FUNDAMENTALS OF MATHEMATICS

LIA VAŠ

Introduction

Existing approaches to "bridging". The standard "calculus trilogy" and comparable courses are usually geared towards more general student population, not only those students who may be interested in the methods of proving mathematical statements and a more rigorous introduction to higher mathematics. The emphasis of such courses is often closer to the applications of mathematics, not to its theoretical aspect.

So, a transition from these general mathematics requirements to proof-heavier courses like Real Analysis or Modern Algebra has to happen at some point between these two groups of courses and a course in which this transition happens is often referred to as the **bridge course**. There are three standard approaches to "bridging".

The **first approach** is to require a specific course, like Linear Algebra, for example, which introduces students to basic elements of proofs and then to start Real Analysis or Modern Algebra courses with further introduction to proofs and some prerequisites before the standard material which these courses cover. This approach patches the problem to an extent, but an introduction to proofs using only the statements of Linear Algebra may cause a student to associate the proofs in general only to the Linear Algebra material. In addition, covering the standard required material of Linear Algebra may not leave enough space for a gradual and thorough introduction to proofs. Starting Real Analysis and Modern Algebra with an extensive introduction may cause some standard topics of these course not to be covered.

The **second approach** is to require a specific course, often containing the word "proof" in the title (e.g. Introduction to Proofs), which focuses specifically on proving various mathematical statements. This does provide an introduction to proofs, but a possible lack of cohesion between the statements the students are expected to prove can make the proving techniques seem almost random to a novice. A good number of such courses are notoriously hard to students, dreaded by mathematics majors and avoided by other majors.

The **third approach** is to require students to take a Discrete Mathematics course. Such a course typically contains some of the topics this text also contains, but they are often covered with a focus on applications of mathematics in Computer Science, not with a focus on introducing students to proofs. In addition, a typical Discrete Mathematics course contains a good number of topics which are prerequisites for applications of mathematics in Computer Science, not for the upper level mathematics courses.

The main goals of the course which uses this text. This text is an attempt to present the material for a bridge course without the above mentioned downsides: this material is for a **single (one-semester) course** solely dedicated to

- presenting a background and prerequisites for some upper-level mathematics courses through
- an introduction to mathematical proofs, logical reasoning, and the language of modern mathematics.

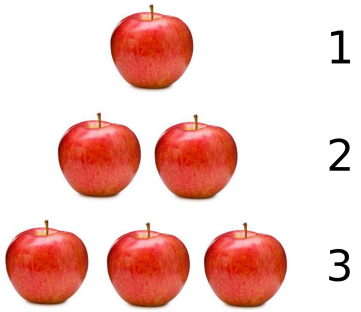
In addition, the students are also

- introduced to various areas of mathematics and as well as to reasons for their study.

The material is presented with a cohesion: the subsequent sections relate to the previous ones and there is an **arc in the story-line**: the material can be seen as a journey from the very basics of mathematical arguments, via the main objects of mathematics (sets, relations, and functions), eventually reaching the formation of the number sets and ending with the formation of the (algebraically closed) field of complex numbers. Proofs using different techniques are present in every section and they elevate as the course progresses. While the focus is on mathematics and not Computer Science or other disciplines, the material is suitable for students majoring in non-mathematics disciplines who may be interested in higher mathematics or in mastering techniques of proving mathematical statements.

In addition, this text is written with another goal in mind: to **introduce students to areas of higher mathematics**. Besides prerequisites for Real Analysis and Modern Algebra, the course contains **prerequisites** for any of the following undergraduate courses: Topology, Complex Analysis, Set Theory, Logic, Graph Theory, and some others, and, in addition, prerequisites for general graduate courses in pure mathematics. As the necessary requirements of a mathematics major tend not to include an introduction to history of mathematics, we include **historical remarks** whenever possible. We also present some **major results** which shaped modern mathematics.

The **introduction to proofs is gradual**: most of the text does not even contain the references to propositions or theorems, only to exercises, examples and practice problems. The label "proof" is used for the first time only after Cantor's Theorem in section 6. The absence of the labels *theorem, proposition* and *corollary* until section 10 may cause some eager students to feel like they are not mastering the techniques of proving such statements before section 10. This sentiment of the seeming lack of a fast progression was shared with the main character, Daniel, of the 1984 movie Karate Kid. Harassed by bullies and wanting to learn to defend himself, Daniel becomes a student of a karate master, Mr. Miyagi. However, instead of an instruction in karate, Daniel is given menial tasks of painting the fence, sanding the wooden floor, and waxing Mr. Miyagi's car ("wax on, wax off" was Mr. Miyagi's input). After



Doing exercises,

examples, and

practice problems

getting frustrated, Daniel complains to Mr. Miyagi. In response, Mr. Miyagi demonstrates that the repetitive movements enabled Daniel's muscle to develop "muscle memory"and provided essentials for growing his defensive skills. Daniel indeed masters karate soon after.

We adopt Mr. Miyagi's **wax-on-wax-off** method as our **approach to presentation**: examples, exercises, and, at the end of each section, practice problems are, in fact, lemmas, propositions and theorems and their solutions are, in fact, proofs. By the end of the course,

students' abilities to prove more complex statements will be significantly developed.

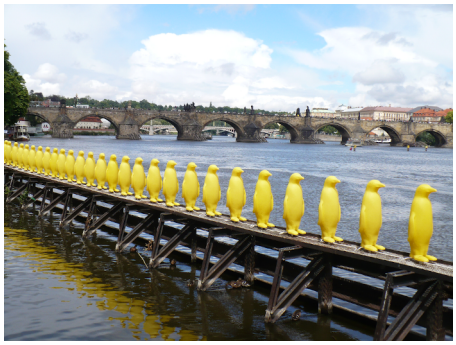
Proving theorems

The content of sections. Sections 1 and 2 provide background in **logic** needed both for the presentation in the rest of the text and for understanding the basics of proofs (for example, techniques of proving a statement of the form "if P, then Q"). These sections also facilitate students' writing and understanding of mathematical statements in subsequent courses. For example, knowing how to move a negation through the quantifiers and logical connectives facilitates the understanding of showing that a function is not continuous at a given value of the domain in Real Analysis.

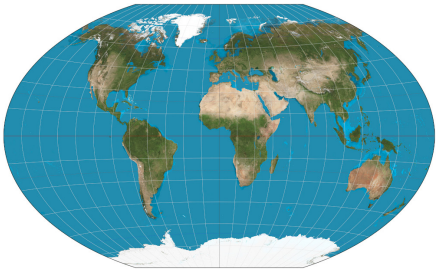
An implication

Section 3 contains an introduction to **sets**, basic objects in almost all areas of mathematics. Some most relevant operations and relations on sets are introduced. By proving basic properties of those, students get a further exposure to proofs.

Section 4 contains an introduction to **relations**. **Equivalence** relations enable one to create a new set by *"equating"* elements of another set. This construction is used in subsequent sections: when integers are created from natural numbers, rationals from integers, and reals from rationals. This construction is also relevant for understanding some prominent definitions in Modern Algebra (for example that of a quotient of a group with respect to a normal subgroup). **Partial order** relations introduce a concept of hierarchy among elements of a set. This hierarchy is present when working with intervals of real numbers and with concepts like lower and upper bound, minimal and maximal elements and supremum and infimum.


A total order

Section 5 focuses on another fundamental concept of mathematics, **functions**, and the related concepts such are domain, codomain, image and inverse image of sets, inverse function, and a bijective correspondence. These notions are prominently used in almost all areas of mathematics: from homomorphisms on specific algebraic structures in Modern Algebra


A mapping

and continuous functions on topological sets (giving rise to the concept of continuity on metric spaces) to generalizations of sets and functions as in category theory.

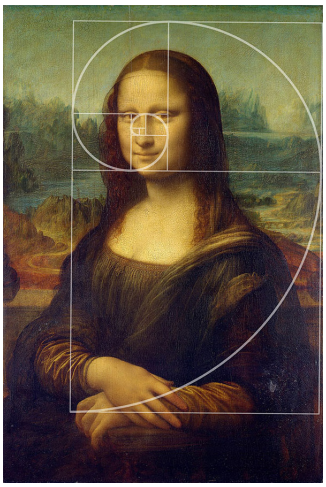
Cardinals?

The concept of a bijective correspondence from section 5 is essential when introducing **cardinality** in section 6 and when answering the following questions: Do any two sets with infinitely many elements have the same number of elements? If not, how do we measure different infinities? What do we even mean by "the number of elements" if this number is not finite? Cantor's Theorem, shown in this section, opens the doors to Continuum Hypothesis which eventually leads to Gödel's Incompleteness Theorems.

The **natural numbers** are introduced as finite cardinals in section 7. Section 7 contains an extensive part on **mathematical induction.**

The consideration of functions which are compatible with operations on sets leads to **homomorphisms** and the consideration of equivalences which are compatible with operations on sets leads to **congruences**. These concepts, as well as the idea of **diagram chasing**, are considered in section 8. Besides their use in Modern Algebra, the creation of the number sets $\mathbb{Z}$ and $\mathbb{Q}$ involves congruences.

In section 9, the **integer numbers** are formed from the natural numbers and then the **rational numbers** are formed from the integers.



The golden ratio $\frac{1+\sqrt{5}}{2}$

In section 10, we introduce the **real numbers** as the equivalence classes of Cauchy sequences. We opt for using Cauchy sequences instead of Dedekind cuts or axiomatic approach because of the study of convergent sequences in Real Analysis. This section also includes some "classic" results as, for example, the proof that $\sqrt{2}$ is not rational, that the cardinal equality $\mathfrak{c} = 2^{\aleph_0}$ holds, and that the rationals are dense in the reals. In this section, the terms *lemma, proposition, theorem,* and *corollary* are introduced.

In section 11, we finish the process of enlarging number sets by reaching the **complex numbers**. The *Fundamental Theorem of Algebra* shows that we do not need to go any further - constituting an algebraically closed field, the complex numbers are indeed the end of the road not just for us in a semester but also for the progression $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ which needs no further expansion.

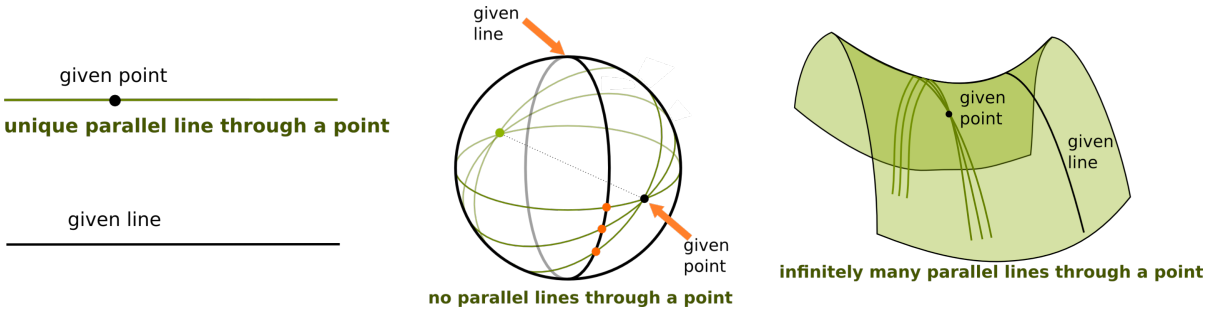
Lia Vaš,
fall 2023

Contents

1. Fundamentals of Logic

Building solid fundamentals. Let us start the story of Fundamentals of Mathematics with David Hilbert who was looking for an overarching treatment of the existing mathematical theories in the early 20th century. Such a treatment is also supposed to ensure that no contradictory statement can be deduced with in a given theory. Hilbert also wanted to distinguish **the axioms**, the statements whose validity we do not question, from **provable claims** (like theorems and propositions) whose validity we demonstrate.

For example, the statement that every two points determine a line, known as the Euclid's Fifth Postulate, was accepted to be true. However, through the centuries, mathematicians had problems proving this claim, so they begin to doubt its validity in just any theory we may want to call a "geometry". And, indeed, by the early 19th century, models of geometries in which Euclid's Fifth Postulate fails begin to emerge.



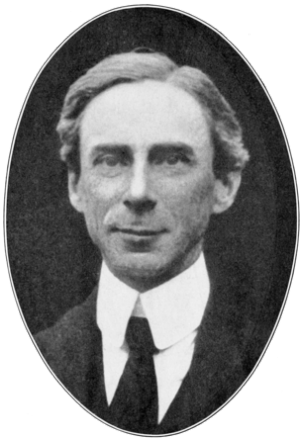
Without going into these different geometries (the on geometry has more details), the Fifth Postulate illustrates how certain claims can be taken as *axioms*, the statements which we assume to be true and use to build a certain theory, and that those should be distinguished from statements whose validity can be shown from the axioms using the specified rules called **the rules of inference.** So, if the Euclid's Fifth Postulate is accepted as an axiom, one builds a geometry, called Euclidean geometry, in which there is only one line passing a given point and not intersection a given line.

In his book "The Foundations of Geometry", published in 1899, David Hilbert proposed a list of assumptions in order to create a foundation for such treatment of Euclidean geometry. Hilbert also proposed that our mental perception of a "point", a "line", and a "plane" does not have to matches the expected representation when building non-Euclidean geometries, like, for example, as in the second geometry model above in which "lines" are large circles on a sphere).

Hilbert's treatment of geometry gave rise to a more general idea: an area of mathematics should be build on specific assumptions, **the axioms**, and the rules, **the rules of inference**, which specify how one derives statements from the axioms. For example, the following argument, known since the antique times, is a rule of inference.

All men are mortal. Socrates is a man. Hence, Socrates is mortal.

If one builds a mathematical theory in this way, one of the main concerns is whether such a theory is **consistent**, i.e. whether assuming that the axioms are true, the rules of inference do not produce a false statement.



Just two years after Hilbert's Foundations of Geometry was published and when his ideas of axiomatic treatment of mathematical theories started being circulated, Bertrand Russell noted a dramatic paradox in set theory, one of the most basic theories in mathematics.

