctan : \mathbb{R} \to (-\pi/2, \pi/2)$ is a bijection, so $\mathbb{R} \approx (-\pi/2, \pi/2)$.

Theorem 8.7. *The relation $\approx$ is an equivalence relation on $\mathcal{P}(U)$. The equivalence class of A is denoted $|A|$ and is called the cardinality of A.*

Proof. It suffices to consider nonempty subsets. Indeed, $\approx$ is reflexive, since $id_A : A \to A$ is a bijection. If $A \approx B$, let $f : A \to B$ be a bijection. Then $f^{-1} : B \to A$ is also a bijection, hence $B \approx A$, so $\approx$ is symmetric. Assume $A \approx B$ and $B \approx C$. Then there are bijections $f : A \to B$ and $g : B \to C$. Consider $g \circ f : A \to C$. Then $g \circ f$ is a bijection, hence $A \approx C$, and $\approx$ is transitive. □

Corollary 8.8. We have $|\mathbb{R}| = |(0, 1)|$.

Remark 8.9. Cardinals are generalizing natural numbers. Indeed, we can think of 0 as $|\emptyset|$, 1 as $|\{\emptyset\}|$, 2 as $|\{\emptyset, \{\emptyset\}\}|$, and in general $n + 1$ as $|n \cup \{n\}|$. The idea is that all sets containing exactly n elements have cardinality n.

Theorem 8.10. *Let A, B, C, D be sets such that $A \approx C$ and $B \approx D$. Then $A \times B \approx C \times D$.*

Proof. Let $f : A \to C$ and $g : B \to D$ be bijections. Define $f \times g : A \times B \to C \times D, (f \times g)(\langle a, b\rangle = \langle f(a), g(b)\rangle)$. Then $f \times g$ is a bijection. □

Theorem 8.11. *Let A, B, C, D be sets such that $A \approx B, C \approx D, A \cap C = \emptyset$ and $B \cap D = \emptyset$. Then $A \cup C \approx B \cup D$.*

Proof. Consider bijections $f : A \to B$ and $g : C \to D$ and define

$$f \cup g : A \cup C \to B \cup D, (f \cup g)(x) = \begin{cases} f(x) & \text{if} \quad x \in A \\ g(x) & \text{if} \quad x \in C. \end{cases}$$

Then $f \cup g$ is well defined since $A \cap C = \emptyset$. It is one-to-one since f and g are one-to-one. It is onto since f, g are onto and $B \cap D = \emptyset$. □

Definition 8.12. For arbitrary sets A, B in a fixed universe U, we write $|A| \leq |B|$ if there is a one-to-one function $f : A \to B$ and $|A| < |B|$ if $|A| \leq |B|$ and $A \not\approx B$.

Theorem 8.13. *(Cantor) If A is a set, then $|A| < |\mathcal{P}(A)|$.*

Proof. This is clear for $A = \emptyset$ because $|\emptyset| = 0 < 1 = |\{\emptyset\}|$. Assume $A \neq \emptyset$ and define $f : A \to \mathcal{P}(A)$ by $f(a) = \{a\}$. Then f is injective, since $f(a_1) = f(a_2)$ implies $\{a_1\} = \{a_2\}$, hence $a_1 = a_2$. We deduce that $|A| \leq |\mathcal{P}(A)|$. To prove the strict inequality, assume that there is a bijection $g : A \to \mathcal{P}(A)$, and define

$$B = \{a \in A : a \notin g(a)\}$$

(recall that $g(a) \subseteq A$). Then $B \subseteq A$, hence $B \in \mathcal{P}(A)$. Since g is onto, there is $b \in A$ with $g(b) = B$. Let's determine if $b \in B$ or not. If $b \in B$, then $b \notin g(b) = B$, contradiction. If $b \notin B$, then $b \in g(b) = B$, contradiction. It follows that g can not be onto, hence $|A| < |\mathcal{P}(A)|$. Notice the similarity of this proof with Russell's paradox. □

Theorem 8.14. *(Cantor-Bernstein) If $|A| \leq |B|$ and $|B| \leq |A|$, then $|A| = |B|$.*

Proof. Since $|A| \leq |B|$ and $|B| \leq |A|$, there are $B' \subseteq B$ with $A \approx B'$ and $A' \subseteq A$ with $B \approx A'$. Consider bijections $f : A \to B'$ and $g : B \to A'$ with inverses $f^{-1} : B' \to A, g^{-1} : A' \to B$. We will construct a bijection $h : A \to B$. Let $a \in A$. If $a \in A'$, then $g^{-1}(a) \in B$. Let's call $g^{-1}(a)$ the first ancestor of a. If $g^{-1}(a) \in B'$, then $f^{-1}(g^{-1}(a)) \in A$, which we call the second ancestor of a. If $f^{-1}(g^{-1}(a)) \in A'$, then $g^{-1}(f^{-1}(g^{-1}(a))) \in B$, the third ancestor. We continue this process.

For each $a \in A$, one of the three possibilities holds

1) a has infinitely many ancestors;

2) a has a last ancestor belonging to A;

3) a has a last ancestor belonging to B.

Define

$$A_\infty = \{a \in A : a \text{ has infinitely many ancestors}\}$$
$$A_0 = \{a \in A : a \text{ has an even number of ancestors}\}$$
$$A_1 = \{a \in A : a \text{ has an odd number of ancestors}\}.$$

Note that $A_\infty \subseteq A'$, $A \setminus A' \subseteq A_0$, and $A = A_\infty \cup A_0 \cup A_1$ with A_∞, A_0, A_1 mutually disjoint. In a similar way we decompose $B = B_\infty \cup B_0 \cup B_1$. We claim that f takes A_∞ onto B_∞, and takes A_0 onto B_1, while g^{-1} sends A_1 onto B_0. Indeed, if $a \in A$ has infinitely many ancestors, then $f(a) \in B$ has infinitely many ancestors; if $a \in A$ has an even number of ancestors, then $f(a) \in B$ has an odd number of ancestors, and if $a \in A$ has an odd number of ancestors, then $g^{-1}(a) \in B$ has an even number of ancestors. We can define

$$h : A \to B, h(x) = \begin{cases} f(x) & x \in A_\infty \cup A_0 \\ g^{-1}(x) & x \in A_1. \end{cases}$$

Since $f \mid_{A_\infty} : A_\infty \to B_\infty, f \mid_{A_0} : A_0 \to B_1$ and $g^{-1} \mid_{A_1} : A_1 \to B_0$ are bijections, we conclude that h is a bijection and $|A| = |B|$. □

Exercise 8.15. Let A be a set. Recall that $\{0,1\}^A$ denotes the set of all functions $f : A \to \{0,1\}$. Using characteristic functions, prove that $|\{0,1\}^A| = |\mathcal{P}(A)|$.

8.2. Finite and infinite sets

Definition 8.16. Let $\mathbb{N}_0 = \emptyset$ and for $n \geq 1$, denote $\mathbb{N}_n = \{0, 1, 2, ..., n-1\}$. A set A is finite iff $A \approx \mathbb{N}_n$ for some $n \in \mathbb{N}$. In this case we say that A has n elements and write $|A| = n$. (Note in particular that $\emptyset$ is finite and it has 0 elements). A set is *infinite* if it is not finite. The sets $\mathbb{P}, \mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{R} \setminus \mathbb{Q}, \mathbb{C}$ are infinite.

Theorem 8.17. *If A, B are finite and disjoint, then $A \cup B$ is finite and $|A \cup B| = |A| + |B|$.*

Proof. Let $|A| = n, |B| = m$. We can find a bijection $f : A \to \{1, 2, ..., n\}$ and a bijection $g : B \to \{n+1, n+2, ..., n+m\}$. Then

$$h : A \cup B \to \{1, 2, ..., n+m\}, h(x) = \begin{cases} f(x) & \text{if} \quad x \in A \\ g(x) & \text{if} \quad x \in B \end{cases}$$

is a well defined bijection and shows that $|A \cup B| = n + m$. □

Theorem 8.18. *If $A \subset B$ and B is finite nonempty, then A is finite and $|A| < |B|$.*

Proof. Let $|B| = n$. If $n = 1$, then $A = \emptyset$ and $|A| = 0 < 1$. Suppose that the result is true for $n = k$. Consider $A \subset B$ with $|B| = k + 1$. We can assume $B = \{b_1, b_2, ..., b_k, b_{k+1}\}$. There are two cases: $b_{k+1} \notin A$ and $b_{k+1} \in A$. In the first case, $A \subset \{b_1, b_2, ...b_k\}$ and we are done. In the second case, it follows that $A_1 = A \cap \{b_1, b_2, ...b_k\} \subset \{b_1, b_2, ...b_k\}$ and $A = \{b_{k+1}\} \cup A_1$. We know that $|A_1| < k$ and therefore $|A| = 1 + |A_1| < k + 1$. □

Theorem 8.19. *Every set containing an infinite subset is infinite. An infinite set is equipotent to a proper subset.*

Proof. If $A \subseteq B$ and A is infinite, then B is infinite. Indeed, we already proved the contrapositive: if B finite and $A \subseteq B$, then A is finite.

For the second part, assume A is infinite. First we use the Axiom of choice to prove that it contains an infinite set of the form $C = \{x_1, x_2, x_3, ...\}$. Since A is infinite, it is non-empty. Choose $x_1 \in A$. The set $A \setminus \{x_1\}$ is also infinite; choose $x_2 \in A \setminus \{x_1\}$. Inductively we can choose $x_n \in A \setminus \{x_1, x_2, ..., x_{n-1}\}$ for all $n \geq 2$. At each step, the set $A \setminus \{x_1, x_2, ..., x_{n-1}\}$ is not empty since A is infinite. Define $f : A \to A$ by $f(x_i) = x_{2i}$ for all $x_i \in C$ and $f(a) = a$ for all $a \notin C$. Then f is a bijection of A onto the proper subset $A' = A \setminus \{x_1, x_3, x_5, ...\}$. □

Remark 8.20. In fact, if a set A is equipotent to a proper subset, then A is infinite. This property is taken sometimes as the definition of an infinite set.

8.3. Countable and uncountable sets

Definition 8.21. A set is called *countable* iff $A \approx \mathbb{N}$. A set is called *at most countable* if it is finite or countable. A set which is not at most countable is called *uncountable*. The cardinality of $\mathbb{N}$ is denoted by $\aleph_0$ (read aleph zero), so $|\mathbb{N}| = \aleph_0$.

Examples 8.22. 1. The set $\mathbb{P}$ of positive integers is countable, since $f : \mathbb{P} \to \mathbb{N}, f(n) = n - 1$ is a bijection.

2. The set $\mathbb{Z}$ is countable. Indeed, the function

$$f : \mathbb{N} \to \mathbb{Z}, f(n) = \begin{cases} k & \text{if } n = 2k \\ -k & \text{if } n = 2k+1 \end{cases}$$

is a bijection (exercise!).

3. The set E of even integers is countable. Indeed, $f : \mathbb{Z} \to E, f(k) = 2k$ is a bijection.

Theorem 8.23. *Let A be a nonempty set. The following are equivalent:*

(1) There is an onto function $f : \mathbb{N} \to A$.

(2) There is one-to-one function $g : A \to \mathbb{N}$.

(3) A is at most countable.

Proof. (1) ⇒ (2). Let $f : \mathbb{N} \to A$ be a surjection. Define $g : A \to \mathbb{N}$ by $g(a) =$ the least element of $f^{-1}(a)$. The function g is well defined because f is onto, so

$f^{-1}(a) \neq \emptyset$. To show that g is one-to-one, notice that for $a_1 \neq a_2$, the sets $f^{-1}(a_1)$ and $f^{-1}(a_2)$ are disjoint, so $g(a_1) \neq g(a_2)$.

(2) $\Rightarrow$ (3). Fix $g : A \to \mathbb{N}$ one-to-one. To prove that A is at most countable, notice that it suffices to show that any subset B of $\mathbb{N}$ is at most countable, since A is in bijection with $g(A)$. If B is finite, it is at most countable by definition. Assume $B \subseteq \mathbb{N}$ infinite, and let's construct a bijection $h : \mathbb{N} \to B$. Let $h(0)$ be the least element of B, let $h(1)$ be the least element of $B \setminus \{h(0)\}$, and in general let $h(n)$ be the least element of $B \setminus \{h(0), ..., h(n-1)\}$. For all n, the set $B \setminus \{h(0), ..., h(n-1)\}$ is not empty since B is infinite, and the least element exists by the Well ordering Principle. Notice that by construction h is one-to-one since for $m < n$ the element $h(m)$ belongs to $\{h(0), ..., h(n-1)\}$, so $h(m) \neq h(n)$. In particular $h(\mathbb{N})$ is infinite. To show that h is onto, let $b \in B$ and choose $n \in \mathbb{N}$ such that $h(n) > b$. Let m be the smallest natural number such that $h(m) \geq b$. Then for all $j < m$ we must have $h(j) < b$, so $b \notin h(\{0, 1, ..., m-1\})$. By definition, $h(m)$ is the smallest element of $B \setminus h(\{0, 1, ..., m-1\})$, so $h(m) \leq b$. It follows that $h(m) = b$ and h is onto.

(3) $\Rightarrow$ (1). Suppose A is at most countable. If A is infinite, there is a bijection $f : \mathbb{N} \to A$ by definition; in particular this f is onto. If A is finite, we can find a bijection $f : \mathbb{N}_n \to A$ for some $n \geq 1$. We can extend f to a surjection $\tilde{f} : \mathbb{N} \to A$ by defining $\tilde{f}(m) = f(0)$ for $m \geq n$. □

Corollary 8.24. A subset of a countable set is at most countable.

Theorem 8.25. *If A is finite and B is at most countable, then $A \cup B$ is at most countable.*

Proof. If B is finite, then $A \cup B$ is finite, hence at most countable. Assume B infinite. Since $A \cup B = (A \setminus B) \cup B$ and $A \setminus B$ is finite, it suffices to consider disjoint sets. Consider bijections $f : A \to \mathbb{N}_n$ for some $n \geq 0$ and $g : B \to \mathbb{N}$. Define $h : A \cup B \to \mathbb{N}, h(a) = f(a)$ if $a \in A$ and $h(b) = n + g(b)$ if $b \in B$. Since $A \cap B = \emptyset$, h is well defined and it is bijective (exercise!). □

Theorem 8.26. *If A, B are at most countable sets, then $A \cup B$ is at most countable.*

Proof. As before, we may assume A, B disjoint and infinite. To show that $A \cup B$ is countable, we first define bijections $f : A \to E$ and $g : B \to \mathbb{Z} \setminus E$, where E is the set of even integers. Define $h : A \cup B \to \mathbb{Z}$ as $h = f \cup g$. Then h is a bijection. □

Corollary 8.27. A finite union of at most countable sets is at most countable.

Theorem 8.28. *The set $\mathbb{N} \times \mathbb{N}$ is countable. If we define the product of cardinals as $|A| \cdot |B| = |A \times B|$, then $\aleph_0 \cdot \aleph_0 = \aleph_0$.*

Proof. Let $f : \mathbb{N} \times \mathbb{N} \to \mathbb{P}, f(\langle m, n\rangle) = 2^m(2n+1)$. Then f is a bijection. Indeed, if $f(\langle m, n\rangle) = f(\langle m', n'\rangle)$, then $2^{m'}(2n'+1) = 2^m(2n+1)$, hence $m = m'$ and $n' = n$ and f is one-to-one. Given a positive integer k, then write $k = 2^m(2n+1)$ for some $m \geq 0$ and $n \geq 0$, hence f is onto. Since $\mathbb{P} \approx \mathbb{N}$, we get that $\mathbb{N} \times \mathbb{N} \approx \mathbb{N}$. □

Theorem 8.29. *The set $\mathbb{Q}^+$ of positive rational numbers is countable.*

Proof. Write

$$\mathbb{Q}^+ = \left\{ \frac{p}{q} : p, q \in \mathbb{P} \text{ and } \gcd(p,q) = 1 \right\}$$

and define $f : \mathbb{Q}^+ \to \mathbb{N} \times \mathbb{N}$, $f(p/q) = \langle p, q \rangle$. Then f is one-to-one, hence $|\mathbb{Q}^+| \le \aleph_0$. Since $g : \mathbb{P} \to \mathbb{Q}^+, g(p) = \dfrac{p}{1}$ is also one-to-one, we get $\aleph_0 \le |\mathbb{Q}^+|$, hence equality. □

Corollary 8.30. The set of rational numbers $\mathbb{Q}$ is countable.

Proof. If $\mathbb{Q}^-$ denotes the set of negative rational numbers, then $f : \mathbb{Q}^+ \to \mathbb{Q}^-, f(x) = -x$ is a bijection. Now use the fact that $\mathbb{Q} = \mathbb{Q}^+ \cup \{0\} \cup \mathbb{Q}^-$. □

Exercise 8.31. Consider a bijection $\phi : \mathbb{Q} \to \mathbb{N}$ and define a relation R on $\mathbb{Q}$ such that xRy iff $\phi(x) \le \phi(y)$. Prove that $(\mathbb{Q}, R)$ is an well-ordered set.

Theorem 8.32. *The interval* $(0,1)$ *is uncountable.*

Proof. Suppose $f : \mathbb{P} \to (0,1)$ is a bijection. We list all real numbers in $(0,1)$ in decimal form, not ending with an infinite string of nines:

$$\begin{aligned} f(1) &= 0.a_{11}a_{12}a_{13}... \\ f(2) &= 0.a_{21}a_{22}a_{23}... \\ f(3) &= 0.a_{31}a_{32}a_{33}... \\ &\vdots \\ f(n) &= 0.a_{n1}a_{n2}a_{n3}... \\ &\vdots \end{aligned}$$

Define

$$b_k = \begin{cases} 2, & \text{if } a_{kk} \neq 2 \\ 4, & \text{if } a_{kk} = 2. \end{cases}$$

Notice that the number $b = 0.b_1b_2b_3... \in (0,1)$ does not appear on the list because $b_k \neq a_{kk}$ and $b_k \neq 9$. This is a contradiction with the fact that f is a bijection, so $(0,1)$ is uncountable. This proof technique is called the Cantor's diagonal argument. □

The cardinality of $(0,1)$ or $\mathbb{R}$ is denoted by $\mathbf{c}$, called the continuum.

Exercise 8.33. Denote by $\mathcal{P}_f(\mathbb{N})$ the set of finite subsets of $\mathbb{N}$. Prove that $\mathcal{P}_f(\mathbb{N})$ is countable.

Exercise 8.34. Prove that the set of irrational numbers is uncountable.

Exercise 8.35. A real number α is called algebraic if it satisfies a polynomial equation with integer coefficients

$$x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 = 0.$$

For example, $1 + \sqrt{2}$ is algebraic since it satisfies $x^2 - 2x - 1 = 0$. Assuming that each polynomial equation has finitely many roots, prove that the set of algebraic numbers is countable.

Exercise 8.36. Let S be the set of all infinite sequences of 0s and 1s. Use Cantor's diagonal argument to prove that S is uncountable.

Exercise 8.37. Show that a countable union of countable sets is countable.

Exercise 8.38. Find a bijection $f : (0,1) \to [0,1]$. (Hint: choose a countable subset $\{x_0, x_1, x_2, ...\}$ of $(0,1)$ and define $f(x_0) = 0, f(x_1) = 1$ and for $n \geq 2$ let $f(x_n) = x_{n-2}$. Extend f to a bijection).

Exercise 8.39. Suppose there are injective functions $f : A \to B, g : B \to C$ and $h : C \to A$. Prove that $A \approx B \approx C$.

Remark 8.40. We have $\aleph_0 < |\mathcal{P}(\mathbb{N})| = 2^{\aleph_0}$, where for a set A we define $2^{|A|}$ as $|\mathcal{P}(A)|$.

We accept the **Continuum hypothesis**. There is no set X with $\aleph_0 < |X| < \mathbf{c}$.

Corollary 8.41. We have $\mathbf{c} = 2^{\aleph_0}$.

Chapter 9

Counting techniques and combinatorics

In this chapter we will learn how to count the number of elements in certain finite sets, using inclusion-exclusion principle, multiplication principle and more. We will introduce permutations and combinations, binomial coefficients, recursive sequences and recurrence relations.

Theorem 9.1. *Let $A_1, ..., A_n$ be disjoint finite sets. Then*

$$|A_1 \cup ... \cup A_n| = |A_1| + ... + |A_n|.$$

Proof. We have seen in Theorem 8.17 that for A, B disjoint we have $|A \cup B| = |A| + |B|$. The proof now proceeds by induction. □

Example 9.2. Let A be the set of all integers n from 1 to 100 which have at least one digit of 4. Then $|A| = 19$. Indeed, we have $A = A_1 \cup ... \cup A_{10}$, where $A_1 = \{4\}, A_2 = \{14\}, A_3 = \{24\}, ..., A_5 = \{41, 42, ..., 49\}, ..., A_{10} = \{94\}$. Then $|A_5| = 10$ and $|A_i| = 1$ for $1 \leq i \leq 10$, $i \neq 5$. Thus $|A| = |A_1| + ... + |A_{10}| = 19$.

9.1. Counting principles

Theorem 9.3. *(Inclusion-exclusion principle) Let A, B be finite sets. Then*

$$|A \cup B| = |A| + |B| - |A \cap B|.$$

Proof. We can write $A = (A \setminus B) \cup A \cap B$ and $B = (B \setminus A) \cup A \cap B$ and the sets $A \setminus B, B \setminus A$ and $A \cap B$ are disjoint. It follows that

$$|A \cup B| = |A \setminus B| + |B \setminus A| + |A \cap B| =$$

$$= |A| - |A \cap B| + |B| - |A \cap B| + |A \cap B| = |A| + |B| - |A \cap B|.$$

□

Corollary 9.4. Let $A_1, A_2, ..., A_n$ be finite sets. Then

$$|A_1 \cup A_2 \cup \cdots \cup A_n| =$$

$$= \sum_{i=1}^{n} |A_i| - \sum_{i<j} |A_i \cap A_j| + \sum_{i<j<k} |A_i \cap A_j \cap A_k| - \cdots + (-1)^{n+1} |A_1 \cap A_2 \cap \cdots \cap A_n|.$$

Proof. By Induction. □

Exercise 9.5. Suppose $|A \cup B| = 7, |A| = 5$ and $|B| = 4$. Find $|A \cap B|$.

Example 9.6. How many positive integers from 1 to 100 are divisible by $2, 3$ or 5?

Solution. There are 50 integers divisible by 2, 33 divisible by 3, 20 divisible by 5, 16 divisible by 6, 10 divisible by 10, 6 divisible by 15 and 3 divisible by 30. Using the inclusion-exclusion principle, the number of integers from 1 to 100 divisible by $2, 3$ or 5 is

$$50 + 33 + 20 - 16 - 10 - 6 + 3 = 74.$$

Exercise 9.7. Three sets have 100 elements each. Any two of them have exactly 50 elements in common. Exactly 25 elements are in all three. How many elements are in the union?

Exercise 9.8. 73% of British people like cheese, 76% like apples and 10% like neither. What percentage like both cheese and apples?

Exercise 9.9. Find the number of integers between 1 and 5000 which are divisible by neither 3 nor 4. Find the number of integers between 1 and 5000 which are divisible by one or more of the numbers $4, 5$ and 6.

Theorem 9.10. *(Multiplication principle) For $A_1, A_2, ..., A_n$ finite we have $|A_1 \times ... \times A_n| = |A_1| \cdot ... \cdot |A_n|$.*

Proof. Indeed, $|A \times B| = |A| \cdot |B|$ and we may use induction on n. □

Theorem 9.11. *(Exponential principle) Recall that A^B denotes the set of functions $f : B \to A$. For A, B finite sets we have $|A^B| = |A|^{|B|}$.*

Proof. We use induction on $|B|$. For $|B| = 1$, the set A^B has exactly $|A|$ elements. Assume that the formula is true for $|B| = k$. Then for $|B| = k + 1$, let's assume $B = \{b_1, b_2, ..., b_k, b_{k+1}\}$. A function $f : B \to A$ is determined by $f\mid_{\{b_1,b_2,...,b_k\}}$ and $f(b_{k+1})$. Since there are $|A|^k$ possibilities for the restriction $f\mid_{\{b_1,b_2,...,b_k\}}$ and $|A|$ possibilities for $f(b_{k+1})$, we obtain that $|A^B| = |A|^k \cdot |A| = |A|^{k+1} = |A|^{|B|}$.

□

Remark 9.12. For infinite sets A, B, we define $|A|^{|B|}$ to be $|A^B|$. This is consistent with the exponential principle.

Exercise 9.13. How many integers between 1 and 1000 have distinct digits?

Exercise 9.14. In a certain state, a license plate consists of three uppercase English letters followed by three digits from 0 to 9. How many license plates can be issued?

Exercise 9.15. Suppose 2000 people are at a gathering. Then some people have the same birthday. Find the minimum number of such people.

9.2. Permutations and combinations

Definition 9.16. A permutation of $A = \{a_1, ..., a_n\}$ is a bijection $\pi : A \to A$.

Theorem 9.17. *There are $n! = 1 \cdot 2 \cdot 3 \cdots n$ permutations of a set with $n \geq 1$ elements.*

Proof. Let $A = \{a_1, ..., a_n\}$ be a set with $n \geq 1$ elements. For a bijection $\pi : A \to A$, there are n possibilities for $\pi(a_1)$. Once we fix $\pi(a_1)$, there are $n-1$ possibilities for $\pi(a_2)$. Once we fix $\pi(a_2)$, there are $n-2$ possibilities for $\pi(a_3)$. Continuing in this way, there is only one possibility for $\pi(a_n)$. Multiplying, we get $n(n-1)\cdots 1 = n!$ bijections $\pi : A \to A$. □

Definition 9.18. A permutation of size k of n objects with $1 \leq k \leq n$ is an ordered list of length k of elements of a set A with n elements.

Theorem 9.19. *If we denote by $P(n,k)$ the number of permutations of length k of a set with n elements, then*

$$P(n,k) = n(n-1)\cdots(n-k+1) = \frac{n!}{(n-k)!},$$

where by definition $0! = 1$.

Proof. Indeed, for the first position there are n choices, for the second position there are $n-1$ choices,..., for the kth position there are $n-k+1$ choices. □

Definition 9.20. Let A be a set with n elements, and let k with $0 \leq k \leq n$. A subset of A with k elements is called a combination of size k chosen from A. The number of such combinations is denoted by $C(n,k)$. Another notation is C_n^k or $\left(\begin{array}{c} n \\ k \end{array}\right)$ (read n choose k).

Theorem 9.21. *For $n \geq 1$, we have*

$$C(n,k) = \frac{P(n,k)}{k!} = \frac{n!}{k!(n-k)!}.$$

Proof. Since we relax the condition that in the list of k elements the order counts, we get $P(n,k) = C(n,k) \cdot k!$, hence $C(n,k) = \dfrac{P(n,k)}{k!}$. □

Exercise 9.22. From a club with 20 members, a president, a vice-president and a secretary are to be chosen. In how many ways can this be done?

Exercise 9.23. In how many ways can the letters of the word *land* be rearranged? Same question for *mara* and *llama*.

Exercise 9.24. In how many ways can eight identical rooks be placed on a 8×8 chessboard so that no rook attacks another rook?

Remark 9.25. We have $C(n,k) = C(n,n-k)$, $C(n+1,k) = C(n,k)+C(n,k-1)$ and $(n-k)C(n,k) = nC(n-1,k)$.

Proof. Indeed,

$$\frac{n!}{k!(n-k)!} = \frac{n!}{(n-k)!(n-(n-k))!},$$

$$\frac{n!}{k!(n-k)!} + \frac{n!}{(k-1)!(n-k+1)!} = \frac{(n-k+1)n! + kn!}{k!(n+1-k)!} =$$

$$= \frac{(n+1)n!}{k!(n+1-k)!} = \frac{(n+1)!}{k!(n+1-k)!},$$

$$(n-k)\frac{n!}{k!(n-k)!} = \frac{n!}{k!(n-k-1)!} = n\frac{(n-1)!}{k!(n-1-k)!}.$$

□

The numbers $\binom{n}{k}$ are also called binomial coefficients. They have a triangular representation, called the Pascal's triangle.

$$\begin{array}{ccccccccccc}
 & & & & & 1 & & & & & \\
 & & & & 1 & & 1 & & & & \\
 & & & 1 & & 2 & & 1 & & & \\
 & & 1 & & 3 & & 3 & & 1 & & \\
 & 1 & & 4 & & 6 & & 4 & & 1 & \\
1 & & 5 & & 10 & & 10 & & 5 & & 1 \\
 & & & & & \cdots & & & & &
\end{array}$$

In each row, we use the identity $C(n+1,k) = C(n,k)+C(n,k-1)$.

Theorem 9.26. *We have the binomial formula*

$$\begin{aligned}(x+y)^n &= \binom{n}{0}x^n + \binom{n}{1}x^{n-1}y + \binom{n}{2}x^{n-2}y^2 + \cdots + \binom{n}{n-1}xy^{n-1} + \binom{n}{n}y^n \\ &= \sum_{m=0}^{n}\binom{n}{m}x^{n-m}y^m.\end{aligned}$$

Proof. For $n = 1$ this is clear, since $(x+y)^1 = x+y = \binom{1}{0}x + \binom{1}{1}y$. Assume

$$(x+y)^k = \sum_{m=0}^{k}\binom{k}{m}x^{k-m}y^m.$$

Then

$$\begin{aligned}(x+y)^{k+1} &= (x+y)(x+y)^k = \\ &= x^{k+1} + \sum_{m=1}^{k} \binom{k}{m} x^{k-m+1} y^m + \sum_{m=0}^{k-1} \binom{k}{m} x^{k-m} y^{m+1} + y^{k+1} = \\ &= x^{k+1} + \sum_{m=1}^{k} \left[\binom{k}{m} + \binom{k}{m-1} \right] x^{k+1-m} y^m + y^{k+1} = \\ &= \sum_{m=0}^{k+1} \binom{k+1}{m} x^{k+1-m} y^m.\end{aligned}$$

□

Corollary 9.27. We have

$$\sum_{k=0}^{n} \binom{n}{k} = 2^n. \tag{9.1}$$

$$\sum_{k=1}^{n} k \binom{n}{k} = n2^{n-1}. \tag{9.2}$$

$$\binom{2n}{n} = \sum_{k=0}^{n} \binom{n}{k}^2. \tag{9.3}$$

Proof. For (9.1), take $x = y = 1$ in the binomial formula.

For (9.2), differentiate $(1+x)^n = \sum_{k=0}^{n} \binom{n}{k} x^k$ and then take $x = 1$.

For (9.3), write $(1+x)^{2n} = (1+x)^n(1+x)^n$ and identify the coefficient of x^n both sides. □

Exercise 9.28. Expand the binomials $(2x+y)^3, (2x+3y)^4, (2x-y)^5$.

Exercise 9.29. Find a such that

$$1 + \frac{1}{2}\binom{n}{1} + \frac{1}{3}\binom{n}{2} + \cdots \frac{1}{n+1}\binom{n}{n} = \frac{a}{n+1}.$$

Exercise 9.30. Twelve balls are placed in a jar. Four are white, three are red, and five are blue. Five balls are taken from the jar. How many selections are possible that contain exactly three white balls?

Exercise 9.31. Prove that

$$\sum_{r=0}^{k} \binom{m}{k-r}\binom{n}{r} = \binom{m+n}{k}.$$

Exercise 9.32. The digits $1, 2, 3, 4, 5, 6$ are written down in some order to form a six digit number.

a) how many such numbers are there?

b) how many such numbers are even?

c) how many are divisible by 4? By 8? By 11?

9.3. Recursive sequences and recurrence relations

Definition 9.33. Given a sequence $s : \mathbb{N} \to \mathbb{R}$, we write $s = (s_n)_{n\geq 0}$, where $s_n = s(n)$. The sequence $(s_n)_{n\geq 0}$ is called *recursive* if there is $n_0 \in \mathbb{N}$ such that for all $n > n_0$, the term s_n can be expressed as a function of $s_0, s_1, ..., s_{n-1}$. That function is called the *recurrence relation.*

Example 9.34. Let $s_0 = 1$ and let $s_n = 2s_{n-1}$ for $n \geq 1$. Then by induction we can prove that $s_n = 2^n$.

Example 9.35. The Fibonacci sequence $(f_n)_{n\geq 0}$, where $f_0 = f_1 = 1, f_n = f_{n-1} + f_{n-2}$ for $n \geq 2$. The Fibonacci sequence appears in nature and is related to the golden ratio. A formula for the general term is given below.

Example 9.36. Consider n straight lines in the plane such that no two are parallel and no three meet at a point (they are in general position). The number of regions r_n determined in the plane by the n lines satisfies $r_0 = 1, r_{n+1} = r_n + n + 1$.

We will use the following result, which reminds you about solving linear differential equations of second order:

Theorem 9.37. *Let $(x_n)_{n\geq 0}$ be a recursive sequence such that*

$$x_n = bx_{n-1} + cx_{n-2},$$

where $b, c \in \mathbb{R}$ are fixed. If the characteristic equation

$$t^2 - bt - c = 0$$

has distinct (complex) roots r_1, r_2, then

$$x_n = \alpha r_1^n + \beta r_2^n$$

for some α, β, determined by x_0, x_1.

If the equation $t^2 - bt - c = 0$ has repeated roots $r_1 = r_2 = r$, then $x_n = \alpha r^n + \beta n r^n$ for some α, β.