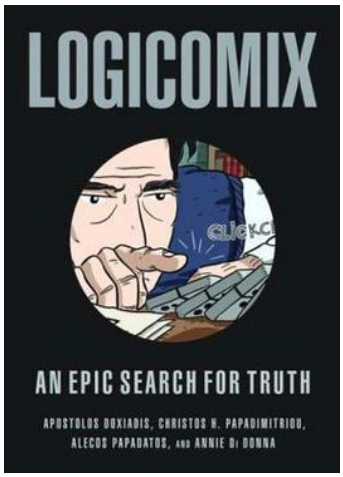
We present this paradox in its set theoretic form section 3. For the time being, we present two non-set-theoretic versions of it.

(1) **The barber paradox.** Say that a barber is defined as a person who shaves those and only those who do not shave themselves and a person is not a barber if somebody else shaves them. The question is who shaves the barber. If it is somebody else who shaves the barber, then this barber would stop being a barber. If the barber shaves himself, then that barber would also stop being a barber. Thus, any answer to this question results in a contradiction.

(2) **The liar paradox.** A liar says 'I am lying'. If he is lying when saying that, then what he says is not true, meaning that "I am not lying" is true, so he is not lying. If he is not lying when saying that, then the statement "I am lying" is true, so he is lying. Thus, we arrive to a contradiction in either case.

Between 1910 and 1930, Russell and A. N. Whitehead published three volumes of Principia Mathematica (the Principles of Mathematics) which presented an approach of building symbolic logic formally and an attempt to solve the paradoxes that became evident in logic and set theory at the turn of the 20th century (including Russell's paradox).

While the Russell-Whitehead treatment pawed a way of the formalism in today's mathematics, a finishing touch to it was made by the work of Kurt Gödel. In 1929, he proved the Consistency Theorem (stating that a statement which is known to be true within a "simple enough" theory can be proved in that theory), and, in 1931 he showed his Incompleteness Theorems (stating that a "sufficiently complicated" theory contains statements which are true but which cannot be proven within that theory). Section 6 has more details.



If you like comic books and are interested in these topics, a comic book **Logicomix: An Epic Search for Truth** (written by Apostolos Doxiadis and Christos Papadimitriou and illustrated by Alekos Papadatos) covers the topics presented so far in more details.

We start our own "epic search for truth" by studying the simplest and most fundamental logic, the propositional logic.

Propositional logic. Logic is often defined as the *study of reasoning.* While we use reasoning in everyday life, logic considers reasoning from a more formal perspective, by building a system with specified rules of inference to deduce whether statements are true or false. *Propositional logic* is a study of the validity of arguments involving **sentences or statements** built from simpler sentences represented by letters using propositional **connectives**.

We represent specific sentences by symbols. For example, we can use p, q, r etc. We also use the symbol $\top$ to denote "true" and $\bot$ for "false" and refer to these as the **truth values**. For example, if p is the sentence "Philadelphia is a city in the United States", we can say that the truth value of p is $\top$ and if q is the sentence "Philadelphia is the capital of Spain" we can say that the truth value of q is $\bot$.

Implication. Necessary and sufficient conditions. The arguments "If I do not water the plans, they will die." or "If I study, I will pass the next exam." are further examples of informal reasoning. While informal, these examples have the same basic format: based on a **premise, antecedent,** or an **assumption** presumed true, one makes a **conclusion, consequent** or an **inference.** If p denotes the premise and q a conclusion, the sentences above can be represented in a format

$$\text{if } p \text{ then } q.$$

As we are assuming the premise p to be true, we conclude that q is true. Instead of being interested in the truth of the two specific examples above, in formal logic we are interested in the validity of the argument that, assuming that the assumption is true, we deduce that the conclusion is true. To simplify the notation, we can also use the symbol $\Rightarrow$ and write "if p then q" shorter as

$$p \Rightarrow q.$$

This introduces an operation $\Rightarrow$ on statements. It produces a new statement $p \Rightarrow q$ given two statements p and q. The operation $\Rightarrow$ is called an **implication** or a **conditional.**

If p is true and if, assuming p, we deduce the validity of q, the implication $p \Rightarrow q$ is true. Thus, the truth value of

$$\top \Rightarrow \top$$

is $\top$. Assuming that I watered the plans and that I studied for the exam, it is true that my plants are not dead and that I passed the exam.

If we deduce a false statement from a true premise, we made a faulty reasoning: assuming that I watered the plants, it is false to conclude that they died (let us not consider subtleties

such as overwatering). Thus, the truth value of

$$\top \Rightarrow \bot$$

is $\bot$.

To indicate that a conclusion of any sort, true or false, can come out of a faulty premise, both $\bot \Rightarrow \top$ and $\bot \Rightarrow \bot$ have the value $\top$. Thus, both sentences below are considered to be true.

> If Philadelphia is in Europe, then the sky is blue.
> If Philadelphia is in Europe, then I can fly to the Moon.

The examples as above illustrate the reasoning behind the definition of the implication values as in the table below.

$\Rightarrow$	$\top$	$\bot$
$\top$	$\top$	$\bot$
$\bot$	$\top$	$\top$

Another common way to represent the validity of $p \Rightarrow q$ for any possible truth value of p and q is as in the following **truth table**.

p	q	$p \Rightarrow q$
$\top$	$\top$	$\top$
$\top$	$\bot$	$\bot$
$\bot$	$\top$	$\top$
$\bot$	$\bot$	$\top$

The statement of the form "q **only if** p" is different that the form "if p, then q". While $p \Rightarrow q$ abbreviates the latter, "q only if p" states that if p does not hold, then q does not hold also (i.e. q cannot hold without p holding), so if q is true, then p must be true. Thus, "q only if p" can be represented as $q \Rightarrow p$. For example, "Vee will get a tattoo only if Bee gets a tattoo" is the same as saying that "If Vee has a tattoo, then Bee also has it".

In the implication $p \Rightarrow q$, q is also called a **necessary condition** for p because having p it is necessary to also have q. The condition p is called a **sufficient condition** for q because to have q it is sufficient to have p.

For example, as the statement "if 9 divides a number, then 3 divides that number" is true, we say that 9 dividing a number is sufficient for 3 dividing a number and that 3 dividing a number is necessary for 9 dividing a number.

Negation, conjunction, disjunction, and equivalence. The **negation** of a sentence p is denoted by $\neg p$. For example, the negation of "Mary has a little lamb" is "Mary does not have a little lamb". If p is true, $\neg p$ is false and if p is false, $\neg p$ is true so the negation has the truth table below.

p	$\neg p$
$\top$	$\bot$
$\bot$	$\top$

The **conjunction** of two sentences p and q is a sentence of the form "p and q". For example, "I am tired and I am hungry." is an example of a conjunction of two sentences. Using $\wedge$ for this operation, we write this conjunction as

$$p \wedge q.$$

The conjunction is true only if both p and q are true. So, the truth table for conjunction is given below.

p	q	$p \wedge q$
$\top$	$\top$	$\top$
$\top$	$\bot$	$\bot$
$\bot$	$\top$	$\bot$
$\bot$	$\bot$	$\bot$

The **disjunction** of two sentences p and q is a sentence of the form "p or q". Using $\vee$ for this operation, we write

$$p \vee q$$

for disjunction. The disjunction is true if either one or both p and q are true. Thus, the truth table for conjunction is given below.

p	q	$p \vee q$
$\top$	$\top$	$\top$
$\top$	$\bot$	$\top$
$\bot$	$\top$	$\top$
$\bot$	$\bot$	$\bot$

Note that the disjunction above is inclusive: for example, a person being left handed or right handed does not include the possibility that a person is ambidextrous. This should not be confused with the exclusive or as in the "either ... or ..." format. For example, if a road forks, one can go either left or right, but one cannot go simultaneously on both sides.

The **equivalence** or a biconditional of two sentences p and q, denoted by $p \Leftrightarrow q$, is a sentence stating that p and q have the same truth value: if p is true, then q is true and if p is false then q is false, or, stated more concisely, p is true *if and only if* q is true. Thus, the truth table of the equivalence is as below.

p	q	$p \Leftrightarrow q$
$\top$	$\top$	$\top$
$\top$	$\bot$	$\bot$
$\bot$	$\top$	$\bot$
$\bot$	$\bot$	$\top$

For example, "Bee and Vee travel only together" is an example of an equivalence because it implies that Bee travels only if Vee travels and Vee travels only if Bee travels.

The equivalence $p \Leftrightarrow q$ is true exactly when both "q, if p" and "q, only if p" are true. In this case, the condition p in $p \Leftrightarrow q$ is both *necessary and sufficient* for q.

Exercise 1. (1) Given the abbreviation below, express the following English-language sentences into sentences of propositional logic.

p stands for "The sky is blue."
q stands for "It is not raining."
r stands for "There are no clouds."

(a) The sky is blue or there are clouds.
(b) If it is raining, the sky is not blue.
(c) The sky is blue only if it is not raining.
(d) A sufficient condition for it to rain is that the sky is not blue.

(e) A necessary condition for the sky to be blue is that it is not raining.
(f) There are no clouds if and only the sky is blue.

(2) Using appropriate abbreviations, represent the next statements as sentences of propositional logic.
(a) A polygon is a triangle if it has three sides.
(b) A polygon is a triangle only if it has three sides.
(c) A sufficient condition for a number to be divisible by 4 is that it is divisible by 8.
(d) A necessary condition for a number to be divisible by 4 is that it is divisible by 2.

Solution. (1) (a) $p \vee \neg r$, (b) $\neg q \Rightarrow \neg p$, (c) $p \Rightarrow q$, (d) $\neg p \Rightarrow \neg q$, (e) $p \Rightarrow q$, (f) $r \Leftrightarrow \neg q$.

(2) Let p stand for "A polygon is a triangle" and q stand for "a polygon has three sides". The sentence in part (a) is $q \Rightarrow p$ and in part (b) $p \Rightarrow q$.

Let p, q and r stand for statements that a number is divisible by 8, 4, and 2. respectively. The sentence in part (c) is $p \Rightarrow q$ and the sentence in part (d) is $q \Rightarrow r$.

Statements of propositional logic. The operations symbols $\neg, \wedge, \vee, \Rightarrow$ and $\Leftrightarrow$ are *propositional connectives* and they are used to build more complex sentences from simpler ones, starting with sentences denoted by letters $p, q, r \ldots$.

Any sentence built up by application of the propositional connectives has a truth value that depends on the truth values of the constituent sentences. For example, $((\neg p) \wedge q) \Rightarrow r$ is an example of a sentence of propositional logic and the truth values $\top, \top, \bot$ of p, q, and r, respectively, produces the value $\top$ of the sentence.

Even more formally, a **statement** or a **sentence** of propositional logic is any expression obtained *recursively* in the following way.

(1) All statement letters $p, q, r, \ldots$ are statements of propositional logic.
(2) If P and Q are statements of propositional logic, then $(\neg P)$, $(P \wedge Q)$, $(P \vee Q)$, $(P \Rightarrow Q)$, and $(P \Leftrightarrow Q)$ are statements of propositional logic.
(3) Any statement of propositional logic is obtained by finite number of application of steps (1) and (2).

Thus, the formulas $(\neg(p \vee q))), ((\neg p) \Leftrightarrow (\neg q))$ are sentences of propositional logic while the formulas $p \Rightarrow$, $p(\neg q)$, or $p \wedge q)$ are not.

We **suppress the use of parenthesis** around $\neg P$ and around the entire statement so that $\neg\neg p$ shortens $(\neg(\neg p))$ and $\neg p \Rightarrow \neg q$ shortens $((\neg p) \Rightarrow (\neg q))$.

We also assume that $\wedge$ and $\vee$ are stronger than $\Rightarrow$ and $\Leftrightarrow$ in the same sense as multiplication is stronger than addition. So, just as we assume that $3x + 2$ stands for $(3x) + 2$, we assume that $p \vee q \Rightarrow \neg p$ stands for $(p \vee q) \Rightarrow \neg p$, or, restoring all parentheses, for $((p \vee q) \Rightarrow (\neg p))$.

Exercise 2. For all the sentences below which are sentences of propositional logic, restore all parentheses.

(1) $\neg p \Rightarrow \neg q \wedge \neg p$
(2) $p \Rightarrow q \Rightarrow r$
(3) $\neg p \vee \neg q$
(4) $\neg\neg(p \Rightarrow p \vee q)$
(5) $\neg\neg p \Rightarrow q \vee r$
(6) $pq \Rightarrow r$.

Solution. (1) $((\neg p) \Rightarrow ((\neg q) \wedge (\neg p)))$. (2) This is not a sentence of propositional logic because it is not clear whether it is supposed to abbreviate $(p \Rightarrow q) \Rightarrow r$ or $p \Rightarrow (q \Rightarrow r)$ which are not equivalent: the first expression is true when p, q, and r have values $\bot, \top, \bot$ and the second is false for this set of truth values of p, q, and r. (3) $((\neg p) \vee (\neg q))$, (4) $(\neg(\neg(p \Rightarrow (p \vee q))))$, (5) $((\neg(\neg p)) \Rightarrow (q \vee r))$. (6) This is not a sentence of propositional logic because there is no connective between p and q.

The language we developed by considering the sentences of propositional logic is the object of our study and we refer to it as the **object language**. The language we use to talk about it is called the **metalanguage.** For example, $p \vee q$ is a sentence of the object language and "$p \vee q$ is true if either one or both p and q are true" is a sentence of the metalanguage we use to talk about the object language.

Truth tables. Every truth value of each letter of a sentence of propositional logic uniquely determines the truth value of the sentence. In an example above, the truth values $\top, \top, \bot$ of p, q, and r, respectively, produce the value $\top$ of the sentence $\neg p \wedge q \Rightarrow r$ (recall that this is an abbreviation of $((\neg p) \wedge q) \Rightarrow r$).