Example 9.38. (the Fibonacci sequence) The characteristic equation $t^2 - t - 1 = 0$ has roots

$$r_1 = (1 + \sqrt{5})/2, \quad r_2 = (1 - \sqrt{5})/2.$$

Since

$$\alpha + \beta = 1 \text{ and } \alpha r_1 + \beta r_2 = 1,$$

we get

$$\alpha = \frac{1 + \sqrt{5}}{2\sqrt{5}}, \quad \beta = \frac{\sqrt{5} - 1}{2\sqrt{5}},$$

hence

$$f_n = \frac{1}{\sqrt{5}} \left[\left(\frac{1 + \sqrt{5}}{2} \right)^{n+1} - \left(\frac{1 - \sqrt{5}}{2} \right)^{n+1} \right].$$

Definition 9.39. (Generating functions) Let $(a_n)_{n\geq 0}$ be a sequence of real numbers. The power series

$$f(X) = a_0 + a_1X + \cdots + a_nX^n + \cdots$$

is called the generating function of the sequence, defined for those values of X such that the series converges.

Remark 9.40. The generating function of a recursive sequence can be sometimes used to find the general term of the sequence. In this case, we say that we solved the recurrence. Recall the sum of a geometric series

$$1 + X + X^2 + \cdots + X^n + \cdots = \frac{1}{1-X}$$

for $|X| < 1$. By differentiation, we get

$$1 + 2X + 3X^2 + \cdots + (n+1)X^n + \cdots = \frac{1}{(1-X)^2}.$$

Differentiating again, we get

$$\frac{1}{(1-X)^3} = 1 + \frac{3\cdot 2}{2}X + \frac{4\cdot 3}{2}X^2 + \cdots \frac{(n+2)(n+1)}{2}X^n + \cdots .$$

Example 9.41. Consider the sequence $(a_n)_{n\geq 0}$ with $a_n = 2a_{n-1}, a_0 = 1$. The generating function is

$$f(X) = a_0+a_1X+a_2X^2+\cdots+a_nX^n+\cdots = a_0+2a_0X+2a_1X^2+\cdots+2a_{n-1}X^n+\cdots =$$
$$= a_0 + 2X(a_0 + a_1X + \cdots + a_{n-1}X^{n-1} + \cdots) = 1 + 2Xf(X),$$

hence

$$f(X) = \frac{1}{1-2X} = 1 + 2X + 2^2X^2 + \cdots + 2^nX^n + \cdots$$

for $|X| < 1/2$. We get $a_n = 2^n$ for $n \geq 0$.

Example 9.42. Let $(r_n)_{n\geq 0}$ be the recursive sequence with $r_{n+1} = r_n+n+1, r_0 = 1$. Then

$$\begin{aligned} f(X) &= r_0 + r_1X + r_2X^2 + \cdots + r_{n+1}X^{n+1} + \cdots = \\ &= 1 + (r_0+1)X + (r_1+2)X^2 + \cdots + (r_n+n+1)X^{n+1} + \cdots = \\ &= (1 + X + 2X^2 + \cdots + (n+1)X^{n+1} + \cdots) + X(r_0 + r_1X + \cdots + r_nX^n + \cdots) = \\ &= 1 + \frac{X}{(1-X)^2} + Xf(X) \end{aligned}$$

for $|X| < 1$. We get

$$f(X) = \frac{1}{1-X} + \frac{X}{(1-X)^3}.$$

Since

$$\frac{1}{(1-X)^3} = 1 + \frac{3\cdot 2}{2}X + \frac{4\cdot 3}{2}X^2 + \cdots \frac{(n+2)(n+1)}{2}X^n + \cdots ,$$

we obtain

$$f(X) = 1 + X + X^2 + \cdots X^n + \cdots + X + \frac{3\cdot 2}{2}X^2 + \frac{4\cdot 3}{2}X^3 + \cdots \frac{(n+1)n}{2}X^n + \cdots$$

and

$$r_n = 1 + \frac{n(n+1)}{2}.$$

Exercise 9.43. Solve the recurrence relations

a) $a_n = a_{n-1} + 2a_{n-2}, a_0 = 3, a_1 = 2.$

b) $a_n = 2a_{n-2}, a_0 = 1, a_1 = 2.$

c) $2a_n = 3a_{n-1} - a_{n-2}, a_0 = 1, a_1 = 2.$

d) $a_n = 2a_{n-1} + n/2, a_0 = 1.$

Exercise 9.44. Use generating functions to solve the recurrence $a_n = 4a_{n-1}, a_0 = 2$.

Exercise 9.45. Let b_n be the number of strings of 0 and 1 of length n having no two consecutive 0's. Find a recurrence relation for b_n and solve it.

Exercise 9.46. Consider n straight lines in the plane such that no two are parallel but exactly three are concurrent. In how many regions is the plane divided?

Exercise 9.47. Let (a_n) be a sequence of positive integers such that for all $n \geq 1$ we have $a_{n+1} > a_n$ and $a_{a_n} = 3n$. Find a_1, a_2, a_3. Find a_{100}. What else can you say about the sequence?

Exercise 9.48. The Catalan numbers are defined by $c_0 = 1$ and for $n \geq 1$, c_n represents the number of triangulations of a polygon with $(n+2)$ vertices. It is easy to see that $c_1 = 1, c_2 = 2, c_3 = 5$.

a) Find a recurrence formula for c_n.

b) Compute the generating function $f(X) = \sum_{n=0}^{\infty} c_n X^n$.

c) Derive a formula for c_n.

Chapter 10

The construction of rational numbers

Rational numbers were invented since an equation like $3x = 2$ has no integer solution; you need fractions. People worked with fractions since long time ago: if you want to share a loaf of bread with three other people, each will get one quarter. The modern definition of rational numbers uses the set of integers $\mathbb{Z}$ and an equivalence relation. This construction is generalized in Abstract Algebra to obtain the so-called field of fractions of an integral domain.

10.1. Definition, operations and order

Definition 10.1. Let $\mathbb{Z}^* = \mathbb{Z} \setminus \{0\}$. Define a relation on $\mathbb{Z} \times \mathbb{Z}^*$ by

$$\langle a, b\rangle \sim \langle c, d\rangle \text{ if and only if } ad = bc.$$

Theorem 10.2. *The relation $\sim$ is an equivalence relation on $\mathbb{Z} \times \mathbb{Z}^*$.*

Proof. The relation is reflexive $\langle a, b\rangle \sim \langle a, b\rangle$, since $ab = ba$. It is symmetric since $\langle a, b\rangle \sim \langle c, d\rangle$ implies $\langle c, d\rangle \sim \langle a, b\rangle$. Indeed, $ad = bc$ implies $cb = da$. For transitivity, assume $\langle a, b\rangle \sim \langle c, d\rangle$ and $\langle c, d\rangle \sim \langle e, f\rangle$, hence $ad = bc$ and $cf = de$. Multiplying the first equation by f, we get $adf = bcf = bde$. Canceling $d \neq 0$ we get $af = be$, hence $\langle a, b\rangle \sim \langle e, f\rangle$. □

Definition 10.3. The set of rational numbers $\mathbb{Q}$ is the set of equivalence classes determined by $\sim$. The class containing $\langle a, b\rangle$ is denoted by $[a, b]$ (later this will be denoted in the more traditional fashion by $\dfrac{a}{b}$ or by a/b). The integer a is called numerator, and the integer $b \neq 0$ is called denominator.

Theorem 10.4. *1. We have $[a, b] = [c, d] \Leftrightarrow ad = bc$.*

2. If $[a, b] = [c, d]$ and $[e, f] = [g, h]$, then:

a. $[af + be, bf] = [ch + dg, dh]$ and

b. $[ae, bf] = [cg, dh]$.

Proof. The first part follows from definition. For the second, assume $ad = bc$ and $eh = fg$. For part a, we compute $(af + be)dh = adfh + bdeh = bcfh + bdfg = bf(ch+dg)$, hence $[af+be, bf] = [ch+dg, dh]$. For part b we just multiply the two equations to get $adeh = bcfg$, hence $[ae, bf] = [cg, dh]$. □

Corollary 10.5. We define the addition and multiplication on $\mathbb{Q}$ by

$$[a, b] \oplus [c, d] = [ad + bc, bd]$$

and

$$[a, b] \odot [c, d] = [ac, bd].$$

This definition does not depend on representatives.

Theorem 10.6. *1. We have $[a, b] = [c, b] \Leftrightarrow a = c$.*

2. If $a \neq 0$, then $[a, b] = [a, d] \Leftrightarrow b = d$.

3. We have $[0, 1] \oplus [a, b] = [a, b]$ and $[0, 1] \odot [a, b] = [0, 1]$

4. The operations $\oplus$ and $\odot$ are commutative and associative.

5. The multiplication $\odot$ is distributive with respect to the addition $\oplus$.

6. For $x, y, z \in \mathbb{Q}$ we have $x \oplus y = x \oplus z \Rightarrow y = z$ (cancellation).

7. If $x, y, z \in \mathbb{Q}$ and $x \neq [0, 1]$, then $x \odot y = x \odot z \Rightarrow y = z$ (cancellation).

8. For each $x \in \mathbb{Q}$ there is a unique $y \in \mathbb{Q}$ such that $x \oplus y = [0, 1]$.

Proof. 1. From $ab = bc$ we cancel b and get $a = c$.

2. We have $ad = ab$ and we can cancel a since $a \neq 0$.

3. By definition $[0, 1] \oplus [a, b] = [0 \cdot b + 1 \cdot a, 1 \cdot b] = [a, b]$. Also, $[0, 1] \odot [a, b] = [0 \cdot a, 1 \cdot b] = [0, b] = [0, 1]$.

4. Straightforward computations:

$$[a, b] \oplus [c, d] = [ad + bc, bd] = [c, d] \oplus [a, b],$$
$$[a, b] \oplus ([c, d] \oplus [e, f]) = [a, b] \oplus [cf + de, df] = [adf + bcf + bde, bdf],$$
$$([a, b] \oplus [c, d]) \oplus [e, f] = [ad + bc, bd] \oplus [e, f] = [adf + bcf + bde, bdf],$$
$$[a, b] \odot [c, d] = [ac, bd] = [c, d] \odot [a, b],$$
$$[a, b] \odot ([c, d] \odot [e, f]) = [a, b] \odot [ce, df] = [ace, bdf],$$
$$([a, b] \odot [c, d]) \odot [e, f] = [ac, bd] \odot [e, f] = [ace, bdf].$$

5. We have

$$[a, b] \odot ([c, d] \oplus [e, f]) = [a, b] \odot [cf + de, df] = [acf + ade, bdf]$$

$$([a, b] \odot [c, d]) \oplus ([a, b] \odot [e, f]) = [ac, bd] \oplus [ae, bf] = [abcf + abde, b^2df] = [acf + ade, bdf].$$

6. Let $x = [a, b]$, $y = [c, d]$ and $z = [e, f]$. From $x \oplus y = x \oplus z$ we get $[ad + bc, bd] = [af + be, bf]$, so $[adf + bcf, bdf] = [adf + bde, bdf]$. From 1 we get

$adf + bcf = adf + bde$, hence by cancelation of integers, $cf = de$ and therefore $y = z$.

7. Let $x = [a, b]$ with $a \neq 0$, $y = [c, d]$ and $z = [e, f]$. From $x \odot y = x \odot z$ we get $[ac, bd] = [ae, bf]$, so $[acf, bdf] = [ade, bdf]$. From 1 it follows that $acf = ade$, hence $cf = de$ since $a \neq 0$ and therefore $y = z$.

8. For $x = [a, b]$, we can take $y = [-a, b]$, so such a y exists. If $a \oplus y = x \oplus y' = [0, 1]$, by cancellation we get $y = y'$, so y is unique. □

Definition 10.7. The rational number y such that $x \oplus y = [0, 1]$ is called the additive inverse or opposite of x and is denoted by $\ominus x$. We define the operation of subtraction on $\mathbb{Q}$ by $z \ominus x = z \oplus (\ominus x)$.

Theorem 10.8. *We have*

1. $\ominus[a, b] = [-a, b] = [a, -b]$.
2. $[a, b] \ominus [c, d] = [ad - bc, bd]$.
3. $[1, 1] \odot [a, b] = [a, b]$.
4. *For each* $x \in \mathbb{Q}$ *with* $x \neq [0, 1]$ *there is a unique* $y \in \mathbb{Q}$ *such that* $x \odot y = [1, 1]$.

Proof. Parts 1-3 follow from straightforward computation. For 4, let $x = [a, b]$ with $a \neq 0$. We can take $y = [b, a]$. Uniqueness follows from cancellation. □

Definition 10.9. The rational number y such that $x \odot y = [1, 1]$ is called the reciprocal or multiplicative inverse of x. It is denoted by x^{-1} or $1/x$. We define the operation of division on $\mathbb{Q}$ by $x \div y = x/y = x \odot y^{-1}$ for $y \neq 0$.

Theorem 10.10. *1. For* $[a, b] \in \mathbb{Q}$ *with* $a \neq 0$ *we have* $[a, b]^{-1} = [b, a]$.

2. For $c \neq 0$ *we have* $[a, b]/[c, d] = [ad, bc]$.

Proof. 1. This follows from the computation $[a, b] \odot [b, a] = [ab, ab] = [1, 1]$.

2. Indeed, $[a, b]/[c, d] = [a, b] \odot [c, d]^{-1} = [a, b] \odot [d, c] = [ad, bc]$. □

Definition 10.11. We say that $[a, b] \in \mathbb{Q}$ is positive if and only if $ab > 0$ and that $[a, b]$ is negative if and only if $ab < 0$. We write $x \succ y$ if and only if $x \ominus y$ is positive, and $x \prec y$ iff $y \succ x$.

Theorem 10.12. *We have*

1. $[a, b]$ *is positive iff* $[a, b] \succ [0, 1]$.
2. $[a, b]$ *is negative iff* $[-a, b]$ *is positive.*
3. *If* x *and* y *are positive, then* $x \odot y$ *and* $x \oplus y$ *are positive.*
4. *(Trichotomy) Exactly one of the following is true:* $x \prec y$, $y \prec x$, *or* $x = y$.
5. *(Transitivity)* $x \prec y$ *and* $y \prec z$ *implies* $x \prec z$.
6. $x \prec y \Rightarrow x \oplus z \prec y \oplus z$.
7. $(x \prec y) \wedge (z \prec w) \Rightarrow x \oplus z \prec y \oplus w$.
8. $([0, 1] \prec x) \wedge (y \prec z) \Rightarrow x \odot y \prec x \odot z$.

Proof. 1. Indeed, $[a, b] \ominus [0, 1] = [a, b]$ is positive iff $ab > 0$.

2. We have $ab < 0 \Leftrightarrow (-a)b > 0$.

3. Let $x = [a, b]$ and $y = [c, d]$ with $ab > 0, cd > 0$. Then $x \odot y = [ac, bd]$ and $acbd > 0$. Also, $x \oplus y = [ad + bc, bd]$ and $(ad + bc)bd = abd^2 + b^2cd > 0$.

4. Let $x \ominus y = [a, b] \in \mathbb{Q}$. Then we have either $ab = 0$ or $ab > 0$ or $ab < 0$. In the first case, $x = y$, in the second, $x \prec y$, and in the third, $y \prec x$.

5. If $y \ominus x = [a, b]$ and $z \ominus y = [c, d]$ are positive, then $z \ominus x = [a, b] \oplus [c, d]$ is also positive.

6. Assume $x \prec y$. We have $(y \oplus z) \ominus (x \oplus z) = y \ominus x$, which is positive, hence $x \oplus z \prec y \oplus z$.

7. Assume $x \prec y$ and $z \prec w$. Then $(y \oplus w) \ominus (x \oplus z) = (y \ominus x) \oplus (w \ominus z)$ is positive since $y \ominus x$ and $w \ominus z$ are.

8. Assume $[0, 1] \prec x$ and $y \prec z$. Then $(x \odot z) \ominus (x \odot y) = x \odot (z \ominus y)$ is positive, as the product of positives. □

Definition 10.13. We say that a pair $\langle a, b\rangle \in \mathbb{Z} \times \mathbb{Z}^*$ is in lowest terms iff $b > 0$ and $\gcd(a, b) = 1$.

Remark 10.14. Every nonzero rational number can be represented uniquely by a pair in lowest terms.

Proof. Let $x = [a, b]$ with $a \neq 0$ and $b > 0$. Let $d = \gcd(a, b)$ and let $a' = a/d, b' = b/d$. Then $[a, b] = [da', db'] = [a', b']$, where $b' > 0$ and $\gcd(a', b') = 1$. The numbers a', b' are unique. Indeed, let $[a'', b'']$ another representation of $[a, b]$ in lowest terms. Then $[a', b'] = [a'', b'']$ implies $a'b'' = a''b'$, hence $b' \mid a'b''$. Since $\gcd(a', b') = 1$, it follows from Lemma 7.42 that $b' \mid b''$. A similar argument shows that $b'' \mid b'$, hence $b' = b''$ because they are positive. We also get $a' = a''$, hence we got uniqueness. □

Theorem 10.15. *The subset* $W = \{[a, 1] : a \in \mathbb{Z}\} \subset \mathbb{Q}$ *is isomorphic with* $\mathbb{Z}$.