Considering all possible truth values of the letters of a sentence produces all possible truth values of the sentence. This can be computed by a truth table listing first all possible truth values of the letters, then the values of parts of the sentence constituting the sentence by recursive application of step (2) above. So, for a sentence containing n letters, there are 2^n possible truth values. For example, below is a truth table for the sentence $\neg p \wedge q \Rightarrow r$. Note that the sentence has 3 letters so there are $2^3 = 8$ non-leading rows in the table.

p	q	r	$\neg p$	$\neg p \wedge q$	$\neg p \wedge q \Rightarrow r$
$\top$	$\top$	$\top$	$\bot$	$\bot$	$\top$
$\top$	$\top$	$\bot$	$\bot$	$\bot$	$\top$
$\top$	$\bot$	$\top$	$\bot$	$\bot$	$\top$
$\top$	$\bot$	$\bot$	$\bot$	$\bot$	$\top$
$\bot$	$\top$	$\top$	$\top$	$\top$	$\top$
$\bot$	$\top$	$\bot$	$\top$	$\top$	$\bot$
$\bot$	$\bot$	$\top$	$\top$	$\bot$	$\top$
$\bot$	$\bot$	$\bot$	$\top$	$\bot$	$\top$

Every sentence with n letters determines a **truth function** which has the set of 2^n possible truth values of the letters as the input and the corresponding truth values in the last column as the output.

Exercise 3. Write the truth tables for the following sentences.

(1) $p \vee q \Rightarrow \neg p \wedge q$ (2) $\neg p \Rightarrow (\neg q \Rightarrow r)$

Solution. Let (1) denotes the first sentence and (2) the second.

p	q	$p \vee q$	$\neg p$	$\neg p \vee q$	(1)
$\top$	$\top$	$\top$	$\bot$	$\top$	$\top$
$\top$	$\bot$	$\top$	$\bot$	$\bot$	$\bot$
$\bot$	$\top$	$\top$	$\top$	$\top$	$\top$
$\bot$	$\bot$	$\bot$	$\top$	$\top$	$\top$

p	q	r	$\neg p$	$\neg q$	$\neg q \Rightarrow r$	(2)
$\top$	$\top$	$\top$	$\bot$	$\bot$	$\top$	$\top$
$\top$	$\top$	$\bot$	$\bot$	$\bot$	$\top$	$\top$
$\top$	$\bot$	$\top$	$\bot$	$\top$	$\top$	$\top$
$\top$	$\bot$	$\bot$	$\bot$	$\top$	$\bot$	$\top$
$\bot$	$\top$	$\top$	$\top$	$\bot$	$\top$	$\top$
$\bot$	$\top$	$\bot$	$\top$	$\bot$	$\top$	$\top$
$\bot$	$\bot$	$\top$	$\top$	$\top$	$\top$	$\top$
$\bot$	$\bot$	$\bot$	$\top$	$\top$	$\bot$	$\bot$

Tautologies. If all the output values of the truth function of a sentence are $\top$, the sentence is said to be a *tautology*. Another way to say this is that a sentence is a tautology if it is true for any value of the letters it contains. If P is a tautology, one writes

$$\models P$$

using the double turnstile symbol $\models$. Tautologies have a special significance because of their use in mathematical proofs.

For example, the sentence $p \vee \neg p$ is a tautology because the truth table for this sentence is as follows.

p	$\neg p$	$p \vee \neg p$
$\top$	$\bot$	$\top$
$\bot$	$\top$	$\top$

The tautology $p \vee \neg p$ is called **the law of excluded middle** to indicate that either p is true or false and that no third possibility exists (Latin " tertium non datur"). This law dates back to Aristotle who noted that "it is not be possible to be and not to be the same thing".

As $p \vee \neg p$ is a tautology, a statement of the form $P \vee \neg P$ is true for any sentence P. This enables us to prove that some sentence P is true by showing that $\neg P$ is a contradiction. For example, the argument in Russell's paradox in section 3, the proof of Cantor's Theorem in section 6, and the proof that $\sqrt{2}$ is not a rational number in section 10, all contain the argument that there is no other possibility but P or not P for some statement P.

A digression. Some non-classical approaches. The law of excluded middle was not accepted in *intuitionistic logic*. To an intuitionist, the claim that an object with certain properties exists is a claim that an object with those properties can be constructed. Thus, if P is a statement which we neither proved nor disproved, then the statement $P \vee \neg P$ is not proven and, hence, not true in intuitionist logic.

There are also logic systems which allow more values then just true and false. For example, the truth values in fuzzy logic are real numbers between 0 and 1 and the truth value of, say .3 can be interpreted that the statement has 30% chance of being true.

There are other non classical approaches which either extend or deviate the classical logic (modal logic, quantum logic, dynamic semantic, and others besides fuzzy logic and intuitionist logic).

Logical implications. A sentence P is said to **logically imply** Q (or that Q is a logical consequence of P if every truth assignment to the statement letters of P which makes P true also makes Q true. We write this as

$$P \models Q \quad \text{or} \quad P \therefore Q$$

and say that deducing Q from P is a **valid argument**. For example, deducing that 3 divides a number if 9 divides it is valid. O the other hand, deducing that 9 divides a number if 3 divides it is not valid (3 divides 6, for example, and 9 does not divides 6).

Note that the implication $P \Rightarrow Q$ is true exactly when every truth assignment of the letters in P which makes P true also makes Q true. Thus, $P \models Q$ holds exactly when $P \Rightarrow Q$ is a tautology:

$$P \models Q \text{ if and only if } \models P \Rightarrow Q.$$

Thus, a sentence of the form

$$P \Rightarrow Q \text{ is a tautology if and only if assuming that } P \text{ is true implies that } Q \text{ is true.}$$

To show that $P \Rightarrow Q$ is a tautology, one may not need the entire truth table for $P \Rightarrow Q$: it is sufficient to consider the truth values which make the antecedent P true and to check that these values necessary make the consequent Q true as well. For example, let us consider the sentence

$$p \wedge (p \Rightarrow q) \Rightarrow q$$

which states the argument known as **Modus Ponens**: assuming that p is true and that $p \Rightarrow q$ is true, one concludes that q is true. To show that this argument is logically valid, we can assume that p is true and that the implication $p \Rightarrow q$ is true. Hence, this last implication is of the form $\top \Rightarrow q$. As $\top \Rightarrow \bot$ is false, if the implication $p \Rightarrow q$ is true, then q necessary has to have $\top$ value, so q is true.

Alternatively, one show that this sentence is a tautology by considering its truth table, below.

p	q	$p \Rightarrow q$	$p \wedge (p \Rightarrow q)$	$p \wedge (p \Rightarrow q) \Rightarrow q$
$\top$	$\top$	$\top$	$\top$	$\top$
$\top$	$\bot$	$\bot$	$\bot$	$\top$
$\bot$	$\top$	$\top$	$\bot$	$\top$
$\bot$	$\bot$	$\top$	$\bot$	$\top$

As the truth tables become quite large for sentences with more than a few letters, the first approach used is more efficient and more elegant than using the truth tables.

Exercise 4. Show that the sentences below are tautologies without using the truth tables.

(1) $p \Rightarrow p \vee q$
(2) $p \Rightarrow (\neg p \Rightarrow q)$
(3) $\neg p \wedge \neg q \Rightarrow \neg(p \vee q)$

Solution. (1) Assume that p is true. As the disjunction is true if one of the terms of it is true and p is true, we have that $p \vee q$ is true.

(2) Assume that p is true. Then $\neg p$ is false. As the implication is true if the premise is false, we have that $\neg p \Rightarrow q$ is true.

(3) Assume that $\neg p \wedge \neg q$ is true. As a conjunction is true of both of its constituting sentences are true, we have that $\neg p$ and $\neg q$ are true, so both p and q are false. Then $p \vee q$ is false so $\neg(p \vee q)$ is true.

Recall that an alternative way to show that the three sentences above are tautologies is to create their truth tables and to check that the last column consists of only $\top$ values.

Showing that a sentence of the form $P \Rightarrow Q$ is not a tautology. Both sentences from Exercise 3 are not tautologies because their truth tables contain $\bot$ in the last column. A sentence of the form $P \Rightarrow Q$ is not a tautology if there are

$$\textit{truth values which make } P \textit{ true and } Q \textit{ false.}$$

If one is not interested in the entire truth function of a sentence but only whether a sentence is a tautology or not, one can argue as in the solution of the exercise below.

Exercise 5. Show that the sentences below are not tautologies without using the truth tables.

(1) $p \vee q \Rightarrow \neg p \wedge q$
(2) $\neg p \Rightarrow (\neg q \Rightarrow r)$

Solution. (1) Assume that $p \vee q$ is true and look for the truth values which make $\neg p \wedge q$ false. The truth of $p \vee q$ implies that either p or q is true. As $\neg p \wedge q$ is false if either p is true or q is false, we arrive to the values $\top$ for p and $\bot$ for q which make $p \vee q$ true and $\neg p \wedge q$ false. So, with these values, the implication $p \vee q \Rightarrow \neg p \wedge q$ is false. This answer is confirmed by the truth table from Exercise 3.

(2) Assume that $\neg p$ is true (so that p is false) and that $\neg q \Rightarrow r$ is false, so that $\neg q$ is true and r false. Thus, q is false. This brings us to the values $\bot, \bot, \bot$ for p, q and r which make the sentence false. This answer agrees with the truth table from Exercise 3.

Note that the truth values for the letters which make the sentence false may not be unique in general.

Logical equivalences. One particularly important group of tautologies are tautologies of the form $P \Leftrightarrow Q$ asserting that the sentences P and Q are **logically equivalent** that is, that P and Q have the same truth value for any truth value of their letters. To show that P and Q are logically equivalent, it is sufficient make a truth table listing all the possible values of P and Q and check that they are the same. In addition,

$$P \text{ and } Q \text{ are logically equivalent if and only if } P \models Q \text{ and } Q \models P.$$

Thus, to show that P and Q are logical equivalent, it is sufficient to show that $P \Rightarrow Q$ is a tautology and that $Q \Rightarrow P$ is a tautology. To show that P and Q are not logically equivalent, it is sufficient to show that either $P \Rightarrow Q$ is not a tautology or that $Q \Rightarrow P$ is not a tautology (note that one of these two implications may be a tautology).

The next exercise illustrate this.

Exercise 6. Show that the first two pairs of sentences below are logically equivalent and that the second two pairs of sentences are not logically equivalent.

(1) P is $p \Rightarrow q$ and Q is $\neg q \Rightarrow \neg p$.
(2) P is $p \Rightarrow (q \Rightarrow r)$ and Q is $p \wedge q \Rightarrow r$.
(3) P is p and Q is $p \wedge q$.
(4) P is $(p \Rightarrow q) \Rightarrow r$ and Q is $p \Rightarrow (q \Rightarrow r)$.

Solution.

(1) Showing that $P \Rightarrow Q$: assume that P is true. As Q is an implication, assume that the premise $\neg q$ is true, so q is false. As $p \Rightarrow q$ is true, then p has to be false. Hence, the conclusion $\neg p$ of Q is true, showing that Q is true.

Showing that $Q \Rightarrow P$: assume that Q is true. As P is an implication, assume that the premise p is true. As $\neg q \Rightarrow \neg p$ is true, and the conclusion $\neg p$ is false, the premise $\neq q$ has to be false. Hence, q is true. So, the conclusion q of P is true, showing that P is true.

(2) Showing that $P \Rightarrow Q$: assume that P is true. As Q is an implication, assume that the premise $p \wedge q$ is true, so both p and q are true. Thus, the premise p of P is true which means that the conclusion $q \Rightarrow r$ is also true. As the premise q of this implication is true, the conclusion r has to be true. This shows that the conclusion r of Q is true.

Showing that $Q \Rightarrow P$: assume that Q is true. As P is an implication, assume that the premise p is true, and show that the implication $q \Rightarrow r$ is true. To show that, assume that the premise q is true. Thus, both p and q are true and so the premise $p \wedge q$ of Q is true. As Q is true, this implies that the conclusion r is true. This shows that the conclusion r of the implication $q \Rightarrow r$ is true and so P holds.

(3) Note that Q is true if *both* p and q are true and P is true when p is true. Thus, Q is "strictly stronger" than P indicating that $P \Rightarrow Q$ is not a tautology. Indeed, if p is true and q is false, then P is true and Q is false.

(4) Try to develop a sense whether $P \Rightarrow Q$ is not a tautology or $Q \Rightarrow P$ is not a tautology (or both). In this case, the first implication is, in fact, a tautology (assuming that P and p and q are true, implies that r is true). So, we need to show that $Q \Rightarrow P$ is not a tautology. Assume that Q is true, that the premise $p \Rightarrow q$ of P is true, and that the conclusion r of P is false. Having the truth value for r, look for the values of p and q which make $p \Rightarrow q$ true and Q true. There is more than one option here, for example p being false and q being true, or both p and q being false. Either of these two assignments make Q true and P false.

Some widely used tautologies which have the form of logical equivalences include the associativity and commutativity laws for $\wedge$ and $\vee$.

Associativity for $\wedge$: $p \wedge (q \wedge r) \Leftrightarrow (p \wedge q) \wedge r$
Associativity for $\vee$: $p \vee (q \vee r) \Leftrightarrow (p \vee q) \vee r$

Associativity laws enable us not to consider parenthesis in expressions which contain multiple conjunctions or multiple disjunctions. For example, the sentence $((p \vee q) \vee r) \vee s$ can be written as $p \vee q \vee r \vee s$ without ambiguity. Note that $\Rightarrow$ is not associative (see part (2) of Exercise 2).

Commutativity for $\wedge$: $p \wedge q \Leftrightarrow q \wedge p$
Commutativity for $\vee$: $p \vee q \Leftrightarrow q \vee p$

One can establish the validity of these two tautologies by observing that the multiplication tables for $\wedge$ and $\vee$ are symmetric with respect to the "main diagonal" (the diagonal from the upper left to the bottom right part of the table).

We list some other widely used tautologies. Some of them we will use in the subsequent parts of the course.

Double Negation. $\neg\neg p \Leftrightarrow p$

This tautology implies that elimination of multiple appearances of negation results in equivalent sentences. For example, the sentence $\neg\neg\neg p \wedge \neg\neg q$ is logically equivalent to $\neg p \wedge q$.

De Morgan's laws. $\neg(p \wedge q) \Leftrightarrow \neg p \vee \neg q$ and $\neg(p \vee q) \Leftrightarrow \neg p \wedge \neg q$

The first De Morgan's and the Double Negation laws imply $p \wedge q$ is logically equivalent to

$$\neg(\neg p \vee \neg q).$$

Thus, for every sentence which contains $\wedge$, there is a logically equivalent sentence where every appearance of $\wedge$ is replaced by $\neg$ and $\vee$ by using equivalence of $P \wedge Q$ and $\neg(\neg P \vee \neg Q)$.