Proof. Define $f : \mathbb{Z} \to \mathbb{Q}, f(a) = [a, 1]$. Then f is one-to-one and onto, $f(a + b) = f(a) \oplus f(b), f(ab) = f(a) \otimes f(b)$ and $a < b \Rightarrow f(a) \prec f(b)$. □

From now on, we will write $+, -, \cdot, <, >$ instead of $\oplus, \ominus, \odot, \prec, \succ$. Also, a rational number $[a, b]$ will be denoted by $\dfrac{a}{b}$ or a/b. An integer k is identified with the rational number $[k, 1] = k/1$. The notation a/b for division of rational numbers is consistent with the case when a, b are integers.

Exercise 10.16. Is $f : \mathbb{Q} \to \mathbb{Z}, f([a, b]) = a - b$ a well defined function? (Hint: check if the formula depends on representatives).

Theorem 10.17. *Between any two distinct rational numbers there is another rational number.*

Proof. Suppose $r, s \in \mathbb{Q}$ with $r < s$ and consider $\dfrac{r + s}{2} \in \mathbb{Q}$. Then $r < \dfrac{r + s}{2} < s$ since $r + r < r + s < s + s$. □

Exercise 10.18. Prove that between two rational numbers there are infinitely many rationals.

Theorem 10.19. *(Archimedean Property) If* r, s *are positive rational numbers, then there is a positive integer* n *such that* $nr > s$.

Proof. Let $r = a/b, s = c/d$, where a, b, c, d are positive integers. For n an arbitrary positive integer, the inequality $nr > s$ is equivalent with $\frac{na}{b} > \frac{c}{d}$ or $nad > bc$. We may pick $n = 2bc$ and the inequality is satisfied since $ad \geq 1$. □

Definition 10.20. The absolute value of a rational number is defined as

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

Exercise 10.21. For $x, y \in \mathbb{Q}$ we have the properties:

a. $|x| \geq 0$ and $|x| = \max(x, -x)$.

b. $|x + y| \leq |x| + |y|$.

c. $|xy| = |x||y|$.

d. $\big||x| - |y|\big| \leq |x - y|$.

Remark 10.22. If we repeat the construction of rationals using pairs of rationals instead of pairs of integers, we get back the rationals.

We summarize the properties of the rational numbers by saying that $(\mathbb{Q}, +, \cdot, <)$ is an ordered field with the Archimedean property, containing the set of integers $\mathbb{Z}$. Since the equation $x^2 = 2$ has no rational solution, the field $\mathbb{Q}$ is not complete. It is riddled with "holes“ that will be filled by constructing the field of real numbers.

10.2. Decimal representation of rational numbers

A decimal fraction is a rational number of the form $\frac{a}{10^n}$ where $a \in \mathbb{Z}$ and $n \geq 1$. For example, $\frac{-7}{10^3}$ is a decimal fraction equal to -0.007. You must be familiar with decimal numbers, say from a pocket calculator.

Each rational number $\frac{a}{b}$ can be represented as a decimal number with finitely many nonzero decimals or with repeating decimals. For example

$$\frac{1}{2} = \frac{5}{10} = 0.5, \quad \frac{5}{6} = 0.8333... = \frac{8}{10} + \frac{3}{10^2} + \frac{3}{10^3} + \cdots = 0.8\bar{3},$$

$$-\frac{2}{7} = -0.285714285714... = \frac{-2}{10} + \frac{-8}{10^2} + \frac{-5}{10^3} + \frac{-7}{10^4} + \frac{-1}{10^5} + \frac{-4}{10^6} + \cdots = -0.\overline{285714}.$$

We overline the group of repeating decimals. The trailing zeros are omitted. The decimal representation is not unique, for example

$$\frac{1}{5} = 0.2 = 0.19999... = 0.1\bar{9}.$$

If we avoid repeated nines, then it is unique. In fact, the following is true.

Theorem 10.23. *Any rational number in lowest terms such that the only prime factors of the denominator are* 2 *and/or* 5 *can be expressed as a decimal fraction and has a finite decimal representation. Any rational number in lowest terms such that its denominator has prime factors other than* 2 *and* 5 *has a unique infinite periodic decimal representation and the period starts right after the decimal point. If the denominator has prime factors* 2 *or* 5 *and other primes, then it has a unique* *infinite periodic decimal representation where the period starts later. In the last two cases, we exclude repeated nines.*

Proof. Of course, the integers have no nonzero decimals (we exclude the repeated nines), so we assume that we deal with rational numbers which are not integers. Suppose $\frac{a}{b}$ is in lowest terms and the only prime factors of b are 2 and 5, say $b = 2^m 5^n$. If $m = n$, then we are done, since $\frac{a}{b} = \frac{a}{10^n}$. If $m < n$, then by multiplying both the numerator and the denominator of $\frac{a}{b}$ by 2^{n-m}, we get $\frac{a}{b} = \frac{2^{n-m}a}{10^n}$. Similarly, if $m > n$, then $\frac{a}{b} = \frac{5^{m-n}}{10^m}$.

Suppose now that $\frac{a}{b}$ is in lowest terms and that b is not divisible by 2 or by 5. We may assume $0 < a < b$. The decimals are obtained by the long division algorithm,

$$a = b \cdot 0 + a, \;\; 10a = b \cdot q_1 + r_1, \;\; 10r_1 = b \cdot q_2 + r_2, ...$$

Since there are at most $b-1$ possible remainders, the first remainder a will reappear after at most $b-1$ steps, forcing the decimals to repeat from that step on. The length of the period is at most $b-1$.

Finally, if $\frac{a}{b}$ is in lowest terms and b has prime factors 2 and/or 5 together with other primes, then $b = 2^m 5^n b'$ where b' is not divisible by 2 or by 5. If $m \leq n$ and $n \geq 1$, then $10^n \frac{a}{b} = \frac{a'}{b'}$ with a', b' relatively prime, and as above $\frac{a'}{b'}$ is a periodic decimal number. To get back $\frac{a}{b}$, we divide by 10^n. This amounts to a shift of the decimal point, obtaining a decimal number where the period starts n digits after the decimal point. The case $m > n$ is similar. □

Remark 10.24. We can use any base $b \geq 2$ to express rational numbers as a finite or infinite sum of fractions of the form $\frac{a_n}{b^n}$, where the prime factors of b play a similar role as 2 and 5 in the case $b = 10$.

Example 10.25. We can express $\frac{2}{7}$ as an infinite sum of fractions of the form $\frac{a_n}{9^n}$, using the base $b = 9 = 3 \cdot 3$. Indeed,

$$\frac{2}{7} = \frac{2}{9} + \frac{5}{9^2} + \frac{1}{9^3} + \frac{2}{9^4} + \frac{5}{9^5} + \frac{1}{9^6} + \cdots .$$

Here the period $\overline{251}$ starts right away since 7 is not divisible by 3.

Exercise 10.26. Express $\frac{4}{21}$ as a sum of fractions of the form $\frac{a_n}{9^n}$.

Chapter 11

The construction of real numbers

Though they are structurally the most complicated of all number systems, examples of real numbers were discovered quite early in the mathematical game. In fact, the existence of $\sqrt{2}$ is implied by the Pythagorean Theorem, which has been known for well over two thousand years. We already proved that $\sqrt{2}$ is not rational. In the decimal representation, $\sqrt{2} = 1.41421356237...$ you notice no periodicity, no matter how far you may go. The same will happen for the decimal representation of the number π, the length of a circle of radius $1/2$. The fact that π is irrational is more difficult to prove. In fact, an irrational number can be thought as an infinite decimal number with no periodicity. We will make this more precise later.

Our first approach to the development of Real Number theory is based on ideas first propounded by the German mathematician R. Dedekind more than a hundred years ago, called *Dedekind cuts.* The idea of a cut is to split the rational numbers in two halves whenever there is a "hole". Even though it is strongly related to the order relation, it has certain advantages over our second approach using Cauchy sequences. First, it allows us to construct a specific set of objects and define operations and relations that match our intuitive ideas of how real numbers work. Second, and perhaps even more important, it gives the student a lot of practice in working with inequalities and quantifiers. This experience is almost vital to one who wishes to really understand mathematics. On the other hand, the *Cauchy sequences* approach has the advantage that it can be used in other situations, a process called *completion.*

As before, we begin with a specific system of numbers, in this case the rational numbers, and construct a new system from it. We will freely use any known properties of rationals as we try to prove theorems about reals. We denote by $\mathbb{Q}^+$ the set of positive rational numbers, and by $\mathbb{Q}^-$ the set of negative rational numbers.

11.1. Dedekind cuts approach

There is an intuitive idea underlying the notion of a real number, namely, that each real number is uniquely determined by its position relative to the rational numbers. In other words, if we are given a number and we know exactly which rationals are less than it, then the number is not only known, it can be calculated to an arbitrary degree of precision using rational approximations. Thus, in order to define certain objects which will eventually be called real numbers, we shall begin by considering sets of rationals that, in effect, can be thought of as consisting of all rationals "to the left of" somewhere. Of course, we could choose to talk about all rational numbers "to the right of somewhere", but the situation would be perfectly symmetric. These sets of rationals will be called *cuts*, and their formal definition is below.

In this chapter, unless specifically stated otherwise, capital letters such as A, B, C, and so forth will always stand for cuts. Also lowercase letters x, y, z, p, q, r, s, etc., will generally refer to rational numbers.

Definition 11.1. Suppose $C \subseteq \mathbb{Q}$. We say that C is a *Dedekind cut* if and only if:

1. $C \neq \emptyset$,
2. $C \neq \mathbb{Q}$,
3. $x \in C \Rightarrow \exists y \in C$ with $x < y$,
4. $x \in C$ and $y \in \mathbb{Q}$ with $y < x$ implies $y \in C$.

If C is a cut, then we know four things about C. It contains at least one rational number, because it is non-empty. The fact that C is not equal to the entire set $\mathbb{Q}$ guarantees that there is at least one rational number which is not in C. Condition 3 asserts that C contains no largest member, for no matter what element of C we might choose, there always exists another number in C which is greater. Finally, if x is known to be in C, then every number less than x is also in C.

On the other hand, if we wish to prove that a certain set is a cut, we must establish that all four of the listed criteria are satisfied for the set. This means, for example, that to verify property 1 we must actually describe a rational number in the set or else show that the assumption "the set is empty" leads to a contradiction.

Example 11.2. Let $C = \{x \in \mathbb{Q} : x < 7\}$. We claim that C is a cut.

Proof. To back up the claim we provide a proof in four parts.

1. We need to show that C is non-empty, and this can be done simply by taking a wild guess and checking that the guess is correct. Since $3 < 7$, we see by definition that $3 \in C$. Thus $C \neq \emptyset$. There is nothing special about 3. If we had selected -387, $17/16$, or any other definite rational number less than 7 we would have drawn the same conclusion.

2. In a similar way, as soon as we note that, for example, $8 \notin C$, we have proved that $C \neq \mathbb{Q}$.

3. Since this property is phrased as a conditional, we must begin by examining some arbitrary but definite element of C. Suppose $x \in C$. Then $x < 7$. How can we find something in C which is greater than x? Here, of course, we cannot write down a definite number value since we don't know exactly what x is. But we can do the next best thing. We can write a formula in terms of x which will always generate a number of the desired sort. Recalling that the arithmetic mean of two numbers lies between them is helpful here. In fact, suppose we let $y = \frac{x+7}{2}$. Then certainly $x < y$ and $y < 7$. The second of these inequalities tells us that $y \in C$, while the first one gives us the rest of the existential statement to be proved.

4. Suppose $x \in C$, $y \in \mathbb{Q}$, and $y < x$. By the definition of C, we have $x < 7$, so by transitivity it is also true that $y < 7$. Hence $y \in C$. □

The argument given above can obviously be modified to apply to any similar type of sets of the form $\{y \in \mathbb{Q} : y < r\}$.

Corollary 11.3. For each $r \in \mathbb{Q}$, the set $\{y \in \mathbb{Q} : y < r\}$ is a cut.

Definition 11.4. For each $r \in \mathbb{Q}$, we define the cut $\hat{r} = \{y \in \mathbb{Q} : y < r\}$.

Exercise 11.5. Show that $C = \{x \in \mathbb{Q} : x \geq 1\}$ is not a cut.

The following example is a different type of cut.

Example 11.6. The set

$$D = \{x \in \mathbb{Q}^+ : x^2 < 2\} \cup \{x \in \mathbb{Q} : x \leq 0\}$$

is a cut.

Proof. 1. Since $0 \in D$, D is nonempty.

2. For example $2 \notin D$ since $2^2 = 4 > 2$, hence $D \neq \mathbb{Q}$.

3. Let $x \in D$ and let us find $y \in D$ with $x < y$. If $x \leq 0$, we can take $y = 1$. Let $x > 0$ with $x^2 < 2$ and consider $y = x + \dfrac{2 - x^2}{x + 2} = \dfrac{2x + 2}{x + 2}$. It is clear that $y \in \mathbb{Q}$ and that $y > x$. An easy computation shows that $y^2 - 2 = \dfrac{2x^2 - 4}{(x + 2)^2} < 0$, hence $y \in D$.

4. If $x \in D$ and $r < x$, then there are two cases: $r > 0$ or $r \leq 0$. In the first case, $x > 0$ and $r^2 < x^2 < 2$, so $r \in D$. In the second case clearly $r \in D$.

□

Definition 11.7. If C and D are cuts, then we write $C \prec D$ iff $C \subset D$ (strict inclusion). Also, we write $C \preceq D$ if $C \prec D$ or $C = D$.

Remark 11.8. 1. If $x \notin C$ then for all $y \in C$ we have $y < x$.

2. For all cuts C and D, exactly one of the following is true: $C \prec D, C = D, D \prec C$.

3. $(C \prec D) \wedge (D \prec E) \Rightarrow C \prec E$.

4. $C \prec D \Rightarrow \exists B$ with $C \prec B \prec D$.

Proof. 1. Suppose the conclusion is false. Then there is a $y \in C$ such that $x \leq y$. But $x < y$ is false by part 4 of the definition of a cut and $x = y$ is false since $x \notin C$. Either way we have a contradiction.

Parts 2 and 3 follow from the properties of set inclusion.

4. By hypothesis, there is an r in D such that $r \notin C$. Use property 3 of a cut to find an element r' of D such that $r < r'$. We claim that $C \prec \hat{r'} \prec D$, which means that we may take $B = \hat{r'}$. Indeed, since $r < r'$, we clearly have $r \in \hat{r'}$. This, together with the fact that $r \notin C$, tells us that $C \prec \hat{r'}$. Let $r'' \in D$ such that $r' < r''$. Then clearly $r'' \notin \hat{r'}$, so by definition $\hat{r'} \prec D$.

Note that the second part of the previous proof could be made easier by observing that r' itself is not an element of $\hat{r'}$. □

Definition 11.9. A cut C is positive if $\exists r \in \mathbb{Q}^+$ with $r \in C$. A cut C is negative if $\exists r \in \mathbb{Q}^-$ with $r \notin C$.

Theorem 11.10. *If C is a cut, then exactly one of the following is true:*

C is positive, C is negative, or $C = \hat{0}$.

Proof. Suppose $C \neq \hat{0}$. If there is $r \in \mathbb{Q}^+$ with $r \in C$, then C is positive. If C does not contain any positive rational, it must be made only of negative irrationals. Since $C \neq \hat{0}$, we can find $r \in \mathbb{Q}^-$ with $r \notin C$, hence C is negative. □

Exercise 11.11. Prove the following

a. If C is a cut, then C is positive if and only if $0 \in C$.

b. If C is a positive cut and D is a negative cut, then $D \prec C$.

c. If C is a negative cut and $D \prec C$, then D is a negative cut.

d. $C \prec \hat{0}$ if and only if C is a negative cut.

We want to define the operation of addition for cuts. To find the sum of the cuts $\hat{r}$ and $\hat{s}$, we can just take $\widehat{r+s}$, but since there are other types of cuts, this idea will not suffice.

Definition 11.12. Given cuts C, D, define their sum by

$$C + D = \{x + y : x \in C \text{ and } y \in D\}.$$

Theorem 11.13. *If C and D are cuts, then $C + D$ is a cut.*

Proof. Naturally, there are four parts to the proof because there are four separate properties we need to establish.

1. By property 1 of cuts, there is an x in C and there is a y in D. Thus $x + y \in C + D$, so $C + D$ is not empty.

2. Let $u \notin C$ and $v \notin D$. Suppose $x \in C$ and $y \in D$. We have $x < u$ and $y < v$. Thus, by adding the inequalities, $x + y < u + v$. This shows that the rational number $u + v$ is not in $C + D$, because it is not equal to any element of that set.

3. Suppose $z \in C + D$. Then there exist $x \in C$ and $y \in D$ such that $z = x + y$. By property 3 of cuts, there is a $y' \in D$ for which $y < y'$. By adding x to both sides

of this inequality we obtain $x + y < x + y'$. Since $x + y' \in C + D$ and $z < x + y'$, we have determined an element of $C + D$ which is larger than z.

4. Consider an arbitrary member of $C + D$. It has the form $x + y$, for some $x \in C$ and $y \in D$. If $r < x + y$, then certainly $r - x < y$. Hence $r - x \in D$ by property 4 of cuts. But $r = x + (r - x)$, so r is an element of $C + D$. □

Theorem 11.14. *We have*

1. *Addition of cuts is commutative and associative.*
2. *For any cut C, $C + \hat{0} = C$.*

Proof. Part 1 follows from the corresponding properties of rational numbers. For part 2, let $c \in C$ and $z \in \hat{0}$. Then $c + z < c + 0 = c$, hence $C + \hat{0} \subseteq C$. For the other inclusion, let $c \in C$ and choose $d \in C$ with $c < d$. Then $c - d \in \hat{0}$ and $c = d + (c - d) \in C + \hat{0}$. □

Definition 11.15. If C is a cut, define $-C = \{x \in \mathbb{Q} : x + c < 0 \text{ for all } c \in C\}$.

Remark 11.16. We could also define $-C$ as $-C = \{x \in \mathbb{Q} : x < -y \text{ for some } y \notin C\}$. Notice that $-C$ is not the set $\{-c : c \in C\}$.

Lemma 11.17. *Let $r > 0$ be rational and let C be a cut. Then there are $y \in C$ and $z \notin C$ such that $z - y = r$.*

Proof. Let $x \in C$. By the Archimedean property there is a smallest positive integer n such that $x + nr \notin C$. Let $z = x + nr$ and $y = x + (n - 1)r$. Then $y \in C$ and $z - y = r$. □

Theorem 11.18. *We have the following*

1. *If C is a cut, then $-C$ is a cut and $C + (-C) = \hat{0}$.*
2. *If C is a positive cut, then $-C$ is a negative cut.*
3. *If C is a negative cut, then $-C$ is a positive cut.*
4. *$C + D = C + E \Rightarrow D = E$.*

Proof. 1. First we show that $-C$ is a cut, by verifying the four defining properties. If $x > c$ for all $c \in C$, then $-x \in -C$, hence $-C$ is not empty. Given $c \in C$ we have $-c \notin -C$ since $(-c) + c = 0 \geq 0$, hence $-C \neq \mathbb{Q}$. Given $x \in -C$ let us find $y \in -C$ with $x < y$. We have $x + c < 0$ for all $c \in C$. Fixing $c \in C$ arbitrary, let $d \in \mathbb{Q}^+$ with $c + d \in C$. Then $x + d + c < 0$, hence $y = x + d \in -C$ and $x < x + d$. Finally, if $x \in -C$ and $y \in \mathbb{Q}$ with $y < x$, we have $y + c < x + c < 0$ for all $c \in C$, hence $y \in -C$.

By definition, $C + (-C) \subseteq \hat{0}$. If $z \in \hat{0}$, then by lemma 11.17 there is $c \in C$ with $c - z \notin C$. Then $z - c \in -C$ and $z = c + (z - c)$ hence $\hat{0} \subseteq C + (-C)$ and we have equality.

2. Let $r \in C$ with $r > 0$. Then $-r < 0$ and $-r \notin -C$, hence $-C$ is negative.

Parts 3 and 4 are left as exercise.

□

We now define the operation of multiplication.

Definition 11.19. If C and D are positive cuts, we define their product by

$$C \cdot D = \{x \in \mathbb{Q} : x \leq c \cdot d \text{ for some positive } c \in C, d \in D\}.$$

If $C = \hat{0}$ or $D = \hat{0}$, then we define $C \cdot D = \hat{0}$;
if $C \succ \hat{0}$ and $D \prec \hat{0}$, then we define $C \cdot D = -(C \cdot (-D))$;
if $C \prec \hat{0}$ and $D \succ \hat{0}$, then we define $C \cdot D = -((-C) \cdot D)$;
if $C \prec \hat{0}$ and $D \prec \hat{0}$, then we define $C \cdot D = (-C) \cdot (-D)$.

Exercise 11.20. Prove that for $r, s \in \mathbb{Q}$ we have $\hat{r} \cdot \hat{s} = \widehat{rs}$.

Exercise 11.21. Prove that for the cut D in Example 11.6 we have $D \cdot D = \hat{2}$.

Theorem 11.22. *We have*

1. *The product of two positive cuts is a positive cut.*
2. *Multiplication of cuts is commutative and associative.*
3. *Multiplication is distributive over addition of cuts.*
4. *If C is a cut, then $C \cdot \hat{1} = C$.*

Proof. 1. To show that $C \cdot D$ is a cut, first observe that $C \cdot D$ is not empty and not equal to $\mathbb{Q}$. Also, given $x \in C \cdot D$, there are $c \in C$ and $d \in D$ positive with $x \leq c \cdot d$. Let $c' > 0$ with $c + c' \in C$. Then $x + c'd \leq (c + c') \cdot d$, hence $x + c'd \in C \cdot D$ and $x < x + c'd$. The fourth property is obvious. To show that $C \cdot D$ is positive, observe that for $c \in C$ and $d \in D$ positive, $c \cdot d$ is positive and $c \cdot d \in C \cdot D$.

2. For positive cuts, $C \cdot D = D \cdot C$ and $C \cdot (D \cdot E) = (C \cdot D) \cdot E$ by definition and the properties of multiplication of rational numbers. If for example $C \succ \hat{0}$, $D \prec \hat{0}$ and $E \prec \hat{0}$, then $C \cdot D = -(C \cdot (-D))$ and $D \cdot C = -((-D) \cdot C)$, hence $C \cdot D = D \cdot C$. Also $C \cdot (D \cdot E) = C \cdot ((-D) \cdot (-E)) = (C \cdot (-D)) \cdot (-E)$ and $(C \cdot D) \cdot E = (-(C \cdot (-D))) \cdot E = (C \cdot (-D)) \cdot (-E)$, hence $C \cdot (D \cdot E) = (C \cdot D) \cdot E$. The other cases are treated similarly.

3. Let us show that $C \cdot (D + E) = C \cdot D + C \cdot E$ for positive cuts. Let $x \in C \cdot (D + E)$. Then $x \leq c \cdot (d + e)$ for some positive $c \in C, d \in D, e \in E$. We get $x \leq c \cdot d + c \cdot e$ with $c \cdot d \in C \cdot D, c \cdot e \in C \cdot E$, hence $x \in C \cdot D + C \cdot E$. Conversely, let $x \in C \cdot D + C \cdot E$. Then $x = y + z$ with $y \in C \cdot D$, $z \in C \cdot E$, so $y \leq c_1 \cdot d$ and $z \leq c_2 \cdot e$ for positive $c_1, c_2 \in C, d \in D, e \in E$. Let $c = \max(c_1, c_2)$. Then $x \leq c \cdot d + c \cdot e = c \cdot (d + e)$, hence $x \in C \cdot (D + E)$.

If for example $C \succ \hat{0}, D \prec \hat{0}$ and $D + E \succ \hat{0}$, then $E = (D + E) + (-D)$. We get $C \cdot E = C \cdot (D + E) + C \cdot (-D) = C \cdot (D + E) - C \cdot D$, hence $C \cdot D + C \cdot E = C \cdot (D + E)$. The other cases are similar.

4. It suffices to consider the case $C \succ \hat{0}$. Let $x \in C \cdot \hat{1}$. Then $x \leq y \cdot z$ for some positive $y \in C$ and $z \in \hat{1}$. Since $z < 1$, we get $y \cdot z < y$ and $x < y$, so $x \in C$ by the properties of cuts. Conversely, let $x \in C$. Consider $y \in C$ positive with $y > x$. Then $x = y \cdot \frac{x}{y}$ with $\frac{x}{y} \in \hat{1}$, hence $x \in C \cdot \hat{1}$. □

Definition 11.23. If C is a positive cut, define

$$C^{-1} = \{y \in \mathbb{Q} : y < \frac{1}{x} \text{ for some } x \notin C\}.$$

Lemma 11.24. *If C is a positive cut, then C^{-1} is a positive cut.*

Proof. To show that C^{-1} is a cut, we follow the four steps:

1) By definition, there is an $x \notin C$. Since $C \succ \hat{0}$, we have $x > 0$. Since $x+1 > x$, we have $\frac{1}{x+1} < \frac{1}{x}$, so $\frac{1}{x+1} \in C^{-1}$ and $\frac{1}{x+1} > 0$. Thus $C^{-1} \neq \emptyset$ and it contains a positive element.

2) Let $y \in C$ such that $y > 0$. Then $\frac{1}{y} \notin C^{-1}$. Indeed, if $\frac{1}{y} \in C^{-1}$, then $\frac{1}{y} < \frac{1}{z}$ for some $z \notin C$. But then $z < y$, and hence $z \in C$, contradiction.

3) Let $x \in C^{-1}$. Then $x < \frac{1}{y}$ for some $y \notin C$. Take $x' \in \mathbb{Q}$ with $x < x' < \frac{1}{y}$, for example their average. Since, in particular, $x' < \frac{1}{y}$, we have $x' \in C^{-1}$.

4) If $x \in C^{-1}$ and $r < x$, then $x < \frac{1}{y}$ for some $y \notin C$. By transitivity, $r < \frac{1}{y}$, so $r \in C^{-1}$.

Since C^{-1} contains the positive element $\frac{1}{x+1}$, it is a positive cut. □

Theorem 11.25. *If C is a positive cut, then $C \cdot C^{-1} = \hat{1}$.*

Proof. Since both $C \cdot C^{-1}$ and $\hat{1}$ contain all rationals less or equal to 0, it suffices to show that they contain the same positive rationals. Suppose $t \in C \cdot C^{-1}$ and $t > 0$. Then for some positive $x \in C$ and $y \in C^{-1}$ we have $t \leq x \cdot y$. Since $y < 1/z$ for some $z \notin C$, we get $z > x$. Taking reciprocals yields $1/z < 1/x$, which implies $y < 1/x$. Hence $x \cdot y < 1$, so, since $t \leq x \cdot y$, clearly $t \in \hat{1}$. We get $C \cdot C^{-1} \subseteq \hat{1}$.

On the other hand, if $x \in \hat{1}$, with $x > 0$, we can select an $a \in C$ such that $a > 0$ and by lemma 11.17 (with $r = a(1-x)$) we can find $y \in C$ and $z \notin C$ such that $z - y = a(1-x)$. Since $a \in C$, we have $a < z$, so $a(1-x) < z(1-x)$ since $1 - x > 0$. We obtain $z - y < z(1-x)$, hence $z - y < z - zx$, $-y < -zx$, $y > zx$, and therefore $y/x > z$. Thus $x/y < 1/z$, so $x/y \in C^{-1}$. Since $x = y \cdot \frac{x}{y}$ with $y \in C$, we get $x \in C \cdot C^{-1}$, so $\hat{1} \subseteq C \cdot C^{-1}$. □

Corollary 11.26. If C, D, and E are positive cuts, and $C \cdot D = C \cdot E$, then $D = E$.

If C is a positive cut, then $(C^{-1})^{-1} = C$.

If D is a positive cut and $C \succ \hat{1}$, then $C \cdot D \succ D$.

Proof. We prove the last part. Suppose $C \cdot D$ is not greater than D. By trichotomy, either $C \cdot D = D$ or $C \cdot D \prec D$.

Case 1) If $C \cdot D = D$, then $C \cdot D \cdot D^{-1} = D \cdot D^{-1}$. This implies that $C \cdot \hat{1} = \hat{1}$, hence $C = \hat{1}$, contradiction.

Case 2) Suppose $C \cdot D \prec D$. Then there is an $x \in D$ such that $x \notin C \cdot D$. Clearly $x > 0$, since $C \cdot D$ is positive. But since $1 \in C$, we have $1 \cdot x \in C \cdot D$, contradiction.

Here is another proof of the same statement. Suppose $x \in D$. Then $1 \cdot x = x \in C \cdot D$, because $1 \in C$. Thus $D \subseteq C \cdot D$, so $D \preceq C \cdot D$. If equality held, we could multiply both sides by D^{-1} and obtain $\hat{1} = C$, an obvious contradiction. □

Theorem 11.27. *If $x > 1$ and $x \in C$, then $C^{-1} \prec \hat{1}$.*

Proof. Since $x \in C$ and $x > 0$, we have $1/x \notin C^{-1}$. But since $x > 1$, it follows that $1/x < 1$, so $1/x \in \hat{1}$. By definition, $C^{-1} \prec \hat{1}$. □

Definition 11.28. The absolute value of a cut is defined as $|C| = \max(C, -C)$.

Definition 11.29. If C is a negative cut, then we define $C^{-1} = -(-C)^{-1}$.

Theorem 11.30. *1. Given $C \neq \hat{0}$ we have $C \cdot C^{-1} = \hat{1}$.*

2. If $A + C = B$ and C is a positive cut, then $A \prec B$.

3. $A \prec B \Leftrightarrow A + C \prec B + C$.

4. If $C \prec D$ and E is positive, then $C \cdot E \prec D \cdot E$.

Proof. 4. Let $p \in D \setminus C$ and let $q \in D$ with $q > p$. For $c \in E$ positive, set $c_n = c\dfrac{q^{n-1}}{p^{n-1}}$. Consider m the positive integer such that $c_m \in E$ and $c_{m+1} \notin E$. We have $pc_{m+1} = qc_m$. Moreover, $pc_{m+1} > uv$ for all $u \in C$ and $v \in E$ and $pc_{m+1} \notin C \cdot E$. We found $qc_m \in C \cdot E \setminus C \cdot D$, hence $C \cdot E \prec D \cdot E$. □

Definition 11.31. Each Dedekind cut will be called a *real number*. The set of real numbers will be denoted by $\mathbb{R}$.

Theorem 11.32. *If $S = \{\hat{r} : r \in \mathbb{Q}\} \subseteq \mathbb{R}$, then $\mathbb{Q}$ is isomorphic with S. In particular the set of rational numbers $\mathbb{Q}$ can be viewed as a subset of $\mathbb{R}$.*

Proof. Define $f : \mathbb{Q} \to S, f(r) = \hat{r}$. Then f is one-to-one and onto, $f(r+s) = f(r) + f(s)$, $f(rs) = f(r) \cdot f(s)$ and $r < s \Rightarrow f(r) \prec f(s)$. □

As a result, we shall feel free to make the same simplifying conventions as before. In other words r and $\hat{r}$ will be regarded as the same for each rational number r.

Theorem 11.33. *Suppose that C_i is a cut for each $i \in I \neq \emptyset$. If $C = \bigcup_{i \in I} C_i$ and $C \neq \mathbb{Q}$, then C is a cut.*

Proof. Clearly C is not empty and $C \neq \mathbb{Q}$ by hypothesis. Let $x \in C$. There is $i_0 \in I$ with $x \in C_{i_0}$. Since C_{i_0} is a cut, there is $y \in C_{i_0}$ with $x < y$. But then $y \in C$ and $x < y$. If $r < x$, then $r \in C_{i_0}$, hence $r \in C$. □

Suppose $S \subseteq \mathbb{R}$ is a set of real numbers. Recall that

A real number a is an *upper bound* for S iff $a \geq x$ for all $x \in S$.

A real number a is a *lower bound* for S iff $a \leq x$ for all $x \in S$.

A real number a is a *least upper bound* or *supremum* for S iff a is an upper bound for S and $t < a \Rightarrow \exists x \in S$ with $t < x$).

A real number a is a *greatest lower bound* or *infimum* for S iff a is a lower bound for S and $t > a \Rightarrow \exists x \in S$ with $x < t$.

Corollary 11.34. 1. If S is a nonempty subset of $\mathbb{R}$ that has an upper bound, then S has a least upper bound.

2. If S is a nonempty subset of $\mathbb{R}$ that has a lower bound, then S has a greatest lower bound.

Proof. Let $T = \bigcup_{C \in S} C$. Then T is a cut and it is an upper bound for S. To show that T is the least upper bound, let $U \prec T$, hence there is $q \in T \setminus U$. By definition, there is $C \in S$ with $q \in C$, hence $C \succ U$ and U cannot be an upper bound for S. Hence T is the least upper bound of S.

2. We use $\text{glb}S = -\text{lub}(-S)$, where $-S = \{-s : s \in S\}$. We leave the proof as an exercise. □

Remark 11.35. The above property of $\mathbb{R}$ is called the *least upper bound property.* The set $\mathbb{Q}$ does not have this property. Indeed, the set $\{x \in \mathbb{Q}^+ : x^2 < 2\}$ has no least upper bound in $\mathbb{Q}$, since $\sqrt{2}$ is irrational.

We summarize the properties of the set of real numbers in the following

Theorem 11.36. *The set $\mathbb{R}$ with the addition and multiplication operations and with the order defined above contains a copy of $\mathbb{Q}$ and satisfies the properties*

1. $\mathbb{R}$ is closed under addition and multiplication.