Analogously, the second De Morgan's law enable one to "eliminate" $\vee$ using $\wedge$ and $\neg$.

Idempotent laws. $p \wedge p \Leftrightarrow p$ and $p \vee p \Leftrightarrow p$
Distributivity for $\wedge$ and $\vee$. $p \wedge (q \vee r) \Leftrightarrow (p \wedge q) \vee (p \wedge r)$ and $p \vee (q \wedge r) \Leftrightarrow (p \vee q) \wedge (p \vee r)$

All of the above laws are widely used. For example, we use them to show identities for sets in section 3. When considering the connectives $\neg, \wedge$, and $\vee$ as operators, a structure called *Boolean algebra* can be defined by requiring these laws (and a few others) to hold.

Biconditional law. $(p \Leftrightarrow q) \Leftrightarrow (p \Rightarrow q) \wedge (q \Rightarrow p)$

This law asserts that *if and only if* is logically equivalent to *if* together with *if only*. It also specifies how an equivalence can be replaced by implications and and conjunction.

Material Implication. $(p \Rightarrow q) \Leftrightarrow \neg p \vee q$

By this law, every sentence which contains $\Rightarrow$, there is a logically equivalent sentence where every appearance of $\Rightarrow$ is replaced by $\neg$ and $\vee$.

Using Biconditional, De Morgan's law and Material Implication,

every sentence is equivalent with a sentence containing only $\neg$ *and* $\vee$.

Using the same laws,

every sentence is equivalent with a sentence containing only $\neg$ *and* $\wedge$.

The Material Implication and the Double Negation laws imply that $p \vee q$ is logically equivalent with $\neg p \Rightarrow q$. This enables one to "eliminate" $\vee$ using $\Rightarrow$. Thus, using this equivalence together with Biconditional and De Morgan's laws,

every sentence is equivalent with a sentence containing only $\neg$ *and* $\Rightarrow$.

The following tautology expands on the negation of an implication. We already used this law when showing that implication is false if the assumption is true and the conclusion false.

The negation of an implication. $\neg(p \Rightarrow q) \Leftrightarrow p \wedge \neg q$

Besides checking that this sentence is a tautology by writing down its truth table, we can show it is a tautology by using the existing tautologies as follows.

$$\begin{array}{lcll} \neg(p \Rightarrow q) & \Leftrightarrow & \neg(\neg p \vee q) & \text{(by Material Implication)} \\ & \Leftrightarrow & \neg\neg p \wedge \neg q & \text{(by De Morgan's law)} \\ & \Leftrightarrow & p \wedge \neg q & \text{(by Double Negation)} \end{array}$$

The following tautology is often used in mathematical proofs of statements which have a form of an implication.

Contrapositive. $(p \Rightarrow q) \Leftrightarrow (\neg q \Rightarrow \neg p)$

This law, whose validity was shown in Exercise 6, is often used when it may be easier to show the implication $\neg p \Rightarrow \neg q$ that the implication $p \Rightarrow q$. For example, the implication on real numbers a and b stating that

$$\text{if } ab \neq 0, \text{ then } a \neq 0 \text{ and } b \neq 0$$

is logically equivalent to

$$\text{if } a = 0 \text{ or } b = 0, \text{ then } ab = 0$$

by Contrapositive and De Morgan's law. This may be helpful because it might be easier to prove the latter implication (using the identities $0 \cdot b = 0$ and $a \cdot 0 = 0$) instead of the former implication.

Exportation. $(p \Rightarrow (q \Rightarrow r)) \Leftrightarrow (p \wedge q \Rightarrow r)$

This tautology, whose validity was shown in Exercise 6, enables one to prove a chain of implications of the form $P \Rightarrow (Q \Rightarrow R)$ by assuming that P and Q are true and showing that R is true.

Throughout the course, we will encounter and use the above tautologies and the logical reasoning resulting from them.

Exercise 7. Find a sentence which is logically equivalent to the given one and which contains only the specified connectives.

(1) $p \wedge q$ using $\neg$ and $\Rightarrow$
(2) $p \Rightarrow (q \Rightarrow r)$ using $\neg$ and $\wedge$.
(3) $\neg(p \Leftrightarrow q)$ using $\neg$ and $\vee$.

Solution.
(1) Using De Morgan's law, $p \wedge q$ is equivalent with $\neg(\neg p \vee \neg q)$. Using Material Implication, $\neg p \vee \neg q$ is equivalent with $p \Rightarrow \neg q$. Hence, $\neg(\neg p \vee \neg q)$ is equivalent to $\neg(p \Rightarrow \neg q)$.
(2) Using Material Implication, $p \Rightarrow (q \Rightarrow r)$ is equivalent to $p \Rightarrow (\neg q \vee r)$. Using it again for the first implication, we arrive to $\neg p \vee (\neg q \vee r)$. Using De Morgan's law for both disjunction, we obtain $\neg p \vee \neg(q \wedge \neg r)$ and then $\neg(p \wedge (q \wedge \neg r))$ which we may write as $\neg(p \wedge q \wedge \neg r)$, by associativity.

From this last form, note that it becomes readily obvious that $p \Rightarrow (q \Rightarrow r)$ is false exactly when p and q are true and r is false.

Alternatively, one can use Exportation to obtain that $p \wedge q \Rightarrow r$ is equivalent to the given sentence. Then, using Material Implication one obtains $\neg(p \wedge q) \vee r$ and then, using De Morgan's law, $\neg(p \wedge q \wedge \neg r)$.
(3) Using Biconditional $\neg(p \Leftrightarrow q)$ is equivalent to $\neg((p \Rightarrow q) \wedge (q \Rightarrow p))$. Using De Morgan's law, this is equivalent to $\neg(p \Rightarrow q) \vee \neg(q \Rightarrow p)$. Using Material Implication, this is equivalent to $\neg(\neg p \vee q) \vee \neg(\neg q \vee p)$.

Contradiction, contingent and consistent sentences. A statement which is false for all possible truth values of its statement letters is said to be a **contradiction**.

Sometimes, the symbol $\lightning$ is used to denote a contradiction. A negation of a tautology is a contradiction. For example, the sentence $p \wedge \neg p$ is a contradiction. Note that it is equivalent to the negation of the tautology $p \vee \neg p$ by De Morgan's law and Double Negation.

A sentence is **contingent** if it is neither a tautology nor a contradiction (so there is at least one $\top$ and one $\bot$ among its truth values. Both sentences from Exercise 3 are examples of contingent sentences.

A set of sentences is **consistent** or **satisfiable** if it is logically possible for them all to be true at once. Thus, a single sentence is consistent if so there is at least one $\top$ among its truth values. Both sentences from Exercise 3 are consistent and, considered together, they are a consistent set of sentences. A set of sentences is **inconsistent** if it is not consistent.

Exercise 8.
(1) Check whether the following sentences are tautologies, contradictions or contingent sentences.
(a) $\neg(p \Rightarrow q) \Rightarrow (\neg p \Rightarrow \neg q)$

(b) $(\neg p \Rightarrow \neg q) \Rightarrow \neg(p \Rightarrow q)$

(2) Check whether the following sets of sentences are consistent or inconsistent.

(a) The set containing p, q, and $p \Rightarrow q$.

(b) The set containing $p, \neg q$, and $p \Rightarrow q$.

(c) The set containing $\neg(p \Rightarrow q)$ and $\neg p \Rightarrow q$.

Solution. (1) (a) The sentence is a tautology: assuming that $\neg(p \Rightarrow q)$ is true, we have that p is true and q is false. These values make $\neg p \Rightarrow \neg q$ an implication of the form $\bot \Rightarrow \top$ which is true.

(b) The sentence is contingent: the values $\top, \bot$ make it into an implication of the form $\top \Rightarrow \top$ which is true, and the values $\bot, \bot$ make it into an implication of the form $\top \Rightarrow \bot$ which is $\bot$.

(2) (a) The set is consistent since the values $\top, \top$ for p and q make all three sentences true.

(b) The set is inconsistent since if p and $\neg q$ are true, then p is true and q is false so the implication $p \Rightarrow q$ is false.

(c) The set is consistent since the values $\top$ and $\bot$ for p and q make both sentences true.

Practice Problems 1. (1) Given the abbreviation below, express the following English-language sentences into sentences of propositional logic.

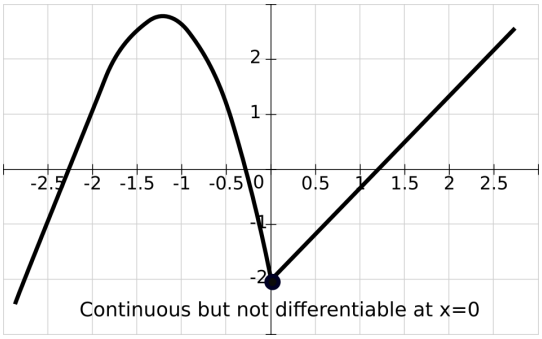
p stands for "Vee is happy."
q stands for "Bee is happy."

(a) Both Vee and Bee are happy.
(b) Bee is happy only if Vee is happy.
(c) For Vee to be happy, it is necessary that Bee is happy.
(d) Bee's happiness is sufficient for Vee's happiness.

(2) Using appropriate abbreviations, represent the next statements as sentences of propositional logic. Then, determine whether the arguments made in the sentences are valid.

For parts (a), (b), and (c), recall that a differentiable function is continuous. Any continuous function with a graph having a sharp turn or a corner at a point is not differentiable at that point.

For the remaining parts, recall that every prime number larger than 2 is odd. The converse is false (for example, 9 is an odd number which is not prime).



(a) A function is continuous only if it is differentiable.
(b) For a function to be continuous, it is sufficient to be differentiable.
(c) A continuous function is necessary differentiable.
(d) A number larger than 2 is prime if it is odd.
(e) A number larger than 2 is prime only if it is odd.
(f) For a number larger than 2 to be prime, it is necessary that it is odd.

(g) For a number larger than 2 to be prime, it is sufficient that it is odd.

(3) For all the sentences below which are sentences of propositional logic, restore all parentheses.
   (a) $(\neg p \Rightarrow \neg q \wedge r) \Rightarrow q \wedge (p \Rightarrow r)$
   (b) $p \wedge q \Rightarrow \neg p \wedge r \Rightarrow \neg q$
   (c) $\neg p \vee \neg q \Leftrightarrow (\neg p \Rightarrow p \vee q)$

(4) Write the truth tables for the following sentences.
   (a) $(\neg p \Rightarrow \neg q) \Rightarrow (p \Rightarrow q)$
   (b) $(p \Rightarrow (q \Rightarrow r)) \Rightarrow ((p \Rightarrow q) \Rightarrow (p \Rightarrow r))$

(5) Show that the sentences below are tautologies. Try not to use the truth tables.
   (a) $p \wedge q \Rightarrow p$
   (b) $\neg(p \vee q) \Rightarrow \neg p \wedge \neg q$
   (c) Material Implication: $(p \Rightarrow q) \Leftrightarrow \neg p \vee q$

(6) Show that the sentences below are not tautologies. Try not to use the truth tables.
   (a) $(p \Rightarrow q) \Rightarrow p \wedge \neg q$
   (b) $\neg p \Rightarrow (\neg q \Rightarrow p)$
   (c) $p \Leftrightarrow p \vee q$
   (d) $p \vee q \Leftrightarrow (p \Rightarrow r)$

(7) Find a sentence which is logically equivalent to the given one and which contains only the specified connectives.
   (a) $p \Rightarrow q$ using $\neg$ and $\wedge$
   (b) $p \Rightarrow (q \Rightarrow r)$ using $\neg$ and $\vee$.
   (c) $\neg p \Leftrightarrow q \vee r$ using $\neg$ and $\vee$.

(8) Check whether the following sentences are tautologies, contradictions or contingent sentences.
   (a) $(p \Rightarrow q) \Rightarrow \neg(q \Rightarrow p)$ (b) $(p \Leftrightarrow (p \Rightarrow q)) \Rightarrow q$

(9) Check whether the following sets of sentences are consistent or inconsistent.
   (a) The set containing p and $p \wedge \neg q$.
   (b) The set containing p, q and $p \wedge \neg q$.
   (c) The set containing $\neg(p \Rightarrow q)$ and $q \Rightarrow p$.

Solutions. (1) (a) $p \wedge q$, (b) $q \Rightarrow p$, (c) $p \Rightarrow q$, (d) $q \Rightarrow p$.

(2) For parts (a), (b), and (c), let p stand for "the function is continuous" and q for "the function is differentiable". By the given reminder of the Calculus 1 material, $q \Rightarrow p$ is true and $p \Rightarrow q$ can be false.

Part (a) can be represented as $p \Rightarrow q$, so it is not true. Part (b) states that $q \Rightarrow p$ so it is true. Part (c) states that $p \Rightarrow q$ so it is not true.

For the remaining parts, let p stand for "the number larger than 2 is prime" and q stand for "the number larger than 2 is odd". By number theory, $p \Rightarrow q$ is true and $q \Rightarrow p$ may not be true.

Part (d) states that $q \Rightarrow p$ so it is not true. Part (e) states that $p \Rightarrow q$ so it is true. Part (f) states that $p \Rightarrow q$ so it is true. Part (g) states that $q \Rightarrow p$, so it is false.