2. Addition and multiplication are commutative and associative.

3. $\mathbb{R}$ contains 0 and $x + 0 = x \ \ \forall x \in \mathbb{R}$.

4. Each $x \in \mathbb{R}$ has an opposite $-x$ such that $x + (-x) = 0$.

5. $\mathbb{R}$ contains 1 such that $1 \neq 0$ and $x \cdot 1 = x \ \ \forall x \in \mathbb{R}$.

6. Any $x \in \mathbb{R} \setminus \{0\}$ has an inverse x^{-1} such that $x \cdot x^{-1} = 1$.

7. The multiplication is distributive over the addition.

8. We have $(x > 0) \wedge (y > 0) \Rightarrow (x + y > 0) \wedge (xy > 0)$ and for any $x \in \mathbb{R}$ exactly one is true: $x > 0, -x > 0$ or $x = 0$.

9. Any nonempty subset of $\mathbb{R}$ which has an upper bound has a least upper bound.

We say that $\mathbb{R}$ is an ordered field with the least upper bound property, or a *complete ordered field.*

Theorem 11.37. *The set of real numbers also has the properties*

1. (Archimedean property) If $x, y \in \mathbb{R}$ and $x > 0$, then there is a positive integer n such that $nx > y$.

2. If $x, y \in \mathbb{R}$ and $x < y$, then there is $r \in \mathbb{Q}$ such that $x < r < y$.

Proof. 1. Let $A = \{nx : n \in \mathbb{P}\}$. If the assertion is false, then y would be an upper bound for A. Let $\alpha = \sup A$. Since $x > 0$, we get $\alpha - x < \alpha$ and $\alpha - x$ is no longer an upper bound for A. Hence there is m with $\alpha - x < mx$, so $\alpha < (m + 1)x \in A$, contradiction.

2. Since $x < y$, we have $y - x > 0$ and from 1 we can find $n \in \mathbb{P}$ such that $n(y - x) > 1$. Similarly, we obtain positive integers m_1 and m_2 such that $m_1 > nx$ and $m_2 > -nx$. We get $-m_2 < nx < m_1$ and we can find an integer m such that $m - 1 \leq nx < m$. Combining the inequalities we get $nx < m \leq 1 + nx < ny$. Dividing by n we get $x < \dfrac{m}{n} < y$. □

It follows that $\mathbb{R}$ is a complete ordered field with the Archimedean property.

Exercise 11.38. Prove that between any two real numbers there is a rational and an irrational number.

Theorem 11.39. *For any real $x > 0$ and any positive integer n there is a unique real y such that $y^n = x$. We write $y = \sqrt[n]{x}$.*

Proof. Let A be the set of all positive real numbers t such that $t^n < x$. To prove that A is not empty, consider $t = \dfrac{x}{x+1}$. Then $0 < t < 1$ and $t^n < t < x$, hence $t \in A$. It is easy to see that $1 + x$ is an upper bound for A. We conclude that $y = \sup A$ exists. Let us prove that $y^n = x$.

Assume $y^n < x$. Choose h such that $0 < h < 1$ and $h < \dfrac{x - y^n}{n(y+1)^{n-1}}$. Then

$$(y+h)^n - y^n < hn(y+h)^{n-1} < hn(y+1)^{n-1} < x - y^n,$$

hence $(y+h)^n < x$ and $y+h \in A$, contradiction. Similarly, the assumption $y^n > x$ leads to a contradiction. We conclude that $y^n = x$. □

Remark 11.40. It can be proved that for $b > 1$ and $x \in \mathbb{R}$ there is a real number b^x such that for $x, y \in \mathbb{R}$ we have $b^{x+y} = b^x b^y$. Also, given $y > 0$ there is a unique real number x such that $b^x = y$. This is called the logarithm of y in base b, denoted $\log_b y$.

Exercise 11.41. Let $C = \{x \in \mathbb{Q} : x^3 < 5\}$. Prove that C is a cut. (Hint: Given $s \in C$, show that $t = \dfrac{15s}{s^3 + 10}$ belongs to C and that $s < t$.)

Exercise 11.42. Let C be a cut and let $s \in \mathbb{Q}$ such that $s > t$ for all $t \in C$. Prove that $s \notin C$.

Exercise 11.43. Prove that there is no rational number x such that $x^3 = 7$. Construct a real number x with this property.

Exercise 11.44. Prove that $\sqrt{2} + \sqrt{3} - \sqrt{5 + 2\sqrt{6}}$ is rational.

Remark 11.45. There are irrational numbers x, y such that x^y is rational. Indeed, consider $\sqrt{2}^{\sqrt{2}}$. If this is rational, take $x = y = \sqrt{2}$. If not, then

$$(\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = \sqrt{2}^2 = 2,$$

so we can take $x = \sqrt{2}^{\sqrt{2}}$ and $y = \sqrt{2}$.

11.2. Cauchy sequences approach

The set of real numbers can be constructed using equivalence classes of certain sequences of rational numbers. You may think of the real numbers as being limits of sequences of rational numbers. This is an analytic process and the proofs might be more involved, but the construction illustrates the more general concept of *completion*, which you may encounter later in Functional Analysis and other branches of mathematics.

Recall that a sequence in a set S is a function $x : \mathbb{N} \to S$. The element $x(n) \in S$ is denoted x_n. We also write a sequence as $x = (x_n)_{n \geq 0}$ or just (x_n). Sometimes a sequence (x_n) is defined only for $n \geq k$ for $k \in \mathbb{N}$. You have studied sequences and limits in Calculus. We will prove that the limit of a sequence of rational numbers is not necessarily a rational number. The real numbers, containing both rational and irrational numbers, are filling those gaps.

Definition 11.46. A *Cauchy sequence* of rational numbers is a sequence $x = (x_n)$ such that for every positive rational ε there is a positive integer N such that for every $m, n \geq N$ we have $|x_n - x_m| < \varepsilon$.

Note that this definition retains the flavor of the definition of the limit. Recall that $L = \lim\limits_{n\to\infty} x_n$ if for any $\varepsilon > 0$ there is n such that $|x_n - L| < \varepsilon$ for all $n \geq N$. However, we will see that a Cauchy sequence in $\mathbb{Q}$ is not necessarily convergent in $\mathbb{Q}$.

Example 11.47. Obviously, a constant sequence $r, r, r, ...$ is a Cauchy sequence. For any $r \in \mathbb{Q}$, denote by $\hat{r}$ the constant sequence $r, r, r, ...$

Example 11.48. Let $x_n = \frac{n+1}{n}$, $n \geq 1$. Then (x_n) is a Cauchy sequence. Indeed,

$$|x_n - x_m| = \left|\frac{m-n}{mn}\right| = \left|\frac{1}{n} - \frac{1}{m}\right| < \frac{1}{\min(m, n)}.$$

Given $\varepsilon > 0$, take $N = \lfloor 1/\varepsilon \rfloor + 1$. For $m, n \geq N$ we have

$$|x_n - x_m| < \frac{1}{N} < \varepsilon.$$

Example 11.49. The sequence such that $x_1 = 0, x_2 = 1$ and $x_n = \frac{1}{2}(x_{n-1} + x_{n-2})$ for $n \geq 3$ is a Cauchy sequence.

Proof. First, let's prove by induction that

$$x_{n+1} - x_n = \frac{(-1)^{n-1}}{2^{n-1}}, n \geq 1.$$

For $n = 1$, $x_2 - x_1 = 1 - 0 = 1 = \frac{(-1)^0}{2^0}$. Suppose $x_{k+1} - x_k = \frac{(-1)^{k-1}}{2^{k-1}}$ for a fixed $k \geq 1$. Then

$$x_{k+2} - x_{k+1} = \frac{1}{2}(x_{k+1} + x_k) - x_{k+1} = -\frac{1}{2}(x_{k+1} - x_k) = \frac{(-1)^k}{2^k}.$$

From the recurrence formula, it is clear that for $m > n$, x_m lies between x_n and x_{n+1}. Given a positive ε, choose N such that $2^{N-1} < 1/\varepsilon$. Then for all $m, n \geq N$,

$$|x_m - x_n| \leq |x_{n+1} - x_n| = \frac{1}{2^{n-1}} < \frac{1}{2^{N-1}} < \varepsilon.$$

□

Example 11.50. Let $x_1 = \dfrac{1}{2}, x_{n+1} = \dfrac{1}{2 + x_n}, n \geq 1$. Then (x_n) is a Cauchy sequence of rational numbers.

Proof. It is clear that $x_n \in \mathbb{Q}$ and $x_n > 0$ for all n. We compute

$$x_{n+1} - x_{n+2} = \frac{1}{2 + x_n} - \frac{1}{2 + x_{n+1}} = \frac{x_{n+1} - x_n}{(2 + x_n)(2 + x_{n+1})}.$$

Since $x_n > 0$, we get $(2+x_n)(2+x_{n+1}) > 4$ and therefore

$$|x_{n+1} - x_{n+2}| < \frac{1}{4}|x_n - x_{n+1}|$$

for all $n \geq 1$. By induction we can prove that $|x_n - x_{n+1}| < \frac{1}{4^{n-1}}$. Indeed,

$$|x_1 - x_2| = |\frac{1}{2} - \frac{2}{5}| = \frac{1}{10} < 1.$$

Assume $|x_k - x_{k+1}| < \frac{1}{4^{k-1}}$. Then

$$|x_{k+1} - x_{k+2}| < \frac{1}{4}|x_k - x_{k+1}| < \frac{1}{4^k}.$$

To prove that (x_n) is Cauchy, fix $\varepsilon > 0$ rational and choose N such that $\dfrac{1}{4^{N-1}} < \dfrac{3}{4}\varepsilon$. For $m > n \geq N$ we have

$$|x_m - x_n| \leq |x_m - x_{m-1}| + |x_{m-1} - x_{m-2}| + \cdots + |x_{n+1} - x_n| < \frac{1}{4^{m-2}} + \frac{1}{4^{m-3}} + \cdots + \frac{1}{4^{n-1}} =$$

$$\frac{1}{4^{n-1}}(1 + \frac{1}{4} + \cdots + \frac{1}{4^{m-n-1}}) = \frac{1}{4^{n-1}} \frac{1 - \frac{1}{4^{m-n}}}{1 - \frac{1}{4}} < \frac{4}{3}\frac{1}{4^{n-1}} < \frac{4}{3}\frac{1}{4^{N-1}} < \varepsilon.$$

For $n > m \geq N$ we similarly obtain $|x_m - x_n| < \varepsilon$, hence (x_n) is Cauchy. It can be proved that $\lim\limits_{n\to\infty} x_n = \sqrt{2} - 1$, an irrational number.

□

Exercise 11.51. Prove that the sequences x, y with

$$x_n = 1 - \frac{1}{3} + \frac{1}{5} - \cdots + \frac{(-1)^n}{2n+1}, \quad y_n = 1 + \frac{1}{1!} + \frac{1}{2!} + \cdots + \frac{1}{n!}$$

are Cauchy sequences of rational numbers.

Definition 11.52. We define addition and multiplication of sequences of rational numbers $x = (x_n)$ and $y = (y_n)$ by

$$x + y = u \text{ where } u_n = x_n + y_n; \quad xy = v \text{ where } v_n = x_n y_n.$$

Clearly, if x and y are sequences of rational numbers, then so are $x + y$ and xy.

Theorem 11.53. *If x and y are Cauchy sequences of rational numbers, then $x + y$ and xy are Cauchy sequences of rational numbers.*

Proof. . Let $\varepsilon > 0$. There exist N_1 and N_2 such that for all $m, n \geq N_1$ we have $|x_n - x_m| < \varepsilon/2$ and for all $m, n \geq N_2$ we have $|y_n - y_m| < \varepsilon/2$. Let $N = \max\{N_1, N_2\}$. For $m, n \geq N$ we have

$$|x_n + y_n - (x_m + y_m)| = |(x_n - x_m) + (y_n - y_m)| \leq |x_n - x_m| + |y_n - y_m| < \varepsilon/2 + \varepsilon/2 = \varepsilon.$$

For the product, we need to show first that a Cauchy sequence x is bounded, i.e. there exists a positive rational number α such that $|x_n| \leq \alpha$ for all n. Indeed, for $\varepsilon = 1$, there is N such that $|x_n - x_m| < 1$ for all $m, n \geq N$. Let

$$\alpha = \max\{|x_1|, |x_2|, \cdots, |x_N|\} + 1.$$

Clearly, for $n \leq N$ we have $|x_n| \leq \alpha$. For $n > N$ we have $|x_n - x_N| < 1$, hence $|x_n| \leq |x_n - x_N| + |x_N| \leq 1 + |x_N|$ and for all n we get $|x_n| \leq \alpha$.

Given $\varepsilon > 0$, there are α_1 and α_2 positive such that $|x_n| \le \alpha_1$ and $|y_n| \le \alpha_2$ for all n. There are integers N_1 and N_2 such that for all $m, n \ge N_1$ we have $|x_n - x_m| < \varepsilon/(2\alpha_2)$ and for all $m, n > N_2$ we have $|y_n - y_m| < \varepsilon/(2\alpha_1)$. Let $N = \max\{N_1, N_2\}$. For all $m, n \ge N$ we have

$$\begin{aligned}|x_n y_n - x_m y_m| &= |x_n y_n - x_m y_n + x_m y_n - x_m y_m| \le \\ &\le |y_n||x_n - x_m| + |x_m||y_n - y_m| < \\ &< \alpha_2 \frac{\varepsilon}{2\alpha_2} + \alpha_1 \frac{\varepsilon}{2\alpha_1} = \varepsilon.\end{aligned}$$

□

Theorem 11.54. *Addition and multiplication of Cauchy sequences are commutative and associative. Multiplication is distributive over addition. Each sequence x has an opposite $-x$, the sequence $\hat{0}$ satisfies $x + \hat{0} = x$ and the sequence $\hat{1}$ satisfies $x \cdot \hat{1} = x$.*

Proof. Exercise. □

Definition 11.55. We define the relation $\sim$ on the set of Cauchy sequences of rational numbers by $x \sim y$ iff for any positive rational number ε there is an integer N such that $|x_n - y_n| < \varepsilon$ for all $n \ge N$.

Example 11.56. Let $x_n = \dfrac{n+1}{n}$ and $y_n = 1$ for all n. Clearly, $x \sim y$ since $x_n - y_n = \dfrac{1}{n}$.

Theorem 11.57. *The relation $\sim$ is an equivalence relation.*

Proof. Indeed, it is reflexive since $x \sim x$ and it is symmetric since $x \sim y \Rightarrow y \sim x$. Let $x \sim y$ and $y \sim z$. Given $\varepsilon > 0$, there are N_1, N_2 such that $|x_n - y_n| < \varepsilon/2$ for $n \ge N_1$ and $|y_n - z_n| < \varepsilon/2$ for $n \ge N_2$. Let $N = \max\{N_1, N_2\}$. Then $|x_n - z_n| \le |x_n - y_n| + |y_n - z_n| \le \varepsilon/2 + \varepsilon/2 = \varepsilon$ for all $n \ge N$, hence $\sim$ is transitive. □

Definition 11.58. A Cauchy sequence $x = (x_n)$ is called *positive* iff there is $\varepsilon > 0$ and an integer N such that $x_n > \varepsilon$ for all $n \ge N$.

Lemma 11.59. *If x, y, u, v are Cauchy sequences in $\mathbb{Q}$ such that $x \sim u$ and $y \sim v$, then $x + y \sim u + v$ and $xy \sim uv$. Moreover, if x is positive, then u is positive.*

Proof. Exercise. □

Theorem 11.60. *1. The sum and the product of two positive Cauchy sequences are positive.*

2. If x is any Cauchy sequence, then exactly one of the following holds true: x is positive, $x \sim \hat{0}$, or $-x$ is positive.

3. If the Cauchy sequence x is not equivalent to $\hat{0}$, there is a Cauchy sequence z with $xz \sim \hat{1}$.

Proof. 1. Let x, y be positive Cauchy sequences. There are $\varepsilon_i > 0$ and integers N_i for $i = 1, 2$ such that $x_n > \varepsilon_1$ for $n \geq N_1$ and $y_n > \varepsilon_2$ for $n \geq N_2$. Then $x_n + y_n > \varepsilon_1 + \varepsilon_2$ and $x_n y_n > \varepsilon_1 \varepsilon_2$ for $n \geq \max\{N_1, N_2\}$.

2. If $x \nsim \hat{0}$, then there is $\varepsilon > 0$ such that for any integer N there is $n > N$ such that $|x_n| > \varepsilon$. Since x is Cauchy, there is N_1 such that $|x_n - x_m| < \varepsilon/2$ for $m, n \geq N_1$. In particular for $N = N_1$ there is $p > N_1$ such that $|x_p| > \varepsilon$. To make a choice, let $x_p > 0$, hence $x_p > \varepsilon$. We have $|x_n - x_p| < \varepsilon/2$ for all $n \geq p$, hence $x_n \geq x_p - \varepsilon/2 > \varepsilon - \varepsilon/2 = \varepsilon/2$ and x is positive. If $x_p < 0$ a similar argument shows that $-x$ is positive.