(3) (a) $(((\neg p) \Rightarrow ((\neg q)) \wedge r) \Rightarrow (q \wedge (p \Rightarrow r)))$
   (b) This is not a sentence of propositional logic: if P stands for $p \wedge q$, Q for $\neg p \wedge r$, and R for $\neg q$, it is not clear whether it is supposed to abbreviate $(P \Rightarrow Q) \Rightarrow R$ or $P \Rightarrow (Q \Rightarrow R)$.
   (c) $(((\neg p) \vee (\neg q)) \Leftrightarrow ((\neg p) \Rightarrow (p \vee q)))$

(4) (a)

p	q	$\neg p$	$\neg q$	$\neg p \Rightarrow \neg q$	$p \Rightarrow q$	$(\neg p \Rightarrow \neg q) \Rightarrow (p \Rightarrow q)$
$\top$	$\top$	$\bot$	$\bot$	$\top$	$\top$	$\top$
$\top$	$\bot$	$\bot$	$\top$	$\top$	$\bot$	$\bot$
$\bot$	$\top$	$\top$	$\bot$	$\bot$	$\top$	$\top$
$\bot$	$\bot$	$\top$	$\top$	$\top$	$\top$	$\top$

(b) Let P stands for $(p \Rightarrow (q \Rightarrow r)) \Rightarrow ((p \Rightarrow q) \Rightarrow (p \Rightarrow r))$.

p	q	r	$q \Rightarrow r$	$p \Rightarrow (q \Rightarrow r)$	$p \Rightarrow q$	$p \Rightarrow r$	$(p \Rightarrow q) \Rightarrow (p \Rightarrow r)$	P
$\top$	$\top$	$\top$	$\top$	$\top$	$\top$	$\top$	$\top$	$\top$
$\top$	$\top$	$\bot$	$\bot$	$\bot$	$\top$	$\bot$	$\bot$	$\top$
$\top$	$\bot$	$\top$	$\top$	$\top$	$\bot$	$\top$	$\top$	$\top$
$\top$	$\bot$	$\bot$	$\top$	$\top$	$\bot$	$\bot$	$\top$	$\top$
$\bot$	$\top$	$\top$	$\top$	$\top$	$\top$	$\top$	$\top$	$\top$
$\bot$	$\top$	$\bot$	$\bot$	$\top$	$\top$	$\top$	$\top$	$\top$
$\bot$	$\bot$	$\top$	$\top$	$\top$	$\top$	$\top$	$\top$	$\top$
$\bot$	$\bot$	$\bot$	$\top$	$\top$	$\top$	$\top$	$\top$	$\top$

This shows that P is, actually, a tautology.

(5) (a) Assume that $p \wedge q$ is true. Thus, both p and q are true. In particular, p is true , so the conclusion p of the implication holds.

(b) Assume that $\neg(p \vee q)$ is true. Thus, $p \vee q$ is false, so both p and q are false. This makes both $\neg p$ and $\neg q$ true, so the conclusion $\neg p \wedge \neg q$ is true.

(c) Since the sentence is an implication, we need to show both directions: $(p \Rightarrow q) \Rightarrow \neg p \vee q$ and $\neg p \vee q \Rightarrow (p \Rightarrow q)$.
To show $(p \Rightarrow q) \Rightarrow \neg p \vee q$, assume that the implication $p \Rightarrow q$ is true. This means that it is not the case that p is true and q is false. This is the only assignment which would make $\neg p \vee q$ false, so $\neg p \vee q$ is true.
To show $\neg p \vee q \Rightarrow (p \Rightarrow q)$, assume that $\neg p \vee q$ is true and that the assumption p of $p \Rightarrow q$ is true. As $\neg p$ is false and $\neg p \vee q$ is true, this makes q necessarily true.

(6) (a) Look for the truth values which make $p \Rightarrow q$ true and $p \wedge \neg q$ false. As $p \wedge \neg q$ is false, p is false and q is true. As this indeed makes $p \Rightarrow q$ true, the sentence is false for these truth value assignments.

(b) Look for the truth values which make $\neg p$ true and $\neg q \Rightarrow p$ false. Thus, $\neg q$ should be true and p false (so $\neg p$ is indeed true). Thus, if both p and q are false, the sentence is false.

(c) The disjunction $p \vee q$ is "strictly weaker" than p. So, show that $p \vee q \Rightarrow p$ is not a tautology which would imply that the given equivalence is not a tautology. Look for the truth values which make $p \vee q$ true and p false and conclude that if p is false and q is true, this indeed happens.

(d) Look for the truth values which make one side of the equivalence true and the other false. For example, if both p and q are false, $p \vee q$ is false and $p \Rightarrow r$ is true (regardless of the value of r). **Another option** would be to consider p and q to be true and r to be false. In this case, $p \vee q$ is true and $p \Rightarrow r$ is false.

(7) (a)

$$\begin{aligned} p \Rightarrow q &\Leftrightarrow \neg p \vee q && \text{(by Material Implication)} \\ &\Leftrightarrow \neg(\neg\neg p \wedge \neg q) && \text{(by De Morgan's law)} \\ &\Leftrightarrow \neg(p \wedge \neg q) && \text{(by Double Negation)} \end{aligned}$$

(b)

$$\begin{array}{rcll} p \Rightarrow (q \Rightarrow r) & \Leftrightarrow & \neg p \vee (q \Rightarrow r) & \text{(by Material Implication)} \\ & \Leftrightarrow & \neg p \vee (\neg q \vee r) & \text{(by Material Implication)} \end{array}$$

(c)

$$\begin{array}{rcll} \neg p \Leftrightarrow q \vee r & \Leftrightarrow & (\neg p \Rightarrow q \vee r) \wedge (q \vee r \Rightarrow \neg p) & \text{(by Biconditional Law)} \\ & \Leftrightarrow & (\neg\neg p \vee (q \vee r)) \wedge (\neg(q \vee r) \vee \neg p) & \text{(by Material Implication for both } \Rightarrow) \\ & \Leftrightarrow & (p \vee (q \vee r)) \wedge (\neg(q \vee r) \vee \neg p) & \text{(by Double Negation)} \\ & \Leftrightarrow & \neg(\neg(p \vee (q \vee r)) \vee \neg(\neg(q \vee r) \vee \neg p)) & \text{(by De Morgan's law)} \end{array}$$

(8) (a) The sentence $(p \Rightarrow q) \Rightarrow \neg(q \Rightarrow p)$ is contingent since the values $\top, \bot$ (and $\bot, \top$) make it true and the values $\top, \top$ (and $\bot, \bot$) make it false.

(b) The sentence $(p \Leftrightarrow (p \Rightarrow q)) \Rightarrow q$ is a tautology as the following truth table shows.

p	q	$p \Rightarrow q$	$p \Leftrightarrow (p \Rightarrow q)$	$(p \Leftrightarrow (p \Rightarrow q)) \Rightarrow q$
$\top$	$\top$	$\top$	$\top$	$\top$
$\top$	$\bot$	$\bot$	$\bot$	$\top$
$\bot$	$\top$	$\top$	$\bot$	$\top$
$\bot$	$\bot$	$\top$	$\bot$	$\top$

(9) (a) The set is consistent since the values $\top$ for p and $\bot$ for q make both sentences true.

(b) The set is inconsistent since if p and q are true, then $p \wedge \neg q$ is false so no truth value of p and q can make both sentences *simultaneously* true.

(c) The set is consistent since if p and q are true (and if they are both false) both sentences $\neg(p \Rightarrow q)$ and $q \Rightarrow p$ are true.

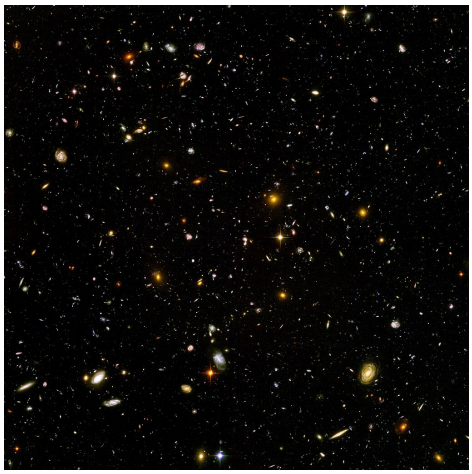
2. Predicate logic

Quantifiers. Let us revisit the logic inference mentioned in the first subsection of the previous section.

All men are mortal. Socrates is a man. Hence, Socrates is mortal.

The correctness of the first sentence "All men are mortal" cannot be determined by considering only the truth values of specific statements that one or the other person is mortal, because it makes a statement on a property of "all men". To represent this sentence in a formal system and to access its validity, we need a logic encompassing statements more general than only statements of propositional logic. In particular, the language of this wider theory should include the **universal quantifier** "for all" denoted by $\forall$.

If A is a certain property, and $A(x)$ means that x has property A, then $(\forall x)A(x)$ means that A holds for each possible x. For example "all men are mortal" can be represented by $(\forall x)A(x)$ if x is to stand for a person and $A(x)$ is to mean that a person x is mortal. In this example, the set of all people is the **domain of the interpretation** or the **universe of discourse**. The property A can be considered as a relation on the domain of the interpretation.



The following reasoning is also valid.

All men are mortal. Socrates is a man. Hence, there is a man who is mortal.

Let us examine the last sentence "There is a man who is mortal". To represent it using formulas, we introduce the **existential quantifier** "exists" denoted by $\exists$. If A is a property $(\exists x)A(x)$ stands for "there is x which has a property A. For example, if $A(x)$ means that a person x is mortal, $(\exists x)A(x)$ is used for "There is a man who is mortal".

Predicates. In the example above, the property A is neither true or false by itself – it becomes true when applied to specific person. For example, if a stands for "Socrates", the statement $A(a)$ abbreviates "Socrates is mortal" and it is true given that $(\forall x)A(x)$ is true and that a is a person.

We use lowercase letters $a, b, c, \ldots$ to denote **constants** which are assigned specific elements of the domain of certain interpretation. For example, specific people (Bee, Vee, Socrates etc) can be represented by constants of the interpretation in which the domain consists of the set of all people.

Properties of the elements of the domain of the interpretation are called the **predicates** or **relations**. For example, the properties of being mortal, having blond hair, or being a student are examples of predicates on the domain of all people. Properties of a single constant are called **unary or monadic** predicates. Properties of two constants are **binary or dyadic** predicates. Properties of n constants are **n-ary predicates.**

For example, somebody being jealous of somebody else is an example of a binary predicate. If $J(x, y)$ is to mean that the person x is jealous of the person y and if b denotes Bee and v denotes Vee, the statement "Bee is jealous of Vee" can be represented by $J(b, v)$. "Everybody

is jealous of somebody" can be represented by

$$(\forall x)(\exists y)J(x,y).$$

Exercise 9. Using appropriate abbreviations, represent the following statements using predicates and constants, negation, implication, or quantifiers, if needed. Assume that the domain of the interpretation is the set of all people.

(1) Bee is a blonde.
(2) Vee is not a blonde.
(3) There is somebody who is not a blonde.
(4) Not everybody is a blonde.
(5) If Vee is not a blonde then not everybody is a blonde.

Solution. Let $B(x)$ stand for "the person x is a blonde", b stands for Bee and v stands for Vee. The first sentence can be represented by $B(b)$, the second by $\neg B(v)$, the third by $(\exists x)\neg B(x)$, the fourth by $\neg(\forall x)B(x)$, and the fifth by $\neg B(v) \Rightarrow \neg(\forall x)B(x)$.

In the previous exercise, the sentences "Not everybody is a blonde" and "There is somebody who is not a blonde" are logically equivalent. In general, for any predicate B (not only for "being a blonde"), $(\exists x)\neg B(x)$ is equivalent to $\neg(\forall x)B(x)$. If $A(x)$ stands for $\neg B(x)$, for any predicate A,

$$(\exists x)A(x) \text{ is equivalent to } \neg(\forall x)\neg A(x)$$

which enables one to eliminate the use of the existential quantifier and use only the universal quantifier without altering the truthfulness of the statements.

Well-defined formulas of the predicate logic. We define statements, usually called the *well-defined formulas* or, shorter, formulas, of predicate logic recursively, analogously to the definition of sentences of propositional logic. The formulas are created using the following symbols.

(1) Variables $x, y, z, \ldots$
(2) Constants $a, b, c, \ldots$
(3) Predicate letters $A, B, C, \ldots$
(4) Parenthesis and the connectives of propositional logic $\neg, \wedge, \vee, \Rightarrow$, and $\Leftrightarrow$.
(5) Quantifiers $\forall$ and $\exists$.

One first defines the basic building blocks of the formulas called **atomic formulas**, recursively, as follows.

(1) Variables and constants are atomic formulas.
(2) If A is an n-ary predicate and $t_1, \ldots, t_n$ are atomic formulas, them $A(t_1, \ldots, t_n)$ is an atomic formula.
(3) Atomic formulas are created by a finite application of steps (1) and (2).

Usually, one uses function letters besides the predicate letters. As every function is a relation (as we will see in section 5), we opt to avoid using the function letters.

A **well-defined formula** (or a sentence or a statement) of the predicate logic is any expression obtained in the following way.

(1) All atomic formulas are well-defined formulas.

(2) If P and Q are well-defined formulas and x is a variable, then $(\neg P)$, $(P \wedge Q)$, $(P \vee Q)$, $(P \Rightarrow Q)$, $(P \Leftrightarrow Q)$, $(\forall x)P$, and $(\exists x)P$ are well-defined formulas.
(3) Any statement of predicate logic is obtained by finite number of application of steps (1) and (2).

For example, the formulas $(\exists x)(A(x) \vee B(x)), ((\neg A(a)) \Leftrightarrow (\forall y)A(y))$ are sentences of predicate logic while the formulas $(\forall x)$, $A(a)(\neg B(x))$, or $A(a) \wedge B(a))$ are not.

The predicate logic is also known as the **first-order logic, quantificational logic,** and **the first-order predicate calculus.** The "first-order" adjective refers to the fact that only variables, and not the predicates, are quantified. In contrast, the adjective "higher-order" is used if predicates or functions are quantified.

We use the same convention for **suppressing the use of parenthesis** in the predicate logic as in the propositional logic. In particular, $(\forall x)A(x)$ shortens $((\forall x)A(x))$ and $(\exists x)A(x)$ shortens $((\exists x)A(x))$.

In addition, the two quantifiers are considered to be stronger than $\Rightarrow$ and $\Leftrightarrow$. For example, this means that

$$(\forall x)A(x) \Rightarrow B(x) \quad \text{stands for} \quad ((\forall x)A(x)) \Rightarrow B(x) \text{ and that}$$
$$(\exists x)A(x) \Leftrightarrow B(x) \quad \text{stands for} \quad ((\exists x)A(x)) \Leftrightarrow B(x)$$

Sometimes, the quantifies are also considered to be weaker than $\vee$ and $\wedge$ and sometimes they are assumed to be the strongest. To avoid any confusion, we will not be making any of the two assumptions.

Exercise 10. For all the sentences below which are sentences of propositional logic, restore all parentheses.