3. Since $x \nsim \hat{0}$, from 2 we get that there is a positive rational ε' and an integer N such that $|x_n| \geq \varepsilon'$ for all $n \geq N$. Consider x' such that $x'_n = \varepsilon'$ for $n < N$ and $x'_n = x_n$ for $n \geq N$. It is easy to show that x' is Cauchy and obviously $|x'_n| \geq \varepsilon'$ for all n. Define the sequence z such that $z_n = \frac{1}{x'_n}$. Given $\varepsilon > 0$, consider N such that $|x'_m - x'_n| < \varepsilon\varepsilon'^2$ for all $m, n \geq N$. Such an N exists since x' is Cauchy. Since $|x'_n| \geq \varepsilon'$ for all n, we have $\dfrac{1}{|x'_m x'_n|} \leq \dfrac{1}{\varepsilon'^2}$ for all m, n. We obtain

$$|z_m - z_n| = \Big|\frac{1}{x'_m} - \frac{1}{x'_n}\Big| = \frac{|x'_m - x'_n|}{|x'_m x'_n|} < \frac{\varepsilon\varepsilon'^2}{\varepsilon'^2} = \varepsilon$$

for all $m, n \geq N$, therefore z is Cauchy. It is clear that $zx' \sim \hat{1}$, and since $x' \sim x$ we conclude that $zx \sim \hat{1}$. □

Definition 11.61. A *real number* is an equivalence class $[x]$ of Cauchy sequences of rational numbers. We say that $[x]$ is positive iff it contains a positive Cauchy sequence. Define addition and multiplication by

$$[x] + [y] = [x + y], \ \ [x] \cdot [y] = [xy].$$

Define $[x] \prec [y]$ iff $[y] - [x]$ is positive.

Remark 11.62. There is a one-to-one function $f : \mathbb{Q} \to \mathbb{R}$ such that $f(r) = [\hat{r}]$ which preserves the order and the operations. This allows us to make an identification of $\mathbb{Q}$ with a subset of $\mathbb{R}$. From now on, we will use x instead of $[x]$, $x < y$ instead of $[x] \prec [y]$, 0 instead of $\hat{0}$ and 1 instead of $\hat{1}$. As usual, the absolute value function is defined as $|x| = \max(x, -x)$.

We summarize the properties of real numbers so far. The set $\mathbb{R}$ with the operations of addition and multiplication, 0, 1 and $<$ satisfy the following:

1) $x + (y + z) = (x + y) + z$.

2) $x + y = y + x$.

3) $0 + x = x$.

4) For each x there is z with $x + z = 0$.

5) $x(yz) = (xy)z$.

6) $xy = yx$.

7) $1 \cdot x = x$.

8) If $x \neq 0$, there exists z such that $xz = 1$.

9) $x(y + z) = xy + xz$.

10) $x, y > 0$ implies $x + y, xy > 0$.

11) Exactly one of $x > 0$, $x = 0$, $-x > 0$ holds.

Theorem 11.63. *Between any two distinct real numbers there is a rational number.*

Proof. Let $x < y$, and let a, b be Cauchy sequences of rational numbers representing x, y. Since $x < y$, we can find a rational ε and an integer N_1 such that $b_n - a_n > 4\varepsilon$ for all $n \geq N_1$. Since a, b are Cauchy sequences, there are N_2, N_3 such that $|a_n - a_m| < \varepsilon$ for $m, n \geq N_2$ and $|b_n - b_m| < \varepsilon$ for $m, n \geq N_2$. Let $N = \max\{N_1, N_2, N_3\} + 1$ and let $s = 3\varepsilon/2$. Consider $z = a_N + s$. We claim that $x < z < y$. Indeed, $a_n - a_N < \varepsilon$ for every $n \geq N$ and therefore $z - a_n = (a_N + s) - a_n > \varepsilon/2 > 0$, so $z - x > 0$. Similarly, $y - z > 0$. □

Theorem 11.64. *(Archimedean property). If x, y are positive real numbers, then there exists a positive integer n such that $nx > y$.*

Proof. Let b be a representative of y. Since Cauchy sequences of rational numbers are bounded, there is $\beta > 0$ such that $b_m \leq \beta$ for all m. Let $d = \hat{\beta}$. We have $y \leq d$. Since $x > 0$ we can find rational numbers s, t such that $0 < s < x$ and $y < t < d$. From the Archimedean property for rational numbers, there is a positive integer n such that $ns > t$. We get $nx > ns > t > y$. □

Theorem 11.65. *A nonempty set of real numbers which has an upper bound has a least upper bound.*

Proof. Let A be a set satisfying the hypothesis. Inductively we construct a sequence of rational numbers (b_n) such that b_n is an upper bound for A but $b_n - \frac{1}{2^n}$ is not. Indeed, let b_0 be an integer such that b_0 is an upper bound for A while $b_0 - 1$ is not. For $n \geq 1$ we define

$$b_n = \begin{cases} b_{n-1} - \frac{1}{2^n} & \text{if } b_{n-1} - \frac{1}{2^n} \text{ is an upper bound} \\ b_{n-1} & \text{if } b_{n-1} - \frac{1}{2^n} \text{ is not an upper bound.} \end{cases}$$

For $m \geq n$ we have $b_n - \frac{1}{2^n} < b_m \leq b_n$, hence $|b_n - b_m| < \frac{1}{2^n}$. We conclude that for any fixed N and $m, n \geq N$ we have $|b_n - b_m| < \frac{1}{2^N}$, therefore $b = (b_n)$ is a Cauchy sequence of rational numbers. Consider $u = [b] \in \mathbb{R}$. We claim that $u = lubA$. It is easy to prove that $b_n - \frac{1}{2^n} \leq u \leq b_n$(exercise!). If there is $a \in A$ with $a > u$, then we can find n with $\frac{1}{2^n} < a - u$ which gives $b_n < a$, contradiction. This proves that u is an upper bound for A. If v is an upper bound with $v < u$, choose n such that $\frac{1}{2^n} < u - v$. Since $b_n - \frac{1}{2^n}$ is not an upper bound, there is $a \in A$ such that $b_n - \frac{1}{2^n} < a$, which gives $b_n - \frac{1}{2^n} < v$. Adding this with $\frac{1}{2^n} < u - v$, we obtain $b_n < u$, contradiction. □

Corollary 11.66. A nonempty subset of real numbers which has a lower bound has a greatest lower bound.

Proof. Exercise. □

Definition 11.67. A sequence $x = (x_n)$ of real numbers is Cauchy if for any positive real number ε there exists a positive integer N such that $|x_m - x_n| < \varepsilon$ for all $m, n \geq N$. A real number L is a limit of a sequence $x = (x_n)$ of real numbers if for any $\varepsilon > 0$ there is N such that $|x_n - L| < \varepsilon$ for all $n \geq N$. We write $L = \lim\limits_{n\to\infty} x_n$ and we say that $x = (x_n)$ is convergent.

Example 11.68. Let $x_1 = 1, x_{n+1} = \dfrac{1}{2}\left(x_n + \dfrac{\sqrt{2}}{x_n}\right)$. Then x is a Cauchy sequence of real numbers. In fact, $x_n \to \sqrt[4]{2}$.

Proof. We have

$$x_{n+1} - x_n = \frac{1}{2}x_n + \frac{\sqrt{2}}{2x_n} - x_n = \frac{\sqrt{2} - x_n^2}{2x_n}.$$

By induction we will prove that $x_n \geq \sqrt[4]{2}$ for all $n \geq 2$, hence $x_{n+1} \leq x_n$ for $n \geq 2$. Indeed, $x_2 = \dfrac{1+\sqrt{2}}{2} \geq \sqrt[4]{2}$. Assume $x_k \geq \sqrt[4]{2}$ for some $k \geq 2$. Then

$$x_{k+1} = \frac{1}{2}\left(x_k + \frac{\sqrt{2}}{x_k}\right) \geq \sqrt[4]{2}$$

since $x_k > 0$ and $(x_k - \sqrt[4]{2})^2 \geq 0$. It follows that $(x_n)_{n\geq 2}$ is decreasing and bounded bellow by $\sqrt[4]{2}$, hence convergent. Since any convergent sequence is Cauchy, we conclude that (x_n) is Cauchy. Let $L = \lim\limits_{n\to\infty} x_n$. We have $L = \frac{1}{2}(L + \frac{\sqrt{2}}{L})$, hence $L = \sqrt[4]{2}$.

□

Exercise 11.69. Prove that

1. A sequence of real numbers has at most one limit.
2. A convergent sequence of real numbers is Cauchy.

Exercise 11.70. A decreasing sequence of real numbers which is bounded below is convergent. Similarly, an increasing sequence of real numbers which is bounded above is convergent.

Lemma 11.71. *Let $a = (a_n)$ be a Cauchy sequence of rational numbers and let L be the real number which it defines. Then a can be viewed as a Cauchy sequence of real numbers and $\lim\limits_{n\to\infty} a_n = L$.*

Proof. The first assertion is clear. Let $\varepsilon > 0$ and let $\delta \in \mathbb{Q}$ with $0 < \delta < \varepsilon$. Since a is Cauchy, there is N such that $|a_m - a_n| < \delta$ for all $m, n \geq N$. Consider $x_n = \widehat{a_n}$. Then $x_n - L \leq \delta$ for $n \geq N$. Similarly, $L - x_n \leq \delta$ for $n \geq N$. We conclude that for all $n \geq N$ we have $|x_n - L| \leq \delta < \varepsilon$, hence $\lim\limits_{n\to\infty} a_n = \lim\limits_{n\to\infty} x_n = L$. □

Theorem 11.72. *Any Cauchy sequence of real numbers is convergent.*

Proof. Assume that $x = (x_n)$ is a Cauchy sequence of real numbers. For each positive integer n we have $x_n < x_n + 1/n$, hence we may find $a_n \in \mathbb{Q}$ with $x_n < a_n < x_n + 1/n$. Given $\varepsilon > 0$ let N_1 be an integer with $N_1 > \varepsilon/3$. For $n \geq N_1$ we have $|x_n - a_n| < \varepsilon/3$. The inequality

$$|a_m - a_n| \leq |a_m - x_m| + |x_m - x_n| + |x_n - a_n|$$

proves that $a = (a_n)$ is a Cauchy sequence, hence it defines a real number L such that $\lim\limits_{n\to\infty} a_n = L$. For the fixed $\varepsilon > 0$ there is N_2 such that $|a_n - L| < \varepsilon/2$ for all $n \geq N_2$. It follows that for $n \geq \max\{N_1, N_2\}$ we get

$$|x_n - L| \leq |x_n - a_n| + |a_n - L| < \varepsilon/3 + \varepsilon/2 < \varepsilon,$$

hence $L = \lim\limits_{n\to\infty} x_n$. □

Remark 11.73. This property of real numbers is called completeness. We have seen that the set of rational numbers does not have this property, since there are Cauchy sequences of rational numbers converging to irrational numbers. We say that the set of real numbers was obtained by completing the set of rational numbers. The set of real numbers forms an Archimedean complete ordered field.

Remark 11.74. The set of rational numbers can be completed in a different way to obtain what is called the field of p-adic numbers denoted $\mathbb{Q}_p$ (here p is a prime number). This field is not Archimedean. We sketch now the construction of the p-adic numbers.

Fix a prime p. Each nonzero $x \in \mathbb{Q}$ can be written in a unique way as $x = p^n \cdot \dfrac{a}{b}$ where $n, a, b \in \mathbb{Z}$ and a, b are not divisible by p. Define

$$|x|_p = p^{-n}.$$

By definition $|0|_p = 0$. For example, $\left|\dfrac{3}{4}\right|_2 = 2^2$. It can be proven that

$$|x + y|_p \leq \max\{|x|_p, |y|_p\} \leq |x|_p + |y|_p$$

and that

$$|xy|_p = |x|_p|y|_p$$

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

A sequence of rational numbers $x = (x_n)$ is Cauchy with respect to $|\cdot|_p$ if for any positive rational $\varepsilon > 0$ there is $n \in \mathbb{N}$ such that $|x_m - x_n|_p < \varepsilon$ for all $m, n \geq N$. The set $\mathbb{Q}_p$ is defined as the set of equivalence classes of Cauchy sequences of rational numbers with respect to $|\cdot|_p$.

11.3. Decimal representation of real numbers

Theorem 11.75. *(Decimal representation). Given a real number x there is a sequence $d_0, d_1, d_2, \ldots$ of integers uniquely determined by x such that*

(i) $d_0 = \lfloor x \rfloor$, the largest integer less than or equal to x;

(ii) $0 \leq d_n \leq 9$ for all $n \geq 1$, in fact $d_n = \lfloor 10^n x \rfloor - 10\lfloor 10^{n-1}x \rfloor$ for $n \geq 1$;

(iii) The sequence defined inductively by

$$y_0 = d_0, y_{n+1} = y_n + \frac{d_{n+1}}{10^{n+1}}$$

is Cauchy and $\lim\limits_{n\to\infty} y_n = x$. We write

$$x = d_0.d_1d_2 \cdots d_n \cdots .$$

The terminating zeros are usually omitted.

Proof. It suffices to consider the case $x \geq 0$. Since $d_0 = \lfloor x \rfloor$, we have $10x = 10d_0 + x_1$, where $0 \leq x_1 < 10$. Let $d_1 = \lfloor x_1 \rfloor$, so $10x_1 = 10d_1 + x_2$ for some x_2 with $0 \leq x_2 < 10$. In general we can find x_n such that $10x_{n-1} = 10d_{n-1} + x_n$ and we set $d_n = \lfloor x_n \rfloor$. We can write

$$x = d_0 + \frac{d_1}{10} + \frac{d_2}{10^2} + \cdots + \frac{d_n}{10^n} + \frac{x_{n+1}}{10^{n+1}},$$

where $0 \leq x_{n+1} < 10$, hence

$$0 \leq x - \left(d_0 + \frac{d_1}{10} + \frac{d_2}{10^2} + \cdots + \frac{d_n}{10^n}\right) = x - y_n < \frac{1}{10^n}.$$

We conclude that $|x - y_n| < 10^{-n}$ and that $\lim\limits_{n\to\infty} y_n = x$. Uniqueness is left as exercise. □

Remark 11.76. Note that of the two possible decimal representations of numbers of the form $\frac{a}{10^b}$ where a, b are non-negative integers, the theorem chooses that one which consists of all zeros after a certain step. For example, $\frac{2}{10} = 0.2$ as opposed to 0.1999...

Theorem 11.77. *A real number is rational if and only if its decimal representation terminates or has an infinitely repeating group of digits.*

Proof. We have seen in Theorem 10.23 in the previous chapter that any rational number has a decimal representation which terminates or has periodicity.

Conversely, if the decimal expansion of $r \in \mathbb{R}$ terminates, say $r = 0.a_1a_2\cdots a_k$ where a_i are digits and $a_k \neq 0$, then

$$r = \frac{a_1 10^{k-1} + a_2 10^{k-2} + \cdots a_k}{10^k}$$

is a rational number. If r has a repeating group of decimals $b_1b_2\cdots b_m$ right after the decimal point, say $r = 0.\overline{b_1b_2\cdots b_m}$, then

$$10^m r = b_1b_2\cdots b_m + r, \quad r = \frac{b_1b_2\cdots b_m}{10^m - 1} \in \mathbb{Q}.$$

If $r = 0.a_1a_2\cdots a_k\overline{b_1b_2\cdots b_m}$, then

$$10^k r = a_1a_2\cdots a_k + 0.\overline{b_1b_2\cdots b_m},$$

$$r = \frac{\frac{b_1b_2\cdots b_m}{10^m-1} + a_1a_2\cdots a_k}{10^k} = \frac{a_1a_2\cdots a_kb_1b_2\cdots b_m - a_1a_2\cdots a_k}{(10^m - 1)10^k} \in \mathbb{Q}.$$

□

Example 11.78.

$$0.\overline{1234} = \frac{1234}{9999}, \quad 0.123\overline{4567} = \frac{1234567 - 123}{9999000} = \frac{1234444}{9999000}.$$

11.4. Algebraic and transcendental numbers

Definition 11.79. A real number α is *algebraic* if there is a polynomial $p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots a_1 x + a_0$ with integer coefficients such that $p(\alpha) = 0$. A number which is not algebraic is called *transcendental*.

Example 11.80. Rational numbers are algebraic. Indeed, $\frac{a}{b}$ is a root of the polynomial $p(x) = bx - a$. Some irrational numbers are algebraic, for example $\sqrt{2}$ is a root of $p(x) = x^2 - 2$. The numbers e and π are transcendental. It can be proved that the set $\mathbb{A}$ of algebraic numbers is countable (in bijection with $\mathbb{N}$).

Exercise 11.81. Show that $1 - \sqrt{3}, \sqrt{5} - \sqrt{2}$ are algebraic.