(1) $(\forall x)(\exists y)A(x,y) \Rightarrow \neg B(x,y) \vee C(x)$.
(2) $(\forall x)A(x) \Rightarrow (\exists y)(\neg B(x,y) \vee C(x))$.
(3) $(\forall x)A(x) \Rightarrow ((\exists y)\neg B(x,y)) \vee ((\exists z)C(x,z))$.

Solution. (1) $(((\forall x)((\exists y)A(x,y))) \Rightarrow ((\neg B(x,y)) \vee C(x)))$.
(2) $(((\forall x)A(x)) \Rightarrow ((\exists y)((\neg B(x,y)) \vee C(x))))$.
(3) $(((\forall x)A(x)) \Rightarrow (((\exists y)(\neg B(x,y))) \vee ((\exists z)C(x,z)))))$.

Scope of a quantifier. Bound and free variables. If P is a well-defined formula which contains the variable x, P is the **scope** of the predicate $(\forall x)$ in the formula $(\forall x)P$ and of the predicate $(\exists x)$ in the formula $(\exists x)P$. If P does not contain x, $(\forall x)P$ and $(\exists x)P$ mean the same as P. If P is a well-defined formula which contains x and an occurrence of x in P is **bound** if it is of the form $(\forall x)$ or $(\exists x)$ or x lies within the scope of a quantifier $(\forall x)$ or $(\exists x)$. Otherwise, the occurrence of x is **free**. A variable x is **free** in a formula P if there is an occurrence of x in P which is free.

For example, both occurrences of both variables are free in $A(x,y)$ and all occurrences of both variables are bound in $(\forall x)(\exists y)A(x,y)$. In $(\forall x)A(x,y)$, all occurrences of x are bound and the occurrence of y is free.

Exercise 11. Determine whether each occurrence of each variable in the formula below is bound or free.

$$(\forall x)(\exists y)A(x,y) \Rightarrow \neg B(x,y) \vee C(x)$$

Solution. The variable x appears four times in the formula. The first two occurrences are bound and the second two are free. Thus, x is considered to be a free variable of the given formula.

The variable y appears three times in this formula. The first two occurrences are bound and the third one is free. Thus, x is considered to be a free variable of the given formula.

Interpretation of a formula. A well-defined formula can be true or false when a meaning is assigned to its constants, variables, and predicates. For example, $(\exists x)B(x)$ is true if $B(x)$ stands for "a person x is a blonde" and if it is given that Bee is a blonde. This example illustrates that the truth value of the formula may depend on the interpretation and its domain. For example, if B denotes the same predicate but the domain of the interpretation is the set of all chairs instead of all people, none of the chairs have hair, so none is a blonde which makes this formula false.

More formally, an **interpretation** of a well-defined formula consists of

(1) a non-empty set D, called the domain of the interpretation,
(2) an assignment of an element of D for each constant present it the list of the constant symbols used, and
(3) an assignment of a relation between the elements of D such that $A(a_1, \ldots, a_n)$ holds for each n-ary predicate A if and only if the elements assigned to the constants $a_1, \ldots, a_n$ are in the relation assigned to A.

To understand this better, let us consider the sentence

$$(\exists x)(\forall y)A(x,y).$$

If the domain is the set of all people, $A(x,y)$ is interpreted as "x is taller or equal in height to y", then this formula is true because the tallest person on the planet is taller or equal to height than any other person. This formula is also true if $A(x,y)$ is interpreted as "$x \leq y$" and the domain of the interpretation is the interval $[0,1]$ because 0 is less than or equal to any other number in this interval. However, if the domain of the interpretation is the set of all real numbers, then this formula is false because there is a number strictly smaller than any given real number.

Exercise 12. Assess the validity of the given formulas in the given interpretations.

(1) $(\forall x)(\exists y)A(x,y)$, the domain is the set of positive integers and $A(x,y)$ is interpreted as $x < y$.
(2) $(\forall x)(\exists y)A(x,y)$, the domain is the set consisting of the numbers $1, 2, 3, 4, 5$ and $A(x,y)$ is interpreted as $x < y$.

(3) $(\forall x)(\forall y)(A(x,y) \Rightarrow A(y,x))$, the domain is the set of real numbers and is interpreted as $x = y$.
(4) $(\forall x)(\forall y)(A(x,y) \Rightarrow A(y,x))$, the domain is the set of real numbers and is interpreted as $x > y$.
(5) $(\forall x)A(x) \Rightarrow A(a)$, the domain is the set of real numbers, a is 55, and $A(x)$ is interpreted as "x is a real number".

Solution. (1) The formula is true in this interpretation since, for every positive integer n, $n+1$, for example, is larger than n.

(2) The formula is false in this interpretation since no element of the domain is larger than 5.

(3) The formula is true in this interpretation since the relation $=$ is *symmetric* so that $a = b$ implies that $b = a$ for any real numbers a and b.

(4) The formula is false in this interpretation since if b is a real number larger than a then it is not the case that a is larger than b.

(5) The formula is true because the premise is true (every real number is indeed a real number) and the conclusion is true (55 is indeed a real number).

Tautologies. The formulas which are true in *every* interpretation play a special significance. Such formulas are analogous to tautologies in propositional logic. Besides the term "tautology" for such a formula, it is also said that such a formula is **logically valid.**

Let us consider the last formula in the previous exercise

$$(\forall x)A(x) \Rightarrow A(a).$$

If D is any set of objects, a is any of its elements and A is any relation the set of elements of D, assuming that the premise of the implication is true, we have that it is true that $A(d)$ holds for any d in D. So, by picking d to be a, we obtain that the conclusion $A(a)$ is also true. Thus, this formula is a tautology.

In a similar manner, one shows that

$$(\forall x)P(x) \Rightarrow P(a)$$

is a tautology for any well-defined formula P.

As another example, let us show that the formula

$$(\exists x)(\forall y)P(x,y) \Rightarrow (\forall y)(\exists x)P(x,y)$$

is a tautology for any well-defined formula P. If D is any set of objects and the predicates appearing in P are interpreted as any relations on D, assume that the premise $(\exists x)(\forall y)P(x,y)$ is true when interpreted on D. Hence, D contains an element a such that for every element b in D, $P(a,b)$ holds. Thus, for every element b, it is the case that there is an element of D (we can pick a to be that element) such that $P(a,b)$ holds. This shows that the conclusion $(\forall y)(\exists x)P(x,y)$ holds.

Showing that a formula is not a tautology. The converse implication in the previous example does not hold: the formula

$$(\forall x)(\exists y)P(x,y) \Rightarrow (\exists y)(\forall x)P(x,y) \text{ is not a tautology.}$$

To show that a formula is not a tautology, one needs to exhibit a set of objects and relations on them such that the formula fails when interpreted on the set of objects as its domain and its predicates interpreted as the relations on the set. For example, we can show that the above formula is not a tautology by noting that

For every integer there is a larger integer, but it is not the case that there is an integer larger than all other integers.

So, let D be the set of integers and let $P(x, y)$ stand for the atomic formula $x < y$. The premise $(\forall x)(\exists y)x < y$ is true since for every integer m, there is another integer n (for example take n to be $m + 1$) such that $m < n$. However, the conclusion is not true since there is no integer larger than all other integers so $(\exists y)(\forall x)x < y$ fails.

Logical implications and equivalences. The term **logical implication** is used in the same sense as in proposition logic: a well-defined formula P logically implies a well-defined formula Q if $P \Rightarrow Q$ is a tautology. The term **logical equivalence** is also used in the same sense as in proposition logic: a well-defined formula P is logically equivalent to a well-defined formula Q if $P \Leftrightarrow Q$ is a tautology.

Just as in propositional logic, some widely used tautologies have the form of logical implications or equivalences. We list some and we show that some of them are indeed tautologies.

The order of the quantifiers:
$$(\forall x)(\forall y)P(x, y) \Leftrightarrow (\forall y)(\forall x)P(x, y)$$
$$(\exists x)(\exists y)P(x, y) \Leftrightarrow (\exists y)(\exists x)P(x, y)$$
$$(\exists x)(\forall y)P(x, y) \Rightarrow (\forall y)(\exists x)P(x, y)$$

As we have seen in the previous example, the implication in this last formula cannot be reversed.

Renaming the variables:
$$(\forall x)P(x) \Leftrightarrow (\forall y)P(y)$$
$$(\exists x)P(x) \Leftrightarrow (\exists y)P(y)$$

For example, these two tautologies imply that the expression below is also a tautology

$$(\forall x)(\exists y)(\forall z)P(x, y, z) \Leftrightarrow (\forall y)(\exists z)(\forall x)P(y, z, x).$$

Universal quantification of free variables: $P \Leftrightarrow (\forall x)P$.

If P is a well-defined formula (it may contain x as a free variable or it may not contain it), then

$$P \Leftrightarrow (\forall x)P$$

is a tautology. This enables one to universally quantifies all the free variables in the formula. For example, to show that $P(x, y, z)$ is true for a well-defined formula with free variables x, y and z, it is equivalent to show that $(\forall x)(\forall y)(\forall z)P(x, y, z)$ is true.

Moving $\neg$ through quantifiers:
$$\neg(\forall x)P \Leftrightarrow (\exists x)\neg P$$
$$\neg(\exists x)P \Leftrightarrow (\forall x)\neg P$$

Moving quantifiers through $\wedge$ and $\vee$:
$$(\forall x)(P \wedge Q) \Leftrightarrow ((\forall x)P) \wedge ((\forall x)Q)$$
$$(\exists x)(P \vee Q) \Leftrightarrow ((\exists x)P) \vee ((\exists x)Q)$$
$$(\forall x)(P \vee Q) \Leftarrow ((\forall x)P) \vee ((\forall x)Q)$$
$$(\exists x)(P \wedge Q) \Rightarrow ((\exists x)P) \wedge ((\exists x)Q)$$

Exercise 13. Show that the formulas

$$((\forall x)P(x)) \vee ((\forall x)Q(x)) \Rightarrow (\forall x)(P(x) \vee Q(x)) \quad \text{and}$$

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

are tautologies and show that inverting the implications in these formulas produces formulas which are not tautologies.

Solution. Assume that the premise of the first formula is true, so $((\forall x)P(x)) \vee ((\forall x)Q(x))$ holds. This means that at least one of $(\forall x)P(x)$ and $(\forall x)Q(x)$ is true. If it is $(\forall x)P(x)$, then $P(a)$ holds for every constant a of every domain D, and so $P(a) \vee Q(a)$ is true on D for every a. Thus, $(\forall x)(P(x) \vee Q(x))$ is true.

Assume that the premise $(\exists x)(P(x) \wedge Q(x))$ is true. Thus, for every domain D, there is a constant a in D such that $P(a) \wedge Q(a)$ is true. This means that taking a for x makes both $(\exists x)P(x)$ and $(\exists x)Q(x)$ true. Hence, the conjunction $((\exists x)P(x)) \wedge ((\exists x)Q(x))$ is true.

To show that $(\forall x)(P(x) \vee Q(x)) \Rightarrow ((\forall x)P(x)) \vee ((\forall x)Q(x))$ is not a tautology, try to come up with a domain in which all the elements will have one or the other property, but in which not all the elements will have only one or only other property. For example, let D be a set $\{1, 2\}$, $P(x)$ be a predicate interpreted as "x is even" and $Q(x)$ be a predicate interpreted as "x is odd". The premise $(\forall x)(P(x) \vee Q(x)$ is true because it is true that every element of D is either even or odd. However, the conclusion $((\forall x)P(x)) \vee ((\forall x)Q(x))$ is false because it is neither the case that all elements of D are even nor that all elements of D are odd.

You do not have to come up with a "mathematical" interpretation. For example, D can be a set of three yellow and two green coffee mugs and $P(x)$ can stand for "x is yellow" and $Q(x)$ can stand for "x is green".

To show that $((\exists x)P(x)) \wedge ((\exists x)Q(x)) \Rightarrow (\exists x)(P(x) \wedge Q(x))$ is not a tautology, try to come up with a domain in which the elements which have one property will not have some other property. For example, we can again use the set $\{1, 2\}$ for D (or two coffee mugs, one green and the other yellow) and P and Q as above. With $\{1, 2\}$ for example, the premise $((\exists x)P(x)) \wedge ((\exists x)Q(x))$ is true D contains an even number, 2, and D contains an odd number 1. However, the conclusion is false because D contains no element which is simultaneously even and odd.

Using known tautologies to show a sentence is a tautology. Once when some tautologies become available, one can use them to show other tautologies.

Exercise 14. Show that the sentences below are tautologies by using sentences previously shown to be tautologies.

(1) $(\forall x)(\neg P(x) \wedge \neg Q(x)) \Leftrightarrow \neg((\exists x)P(x) \vee (\exists x)Q(x))$
(2) $(\forall x)(\forall y)(\exists z)P(x, y, z) \Leftrightarrow (\forall y)(\forall z)(\exists x)P(z, y, x)$

Solution.
(1) Using De Morgan's law, $(\forall x)(\neg P(x) \wedge \neg Q(x))$ is equivalent with $(\forall x)\neg(P(x) \vee Q(x))$. Moving $\neg$ through $\forall$, this last formula is equivalent with $\neg(\exists x)(P(x) \vee Q(x))$. Moving $\exists$ through $\vee$, this is equivalent with $\neg((\exists x)P(x) \vee (\exists x)Q(x))$.
(2) Renaming the variables x to y, y to z and z to x, we have that $(\forall x)(\forall y)(\exists z)P(x, y, z)$ is equivalent to $(\forall y)(\forall z)(\exists x)P(z, y, x)$.

Satisfiable sets of formulas. A set of formulas is satisfiable if there is an interpretation such that each formula is true in that interpretation.

For example, while the formula $(\forall x)(\exists y)P(x, y) \Rightarrow (\exists y)(\forall x)P(x, y)$ is not a tautology, it is satisfiable. Indeed, by considering D to be the set consisting of $1, 2, 3, 4, 5$ and $P(x, y)$ to be the atomic formula interpreted as $x \leq y$, we have that the premise of the implication in the formula is true because

if x is any of $1, 2, 3, 4, 5$ one can take y to be 5 and it is the case that $x \leq y$. The conclusion is also true because by taking 5 for y again, it is the case that any other element of the set is smaller or equal to 5.

Exercise 15. Determine whether the sets consisting of each of the following groups of sentences are satisfiable.

(1) $(\exists x)P(x) \Rightarrow (\forall x)P(x)$.
(2) $(\exists x)P(x)$, $(\forall x)\neg P(x)$.
(3) $(\exists x)(\forall y)P(x, y)$, $(\forall x)(\forall y)(P(x, y) \Rightarrow \neg P(y, x))$

Solution. (1) While the given formula is not a tautology, it is satisfiable. For example, think of a domain consisting of only one element which satisfies some property P, so that both the premise and the conclusion of the implication are true. For example, D is the set consisting of a single blue chair and $P(x)$ stands for "x is blue".

You can also think of a property and a domain whose all elements have it so that the conclusion is always true and, hence, so is the implication. For example, let D be the set of positive integers and $P(x)$ stand for "x is a positive integer".

(2) The two formulas are not simultaneously satisfiable because if $P(x)$ holds for some x, then it cannot be the case that $\neg P(x)$ holds for all x.

Alternatively, you can argue that the second formula is equivalent to $\neg(\exists x)P(x)$, let Q stand for $(\exists x)P(x)$ and note that $Q \wedge \neg Q$ is a contradiction, hence not satisfiable.

(3) The set containing two given formulas is satisfiable. For example, take P to be a relation which is strict in the sense that if $P(x, y)$ holds then it is not the case that $P(y, x)$ holds, like, for example, the relation $<$ on a set of real numbers. To ensure that the first formula hold, restrict this set so it has the least element. For example, the set of real numbers in the interval $[0, 1]$, or the interval $[0, \infty)$. So, with $D = [0, 1]$, for example and $P(x, y)$ standing for $x < y$, we have that both formulas hold: the first because we can take x to be zero, and the second because if $x < y$ then it is not the case that $y < x$.

Restricted quantification. In many interpretations, we would like to restrict quantifiers to only a portion of the elements of the domain.

For example, when making statements about integers, we can let quantificator apply only to positive integers. If $A(x)$ is a predicate and we want to state that *a formula $P(x)$ holds for every x with property A,* we write

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

which shortens

$$(\forall x)(A(x) \Rightarrow P(x)).$$

Similarly, if we want to state that *a formula $P(x)$ holds for some x with property A,* we write

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

which shortens

$$(\exists x)(A(x) \wedge P(x)).$$

In the example when D is the set of integers and $A(x)$ stands for $x > 0$, we write

$$(\forall x : x > 0)P(x) \text{ shorter as } (\forall x > 0)P(x)$$

and

$$(\exists x : x > 0)P(x) \text{ shorter as } (\exists x > 0)P(x).$$

The rules for moving $\neg$ through restricted quantifiers are the same as for nonrestricted quantifiers.

Moving $\neg$ through restricted quantifiers: $\neg(\forall x : A(x))P \Leftrightarrow (\exists x : A(x))\neg P$
$\neg(\exists x : A(x))P \Leftrightarrow (\forall x : A(x))\neg P$

To illustrate the validity of the first rule above, let us assume that $\neg(\forall x : A(x))P$ is true and recall that this shortens $\neg(\forall x)(A(x) \Rightarrow P)$. Using tautology for moving $\neg$ through (unrestricted) universal quantifier, we obtain that this is equivalent with $(\exists x)\neg(A(x) \Rightarrow P)$. As the implication $A(x) \Rightarrow P$ fails if $A(x)$ is true and P false, this is equivalent with $(\exists x)(A(x) \wedge \neg P)$. This last formula can be written shorter as $(\exists x : A(x))\neg P$. The converse is shown reversing the steps of the above proof.

Real analysis example. Restricted formula quantification appears in many statements of different branches of mathematics. For example, the definition of a real-valued function f being *continuous* at a real number x_0 contains as many as three restricted quantifiers. If a set of real numbers D is the domain of f, f is continuous at x_0 in D if

> for every positive real number ε there is a positive real number δ such that for every real number x in the domain, if the distance from x to x_0 is less than δ, then the distance from $f(x)$ to $f(x_0)$ is less than ε.

Without going into the meaning meaning of this definition, let us consider purely syntax form of this statement and write it as a formula of predicate logic.

For brevity, we introduce the relation $\in$ which stands for "is an element of". So, saying that x is an element of the domain D, can be written shortly as $x \in D$. Note also that $|x - x_0| < \delta$ represents the statement that the distance from x to x_0 is less than δ and $|f(x) - f(x_0)| < \varepsilon$ represents the statement that the distance from $f(x)$ to $f(x_0)$ is less than ε. So, the definition above is represented by the formula below.

$$(\forall \varepsilon > 0)\ (\exists \delta > 0)\ (\forall x \in D)(|x - x_0| < \delta\ \Rightarrow\ |f(x) - f(x_0)| < \varepsilon)$$

Equally relevant to being able to check if a given function is continuous at a point, is being able to check if a given function is *not* continuous at a point, in other words, whether

$$\neg(\forall \varepsilon > 0)(\exists \delta > 0)(\forall x \in D)(|x - x_0| < \delta \Rightarrow |f(x) - f(x_0)| < \varepsilon)$$

holds. Next exercise helps you get an operational knowledge of checking that a function is not continuous at a given point.

Exercise 16. Move the negation through the quantifiers of the formula

$$\neg(\forall \varepsilon > 0)(\exists \delta > 0)(\forall x \in D)(|x - x_0| < \delta \Rightarrow |f(x) - f(x_0)| < \varepsilon)$$

and through connectives so that only the atomic formulas are negated.

Solution. Using the tautologies for moving $\neg$ through restricted quantification, we obtain that the above formula is equivalent with

$$(\exists \varepsilon > 0)(\forall \delta > 0)(\exists x \in D)\neg(|x - x_0| < \delta \Rightarrow |f(x) - f(x_0)| < \varepsilon).$$

As the implication is false if the premise is true and the conclusion false, the above formula is equivalent with

$$(\exists \varepsilon > 0)(\forall \delta > 0)(\exists x \in D)(|x - x_0| < \delta \wedge \neg|f(x) - f(x_0)| < \varepsilon).$$

We can write it shortly as

$$(\exists \varepsilon > 0)(\forall \delta > 0)(\exists x \in D)(|x - x_0| < \delta \wedge |f(x) - f(x_0)| \geq \varepsilon).$$

Thus, to show that f is not continuous at x_0, one needs to find a positive number ε such that for all positive numbers δ there is x in the domain such that the distance from x to x_0 is smaller than δ and the distance from $f(x)$ to $f(x_0)$ is larger or equal to ε.

Practice Problems 2. (1) Using appropriate abbreviations, represent the following statements using predicates and constants, negation, implication, or quantifiers, if needed. Assume that the domain of the interpretation is the set of all positive integers. Then, determine whether the sentences are true in this interpretation.

$A(x, y)$ stands for "y is divisible by x".
$B(x)$ stands for "x is even".
$C(x)$ stands for "x is prime".
Constants $1, 2, 3, \ldots$ have the obvious interpretations.

(a) Every positive integer divisible by 6 is divisible by 3.
(b) There is a positive integer divisible by 3 and not divisible by 6.
(c) Every positive integer divisible by 2 is even.
(d) Every positive integer which is prime is odd.
(e) Every prime positive integer divisible by 3 is such that 3 is divisible by it.

(2) Use the interpretation as in the previous problem for the following.
(a) Find a sentence which uses only the predicate A which is equivalent with $B(x)$ (in other words, define "evenness" using only divisibility of numbers).
(b) Find a sentence which uses only the predicate A and equality relation which is equivalent with $C(x)$ (in other words, define "primeness" using divisibility of numbers and relation $=$).

(3) Restore all parentheses in the sentences below and determine whether each occurrence of a variable is bound or free.
(a) $(\forall x)A(x) \Leftrightarrow B(x) \wedge \neg C(x)$
(b) $(\forall y)A(y) \Leftrightarrow ((\forall x)A(x)) \vee ((\forall z)A(z))$
(c) $A(x, y) \wedge \neg B(x) \Rightarrow (\exists x)(\exists z)A(x, z)$.

(4) Assess the validity of the given formulas in the given interpretations.
(a) $(\exists x)(\forall y)A(x, y)$, the domain is the set of positive integers and $A(x, y)$ is interpreted as x divides y.
(b) $(\exists x)(\forall y)\neg A(x, y)$, the domain is the set of positive integers and $A(x, y)$ is interpreted as x divides y.
(c) $(\exists x)A(x) \Rightarrow (\forall x)A(x)$, the domain is the set of three blue and two red balls and $A(x)$ is interpreted as "x is red".

(d) $(\exists x)(\exists y)A(x,y) \Rightarrow (\exists x)A(x,x)$ where the domain is the set of positive integers and $A(x,y)$ is interpreted as $x < y$.
(e) $(\exists x)(\forall y)A(x,y)$, the domain is the interval $[0,1]$ and $A(x,y)$ is interpreted as $x \leq y$.
(f) $(\exists x)(\forall y)A(x,y)$, the domain is the interval $(0,1)$ and $A(x,y)$ is interpreted as $x \leq y$.

(5) Show that the sentences below are tautologies.
(a) $\neg(\exists x)P(x) \Leftrightarrow (\forall x)\neg P(x)$
(b) $(\forall x)(\forall y)P(x,y) \Rightarrow (\forall x)P(x,x)$
(c) $(\forall x)(P(x) \Rightarrow Q(x)) \Rightarrow ((\forall x)P(x) \Rightarrow (\forall x)Q(x))$
(d) $((\exists x)P(x) \Rightarrow (\forall x)Q(x)) \Rightarrow (\forall x)(P(x) \Rightarrow Q(x))$

(6) Show that the sentences below are not tautologies.
(a) $(\forall x)P(x,x) \Rightarrow (\forall x)(\forall y)P(x,y)$
(b) $(\exists x)P(x) \Rightarrow P(x)$
(c) $((\forall x)P(x) \Rightarrow (\forall x)Q(x)) \Rightarrow (\forall x)(P(x) \Rightarrow Q(x))$

(7) Show that the sentences below are tautologies by using sentences previously shown to be tautologies.
(a) $(\exists x)(\forall y)\neg P(x,y) \Leftrightarrow \neg(\forall y)(\exists x)P(y,x)$
(b) $((\exists x)(P(x) \Rightarrow Q(x)) \Leftrightarrow ((\forall x)P(x) \Rightarrow (\exists x)Q(x))$

(8) Determine whether the sets consisting of each of the following groups of sentences are satisfiable.
(a) $(\exists x)P(x), (\exists x)Q(x), (\forall x)(P(x) \Rightarrow Q(x))$
(b) $(\exists x)P(x,x)$, $(\forall x)(\forall y)(\forall z)(P(x,y) \wedge P(y,z) \Rightarrow P(x,z))$

(9) Write the content of the following definitions as sentences of predicate logic. Use restricted quantification when necessary and $\in$ to denote "... is an element of ...". Recall that "the distance from x to y is smaller than a" corresponds to $|x-y| < a$.

Real Analysis and Topology use these definitions, but no understanding of the content of these definitions is presently required.

(a) A real-valued function f defined on an interval $[a,b]$ is *uniformly continuous* on $[a,b]$ if for every positive real number ε, there is positive real number δ such that for every x and y in $[a,b]$, if the distance from x to y is less than δ, then the distance from $f(x)$ to $f(y)$ is less than ε.

(b) A set C of real numbers is *closed* if for every real number x and every positive real number ε there is an element y of C such that if the distance from x to y is smaller than ε, then x is an element of C.

(c) A set O of real numbers is *open* if for every real number x in O, there is a positive real number ε such that for every real number y, if the distance from x to y is smaller than ε, then y is an element of O.

Closed and open

(10) Consider the negation of the formulas you obtained in the previous exercise. Move the negation through the quantifiers and connectives in those formulas.

Solutions. (1) (a) $(\forall x)(A(6,x) \Rightarrow A(3,x)$. This sentence is true in the given interpretation.
(b) $(\exists x)(A(3,x) \wedge \neg A(6,x))$. This sentence is also true in the given interpretation because taking 3 for x, for example, we have that $A(3,3)$ is true and $A(6,3)$ is false.

(c) $(\forall x)(A(2,x) \Rightarrow B(x))$. This sentence is true in the given interpretation.
(d) $(\forall x)(C(x) \Rightarrow \neg B(x))$. This sentence is not true in the given interpretation because 2 is a positive integer which is prime but it is not odd.
(e) $(\forall x)(C(x) \Rightarrow (A(3,x) \Rightarrow A(x,3)))$ or $(\forall x : C(x))(A(3,x) \Rightarrow A(x,3))$. This sentence is true in the given interpretation because if integer is prime and divisible by 3, then it is equal to 3 (so $x = 3$). As $A(3,3)$ holds, the conclusion of the implication holds.

(2) (a) The statement $B(x)$ is equivalent with $A(2,x)$ since a number is even if and only if 2 divides it.
(b) The statement $C(x)$ is $(\forall y)(A(y,x) \Rightarrow y = 1 \vee y = x)$ since a number x is prime if and only if its only divisors are 1 and x.

(3) (a) $(((\forall x)A(x)) \Leftrightarrow (B(x) \wedge (\neg C(x))))$. The first two occurrences of x are bound while the third and the fourth occurrences are free.
(b) $(((\forall y)A(y)) \Leftrightarrow (((\forall x)A(x)) \vee ((\forall z)A(z))))$. All the variables occurring in the formula are bound.
(c) $((A(x,y) \wedge (\neg B(x))) \Rightarrow ((\exists x)((\exists z)A(x,z))))$. The first two occurrences of x are free and the third and the fourth are bound. The only occurrence of y is free. Both occurrences of z are bound.