Exercise 11.82. Prove that if α is algebraic, then $k\alpha$ is algebraic for any integer k. Also, if $\alpha \neq 0$ is algebraic, then the inverse $1/\alpha$ is algebraic.

Exercise 11.83. Prove that if β is transcendental, then $1/\beta$ is also transcendental.

Remark 11.84. Euler's constant $\gamma = \lim\limits_{n\to\infty}(1 + \frac{1}{2} + \cdots + \frac{1}{n} - \ln n)$ is not known to be rational or irrational, algebraic or transcendent. (The existence of the limit can be proved using the Mean value Theorem).

Chapter 12

The construction of complex numbers

Complex numbers were invented to be able to solve polynomial equations like $x^2 + 1 = 0$. You may be familiar with the quadratic formula for solving $ax^2 + bx + c = 0$ for $a \neq 0$. If $b^2 - 4ac < 0$, you get something negative under the square root, and the solutions are complex numbers. We give a formal definition and prove some elementary properties of the set $\mathbb{C}$ of complex numbers. It turns out that $\mathbb{C}$ is an *algebraically closed field*: any polynomial equation with complex coefficients has all the roots in $\mathbb{C}$. This statement is proved in Galois Theory, part of Abstract Algebra.

12.1. The algebraic definition and properties

Definition 12.1. The set of complex numbers is

$$\mathbb{C} = \mathbb{R} \times \mathbb{R} = \{\langle a, b\rangle : a, b \in \mathbb{R}\}$$

with operations

$$\langle a, b\rangle + \langle c, d\rangle = \langle a + c, b + d\rangle \text{ and } \langle a, b\rangle \cdot \langle c, d\rangle = \langle ac - bd, ad + bc\rangle.$$

Theorem 12.2. *The addition + and multiplication · are commutative and associative. The multiplication is distributive with respect to addition. For $z \in \mathbb{C}$, we have*

$$z + \langle 0, 0\rangle = z, \quad z \cdot \langle 0, 0\rangle = \langle 0, 0\rangle, \quad z \cdot \langle 1, 0\rangle = z.$$

For each $z \in \mathbb{C}$ there is a unique w such that $z + w = \langle 0, 0\rangle$. We have cancellation $w + z = u + z \Rightarrow w = u$.

Proof. Commutativity and associativity of addition are easy verifications. We have

$$\langle a, b\rangle \cdot \langle c, d\rangle = \langle ac - bd, ad + bc\rangle = \langle ca - db, da + cb\rangle = \langle c, d\rangle \cdot \langle a, b\rangle.$$

$$(\langle a,b\rangle\cdot\langle c,d\rangle)\cdot\langle e,f\rangle=\langle ac-bd,ad+bc\rangle\cdot\langle e,f\rangle=$$
$$=\langle ace-bde-adf-bcf,acf-bdf+ade+bce\rangle=$$
$$\langle a,b\rangle\cdot\langle ce-df,cf+de\rangle=\langle a,b\rangle\cdot(\langle c,d\rangle\cdot\langle e,f\rangle).$$
$$\langle a,b\rangle\cdot(\langle c,d\rangle+\langle e,f\rangle)=\langle a,b\rangle\cdot\langle c+e,d+f\rangle=\langle ac+ae-bd-bf,ad+af+bc+be\rangle=$$
$$\langle ac-bd,ad+bc\rangle+\langle ae-bf,af+be\rangle=\langle a,b\rangle\cdot\langle c,d\rangle+\langle a,b\rangle\cdot\langle e,f\rangle.$$

We leave the remaining properties as exercise. □

Definition 12.3. If $z=\langle a,b\rangle\in\mathbb{C}$, define the conjugate $\bar z=\langle a,-b\rangle$ and the absolute value of z by $|z|=\sqrt{a^2+b^2}$. Note that $|z|\in[0,\infty)$.

Remark 12.4. A complex number $\langle a,b\rangle$ can be identified with a point in the euclidean plane $\mathbb{R}^2$. The operations have geometric interpretation. For example, the sum of two complex numbers is obtained by the parallelogram rule used for addition of vectors.

Theorem 12.5. *We have*

1. $|z|=0$ *iff* $z=\langle 0,0\rangle$.
2. $|z\cdot w|=|z|\cdot|w|$.
3. $z\bar z=|z|^2$ *and* $|z|=|\bar z|$.
4. $z\cdot w=\langle 0,0\rangle$ *iff* $z=\langle 0,0\rangle$ *or* $w=\langle 0,0\rangle$.
5. $\overline{z+w}=\bar z+\bar w$.
6. $\overline{zw}=\bar z\bar w$
7. $|a|=|\langle a,0\rangle|\le|\langle a,b\rangle|$.
8. $|z+w|\le|z|+|w|$.

Proof. The first six properties are easy to check using the definition.

7. We have $|a|=\sqrt{a^2}\le\sqrt{a^2+b^2}$.
8. Let $z=\langle a,b\rangle$ and $w=\langle c,d\rangle$. We have

$$|z+w|^2=(z+w)(\bar z+\bar w)=z\bar z+z\bar w+\bar z w+w\bar w=$$
$$=|z|^2+\langle ac+bd,bc-ad\rangle+\langle ac+bd,ad-bc\rangle+|w|^2=$$
$$|z|^2+2\langle ac+bd,0\rangle+|w|^2\le|z|^2+2|z\bar w|+|w|^2=$$
$$=|z|^2+2|z||w|+|w|^2=(|z|+|w|)^2.$$

The inequality follows by taking square roots. □

Theorem 12.6. *For each $z\ne\langle 0,0\rangle$ there exists a unique w such that $z\cdot w=\langle 1,0\rangle$.*

If $z\ne\langle 0,0\rangle$ and $z\cdot w=z\cdot u$, then $w=u$.

Proof. Let $z=\langle a,b\rangle$ with $a^2+b^2\ne 0$. Consider $w=\langle\frac{a}{a^2+b^2},-\frac{b}{a^2+b^2}\rangle$. Then $z\cdot w=\langle 1,0\rangle$. Note that $w=\frac{\bar z}{|z|^2}$. This w is called the inverse of z, denoted z^{-1}. For the second property, multiply both sides by z^{-1}. □

Theorem 12.7. *We have $\langle a,0\rangle+\langle b,0\rangle=\langle a+b,0\rangle$ and $\langle a,0\rangle\cdot\langle b,0\rangle=\langle ab,0\rangle$.*

Proof. Exercise. □

Corollary 12.8. The field $(\mathbb{R}, +, \cdot)$ is isomorphic with the subset $\{\langle a, 0\rangle : a \in \mathbb{R}\}$ of $\mathbb{C}$ under addition and multiplication. We identify a real number a with the pair $\langle a, 0\rangle \in \mathbb{C}$.

Remark 12.9. Denote by i the element $\langle 0, 1\rangle$ of $\mathbb{C}$. Then we have

$$i^2 = \langle 0, 1\rangle \cdot \langle 0, 1\rangle = \langle -1, 0\rangle = -1.$$

Any complex number $\langle a, b\rangle$ can be written as $\langle a, b\rangle = \langle a, 0\rangle + \langle b, 0\rangle \cdot \langle 0, 1\rangle = a + bi$. Note that $\overline{a + bi} = a - bi$. The real numbers a and b are called the *real part* and the *imaginary part* of $z = a + bi$. We write $a = \mathrm{Re}(z)$, $b = \mathrm{Im}(z)$.

Exercise 12.10. Determine i^n for $n \in \mathbb{N}$.

Remark 12.11. There is no order relation on $\mathbb{C}$ that extends the usual order relation on $\mathbb{R}$, hence $\mathbb{C}$ it not an ordered field.

Proof. Indeed, if such an order $\preceq$ exists, then $z^2 \succeq 0$ for all $z \in \mathbb{C}$. But $i^2 = -1 \preceq 0$, contradiction. □

Exercise 12.12. Prove that

a. $z + \bar{z} = 2\mathrm{Re}(z)$ and $z - \bar{z} = 2i\mathrm{Im}(z)$.

b. $|\mathrm{Re}(z)| \leq |z|$ and $|\mathrm{Im}(z)| \leq |z|$.

Exercise 12.13. Let $z = 3 + 4i$ and $w = 5 - 2i$. Evaluate and simplify

$$|z|, |w|, z + w, zw, z/w, \overline{iz - 3w}.$$

Where applicable, determine the real part and the imaginary part.

Remark 12.14. The quadratic equation $ax^2 + bx + c = 0$ with complex coefficients can be solved using the quadratic formula,

$$x_{1,2} = \frac{-b + \sqrt{b^2 - 4ac}}{2a},$$

except this involves the square root of a complex number, which in general has two possible complex values.

Example 12.15. Let's find $\sqrt{2 + i} = a + bi$ with $a, b \in \mathbb{R}$. We have $(a + bi)^2 = 2 + i$, so $a^2 - b^2 + 2abi = 2 + i$. The system

$$a^2 - b^2 = 2$$

$$2ab = 1$$

has two real solutions

$$a = \pm\sqrt{\frac{2 + \sqrt{5}}{2}}, \quad b = \pm\frac{1}{\sqrt{4 + 2\sqrt{5}}}.$$

Exercise 12.16. Solve the quadratic equations

$$x^2 - ix + 2 = 0, \quad ix^2 + (1 - i)x + 1 = 0.$$

12.2. The trigonometric form of a complex number

Sometimes it is useful to write a complex number in trigonometric form, similar to polar coordinates in the plane.

Theorem 12.17. *(Trigonometric form) If $z \in \mathbb{C} \setminus \{0\}$, then there is $r > 0$ and $w \in \mathbb{C}$ with $|w| = 1$ such that $z = rw$. The number w is of the form $\cos t + i \sin t$ with $t \in [0, 2\pi)$, so*

$$z = |z|(\cos t + i \sin t).$$

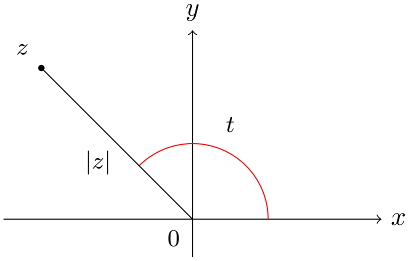
Proof. Consider $r = |z|$ and $w = \dfrac{z}{|z|}$. Then $|w| = 1$ and w is on the trigonometric circle $x^2+y^2 = 1$, hence there is $t \in [0, 2\pi)$ such that $w = \cos t+i \sin t$. The number $r \geq 0$ is the distance from z to the origin, sometimes called the polar radius, and the angle t is the polar angle, also called the *argument* of z. □

Example 12.18. Let's find the trigonometric form of $z = -2 + 2i$. We have

$$|z| = \sqrt{4+4} = 2\sqrt{2}, \quad \frac{z}{|z|} = -\frac{1}{\sqrt{2}} + \frac{1}{\sqrt{2}}i,$$

so $t = \dfrac{3\pi}{4}$ and

$$-2 + 2i = 2\sqrt{2}\left(\cos\frac{3\pi}{4} + i\sin\frac{3\pi}{4}\right).$$



Corollary 12.19. Two complex numbers in trigonometric form $z_n = r_n(\cos t_n + i \sin t_n), n = 1, 2$ can be multiplied by the formula

$$z_1z_2 = r_1r_2(\cos(t_1 + t_2) + i \sin(t_1 + t_2)).$$

Proof. Indeed,

$$(\cos t_1 + i \sin t_1)(\cos t_2 + i \sin t_2) =$$
$$= (\cos t_1 \cos t_2 - \sin t_1 \sin t_2) + i(\sin t_1 \cos t_2 + \sin t_2 \cos t_1) =$$
$$= \cos(t_1 + t_2) + i \sin(t_1 + t_2).$$

□

Theorem 12.20. *We have the formula (De Moivre)*

$$(cost + i \sin t)^n = \cos nt + i \sin nt.$$

Proof. By induction. Clearly this is true for $n = 1$. Assume

$$(cost + i \sin t)^k = \cos kt + i \sin kt$$

for some $k \geq 1$. Then

$$(cost+i \sin t)^{k+1} = (\cos t+i \sin t)^k(\cos t+i \sin t) = (\cos kt+i \sin kt)(\cos t+i \sin t) =$$

$$= (\cos kt \cos t - \sin kt \sin t) + i(\cos kt \sin t + \sin kt \cos t) = \cos(k+1)t + i \sin(k+1)t.$$

□

Theorem 12.21. *The field $\mathbb{C}$ is complete (every Cauchy sequence is convergent).*

Proof. Let (z_n) with $z_n = a_n + b_n i$ be a Cauchy sequence in $\mathbb{C}$. This means that $\forall \varepsilon > 0$ there is $N \in \mathbb{N}$ such that $|z_m - z_n| < \varepsilon$ for all $m, n \geq N$. Since $|a_m - a_n|, |b_m - b_n| \leq |z_m - z_n|$, we conclude that the sequences (a_n) and (b_n) are Cauchy. Since $\mathbb{R}$ is complete, we get $a_n \to a$ and $b_n \to b$. Then $z_n \to a + bi$. □

Exercise 12.22. Let $z = a + bi, w = c + di$. Define $z \prec w$ if $a < c$ or $a = c$ and $b < d$ (lexicographic strict order). Does this order have the least upper bound property?

Exercise 12.23. If $z \in \mathbb{C}$ such that $|z| = 1$, compute $|1 + z|^2 + |1 - z|^2$.

Exercise 12.24. Suppose $z \in \mathbb{C}$ such that $z + \dfrac{1}{z} = 1$. Find $z^2 + \dfrac{1}{z^2}$ and in general $z^n + \dfrac{1}{z^n}$.

Remark 12.25. It is possible to extend the complex number field to a larger system of numbers $\mathbb{H}$. In fact, one can define addition and multiplication on $\mathbb{H} = \mathbb{C} \times \mathbb{C}$ to get a number system called the *quaternions*, invented by Hamilton. More precisely,

$$\langle z_1, w_1\rangle + \langle z_2, w_2\rangle = \langle z_1+z_2, w_1+w_2\rangle, \langle z_1, w_1\rangle \cdot \langle z_2, w_2\rangle = \langle z_1z_2 - w_1\bar{w}_2, z_1w_2 + \bar{z}_2w_1\rangle.$$

We can identify $z \in \mathbb{C}$ with $\langle z, 0\rangle \in \mathbb{H}$. It can be proved that the multiplication of quaternions is associative but not commutative. Any non-zero quaternion has a multiplicative inverse. The set $\mathbb{H}$ becomes a structure called *division ring* or *skew field*.

Exercise 12.26. Denote $j = \langle 0, 1\rangle$ and $k = \langle 0, i\rangle$ as elements in $\mathbb{H}$. Prove that

$$j \cdot j = k \cdot k = \langle -1, 0\rangle, i \cdot j = k, j \cdot k = i, k \cdot i = j, j \cdot i = -k, k \cdot j = -i, i \cdot k = -j.$$

Exercise 12.27. Any quaternion $\langle z, w\rangle \in \mathbb{H}$ can be written in the form $z + wj$.

Remark 12.28. It is possible to give $\mathbb{H} \times \mathbb{H}$ an additive and multiplicative operations, obtaining the *octonions* or *Cayley numbers*. The multiplication is both non-commutative and non-associative. The quaternions and the Cayley numbers are used in Mathematical Physics, Group Representation and Algebraic Topology.

Bibliography

[1] Beck, M. and Geoghegan, R., *The Art of Proof*, Springer 2011.

[2] Birkhoff, G. and Mac Lane, S., *Algebra*, AMS Chelsea Publishing, 1999.

[3] Ciesielski, K., *Set theory for the working mathematician*, Cambridge university press 1997.

[4] Davidson, K.R. and Donsig, A.P. *Real analysis and applications. Theory in practice* Undergraduate Texts in Mathematics. Springer, New York, 2010.

[5] Folland, G. *Real Analysis. Modern techniques and their applications, second edition*, John Wiley & sons, Inc. 1999.

[6] Galovich, S. *Doing Mathematics. An Introduction to proofs and problem solving, second edition*, Thomson Brooks/Cole 2007.

[7] Halmos, P.R., *Naive Set Theory*, Springer-Verlag, 1974.

[8] Hammack, R. *Book of Proof*, 2009

[9] Hewson, S. *A mathematical bridge: an intuitive journey in higher mathematics*, World Scientific 2009.

[10] Krantz, S. *Real analysis and foundations*, CRC Press 2000.

[11] Krantz, S. *The elements of advanced mathematics, 2nd edition*, Chapman & Hall 2002.

[12] Liebeck, M. *A concise introduction to pure mathematics*, CRC Press 2011.

[13] Pedersen, G.K. *Analysis Now*, Springer 1989.

[14] Rudin, W. *Principles of Mathematical Analysis*, McGraw-Hill 1976.

[15] Stoll, R. *Set theory and logic*, Dover 1979.

[16] Sundstrom, T. *Mathematical Reasoning: Writing and Proof.*

[17] Youse, B.K., *The number system*, Dickenson Publishing Company, 1965.

Index