(4) (a) $(\exists x)(\forall y)A(x,y)$ is true because $x = 1$ divides any positive integer y.
(b) $(\exists x)(\forall y)\neg A(x,y)$ is false because it is not the case that there is a positive integer which does not divide any positive integer: any positive integer divides itself.
(c) $(\exists x)A(x) \Rightarrow (\forall x)A(x)$, is false because the premise is true (there is a red ball) but the conclusion is not (it is not the case that all balls are red).
(d) $(\exists x)(\exists y)A(x,y) \Rightarrow (\exists x)A(x,x)$ is false because the premise is true (there are positive integers, 2 and 3 for example, such that $2 < 3$) and the conclusion is false: $x < x$ holds for no positive integer x.
(e) $(\exists x)(\forall y)A(x,y)$ is true because $x = 0$ is less than or equal to any other number in $[0,1]$.
(f) $(\exists x)(\forall y)A(x,y)$ is false because the the interval $(0,1)$ does not contain any number x with the property that x is smaller than or equal to any y in $(0,1)$ (zero is not in $(0,1)$ so $(0,1)$ does not have the minimal element.

(5) (a) Let us first show direction $\Rightarrow$. Assume that $\neg(\exists x)P(x)$ is true. So, it is not the case that $(\exists x)P(x)$ holds. This means that $P(a)$ holds for no element a of the domain of the interpretation. Thus, $\neg P(a)$ holds for every element a of the domain. Thus, $(\forall x)\neg P(x)$ holds.
The converse is similar: it is literally going over the same steps but in the reverse order. Assume that $(\forall x)\neg P(x)$ is true. So, $\neg P(a)$ holds for every element a of the domain of the interpretation. Thus, $P(a)$ holds for no element a of the domain and so it is not the case that $(\exists x)P(x)$ holds. Thus, $\neg(\exists x)P(x)$ holds.
(b) Assume that the premise $(\forall x)(\forall y)P(x,y)$ holds. So, $P(a,b)$ holds for every element a and every element b of the domain. In particular, by taking $b = a$, we have that $P(a,a)$ holds for every a in the domain. Thus the conclusion $(\forall x)P(x,x)$ holds.
(c) Assume that the premise $(\forall x)(P(x) \Rightarrow Q(x))$ holds and that the premise $(\forall x)P(x)$ of the conclusion we need to show also holds. Thus, both $P(a)$ and $P(a) \Rightarrow Q(a)$ hold for every element a of the domain, and, since the assumption $P(a)$ of $P(a) \Rightarrow Q(a)$ is true for every a, the conclusion $Q(a)$ holds for every a in the domain. Thus, $(\forall x)Q(x)$ holds.

(d) Assume that the assumption $((\exists x)P(x) \Rightarrow (\forall x)Q(x))$ is true. To show $(\forall x)(P(x) \Rightarrow Q(x))$, let a be an arbitrary element of the domain and let the premise $P(a)$ be true. This shows that the premise $(\exists x)P(x)$ of the implication $((\exists x)P(x) \Rightarrow (\forall x)Q(x))$ is true, so the conclusion $(\forall x)Q(x))$ is also true. Thus, $Q(a)$ holds. This shows that $(\forall x)(P(x) \Rightarrow Q(x))$ holds.

(6) (a) You can use a number set with a relation like $\leq$ or divisibility which fails to hold for every two elements. For example, with $\leq$ on the set of integers, $x \leq x$ holds for every integer x but $20 \leq 3$ fails, so the conclusion $(\forall x)(\forall y)P(x, y)$ fails.
You can also use some non-mathematical interpretation. For example, consider the set of red and blue balls and let $P(x, y)$ stand for "x has the same color as y". The premise $(\forall x)P(x, x)$ holds because every ball has the same color as itself. The conclusion $(\forall x)(\forall y)P(x, y)$ does not hold because not all the balls are of the same color.

(b) Any domain and its property which holds for some but not all of its elements can be used here. For example, the set of red and blue balls and $P(x)$ being "x is red". The premise $(\exists x)P(x)$ holds because there are some red balls. The conclusion $P(x)$ fails when x is taken to be one of the blue balls.

(c) We need an interpretation in which $(\forall x)P(x) \Rightarrow (\forall x)Q(x)$ is true and $(\forall x)(P(x) \Rightarrow Q(x))$ is not. So, let us choose a domain and two properties of its elements such that if $P(a)$ holds but not $Q(a)$ for some a. For example, let D be the set of blue and red balls, $P(x)$ be "x is red" and $Q(x)$ be "x is blue". As $(\forall x)P(x)$ fails, the implication $(\forall x)P(x) \Rightarrow (\forall x)Q(x)$ is true. The conclusion $(\forall x)(P(x) \Rightarrow Q(x))$ is false, because if a ball is red, then it is not the case that it is blue.

(7) (a)

$$\begin{array}{lcll} (\exists x)(\forall y)\neg P(x, y) & \Leftrightarrow & \neg(\forall x)\neg(\exists y)P(x, y) & \text{(by moving } \neg \text{ through } \forall) \\ & \Leftrightarrow & \neg(\forall x)(\exists y)P(x, y) & \text{(by moving } \neg \text{ through } \exists) \\ & \Leftrightarrow & \neg(\forall y)(\exists x)P(y, x) & \text{(by renaming, } x \text{ to } y, \text{ and } y \text{ to } x) \end{array}$$

(b) This tautology is on moving $\exists$ through $\Rightarrow$. Since we have analogous tautologies available for $\exists$ and $\vee$ and $\Rightarrow$ can be expressed in terms of $\vee$ by using Material Implication, start by using this rule.

$$\begin{array}{lcll} (\exists x)(P(x) \Rightarrow Q(x)) & \Leftrightarrow & (\exists x)(\neg P(x) \vee Q(x)) & \text{(by Material Implication)} \\ & \Leftrightarrow & (\exists x)\neg P(x) \vee (\exists x)Q(x) & \text{(by moving } \exists \text{ through } \vee) \\ & \Leftrightarrow & \neg(\forall x)P(x) \vee (\exists x)Q(x) & \text{(by moving } \neg \text{ through } \exists) \\ & \Leftrightarrow & (\forall x)P(x) \Rightarrow (\exists x)Q(x) & \text{(by Material Implication)} \end{array}$$

(8) (a) Any set some of which elements have properties P and Q such that P implies Q can make this set satisfiable. For example, set of positive integers with $P(x)$ being "x is divisible by 4" and $Q(x)$ being "x is divisible by 2" makes the given sentences satisfiable. Or, for example, a set of red balls and $P(x)$ being "x is red and x is a ball" and $Q(x)$ being "x is red".

(b) A number set with a relation like $=$, $\leq$ or $\geq$ makes the given sentences satisfiable. A set of positive integers with relation $|$ (divisibility) also makes the given sentences satisfiable.

(9) (a) $(\forall \varepsilon > 0)(\exists \delta > 0)(\forall x \in [a, b])(\forall y \in [a, b])(|x - y| < \delta \Rightarrow |f(x) - f(y)| < \varepsilon)$
(b) $(\forall x)(\forall \varepsilon > 0)(\exists y \in C)(|x - y| < \varepsilon \Rightarrow x \in C)$
(c) $(\forall x \in O)(\forall \varepsilon > 0)(\exists y)(|x - y| < \varepsilon \Rightarrow y \in O)$

(10) (a) $(\exists \varepsilon > 0)(\forall \delta > 0)(\exists x \in [a, b])(\exists y \in [a, b])(|x - y| < \delta \wedge |f(x) - f(y)| \geq \varepsilon)$
(b) $(\exists x)(\exists \varepsilon > 0)(\forall y \in C)(|x - y| < \varepsilon \wedge \neg x \in C)$
(c) $(\exists x \in O)(\exists \varepsilon > 0)(\forall y)(|x - y| < \varepsilon \wedge \neg y \in O)$

3. Fundamentals of Set Theory

"Naive" set theory. A **set** is a collection of distinct objects, listed in any order. The elements of the set are listed separated by commas or represented by the defining property in curly brackets.

For example, the set A containing the elements $\square, \triangle, \Diamond$ is represented by

$$A = \{\square, \triangle, \Diamond\}.$$

The requirement that the elements are listed in any order means that the set $\{\Diamond, \triangle, \square\}$ is the same set as A. The requirement that the object in the set are distinct means that $\{\square, \square, \triangle\}$ is not a set.

The **membership relation** $\in$ is a basic relation of set theory. Recall that $\square \in A$ means that $\square$ is an element of the set A. The symbol $\notin$ is used for the negation of the relation $\in$. So, $\heartsuit \notin A$ stands for the statement that $\heartsuit$ is not an element of the set A.

If there are too many elements for them to all be listed, a set can be defined by specifying the property its elements have and the objects which are not the elements of it do not have. For example, if $P(x)$ is a sentence in a variable x which determines a property of certain objects, one can define a set B of elements having the property P by

$$B = \{x \,:\, P(x) \text{ holds}\} \quad \text{or} \quad B = \{x \mid P(x) \text{ holds}\}$$

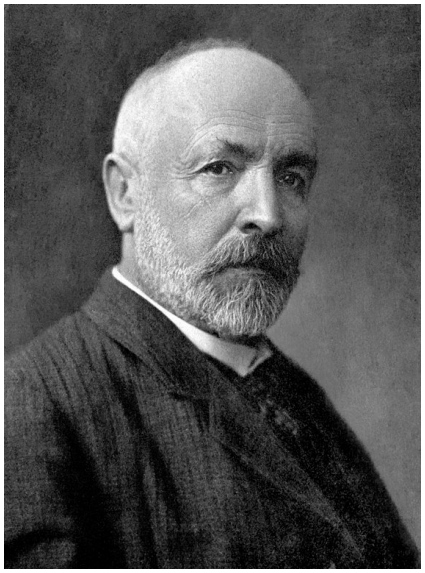
The symbol : (or |) stands for "... such that...", so the above formulas correspond to

B is the set of objects x such that $P(x)$ holds.

One can restrict the scope of elements of B by requiring that they come for another set C which is written by

$$B = \{x \in C \,:\, P(x) \text{ holds}\} \quad \text{or} \quad B = \{x \in C \mid P(x) \text{ holds}\}$$

The father of set theory. George Cantor played such an important role in establishment of the set theory that he is often referred to as its father. He introduced the concept of a bijective correspondence (so shall we in section 5). This made comparison of the sizes of different sets possible and led to proving that there are uncountably many real numbers.

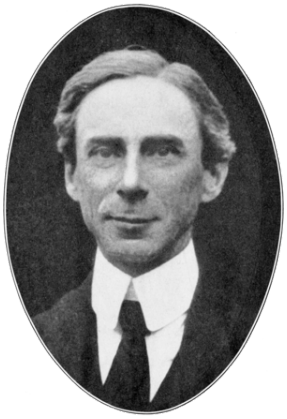


This challenged the established opinion that there were only finite set and that a single concept of "infinity" was in a realm of philosophy rather than mathematics – Cantor's work indicated that there are various levels of "infinity" to be considered. The need to study sets as concepts of a separate mathematical theory became evident after Cantor's introduction and treatment of more than one level of "infinity".

During his life, Cantor's work was often not well-received and some of the leading figures of mathematics at the time even refer to him as a "scientific charlatan", a "renegade", and a "corrupter of youth" and to his work as "utter nonsense", "laughable", and "wrong". Some of this criticism originated from the view that Cantor's theory was too non-constructive – it

asserted the existence of sets satisfying certain properties without producing them explicitly. Even those who appreciated Cantor's work did not always support it publicly: for example, a paper Cantor submitted to a journal was rejected with an explanation it was "... about one hundred years too soon."

During his life, Cantor suffered from depression because of such reception of his work. In the early 20th century, there was an increased appreciation and recognition of Cantor's work. David Hilbert, in particular, defended Cantor's work and is known to have said that "No one shall expel us from the paradise that Cantor has created." Besides these later accolades, Cantor continued to suffer from depression for the rest of his life.



Russell's paradox. Let us consider the case when $P(x)$ is the sentence stating that x is a set such that x is not an element of x (so $P(x)$ stands for $x \notin x$) and let R be the set defined by $P(x)$

$$R = \{x : x \notin x\}.$$

The notation R is used for "the Russell set" how this set is sometimes refer to.

The question is whether R is an element of R or not (and by the law of excluded middle we know that exactly one of the two possibilities have to be the case). So, either $R \in R$ or $R \notin R$.

If $R \in R$ holds, then $P(R)$ holds, so R has the property that it is not its own element, i.e. $R \notin R$ holds. This is a contradiction since we have that both $R \in R$ and $R \notin R$ hold.

On the other hand, if $R \notin R$ holds, then $P(R)$ fails, so R does not have the property that it is not its own element, i.e. R is an element of R so $R \in R$ holds. Thus, we arrive to the same contradiction: both $R \notin R$ and $R \in R$ hold.

This clearly presents a problem.

Russell published a paper containing this paradox in 1901. As it turned out, the same paradox has already been noted (but not published) by Ernst Zermelo in 1899 and by Georg Cantor himself during the late 1890s.

All the versions of the paradox lead to the same problem: one cannot pick just any property $P(x)$ to be used for defining a set A by

$$A = \{x : P(x)\}$$

without any restrictions, but the elements of A have to be *restricted* to being elements of already defined set B in which case A can be defined as

$$A = \{x \in B : P(x)\}.$$

This approach is called the **axiom schema of restricted comprehension** and the approach of the naive set theory is called **unrestricted comprehension.** This makes Russell's paradox

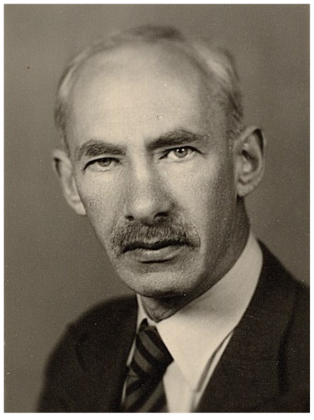
mute since elements of the Russell set R cannot be restricted to any other set: if R is defined as $\{x \in A : x \notin x\}$ for some set A, then the assumption that $R \in A$ leads to the same type of a contradiction: both $R \in R$ and $R \notin R$ would hold. So, it is simply the case that R is not an element of A.

The use of restricted comprehension became a standard way to approach definition of sets and became a part of the axiomatic set theory built by Zermelo, Abraham Fraenkel, and Thoralf Skolem which is called **ZFC theory** (Z for Zermelo, F for Fraenkel and C for "choice" indicating the use of the Axiom of Choice). Russell himself also suggested a theory which avoids unrestricted comprehension by using the *type theory* which considers certain hierarchy between "regular" sets and sets like R of higher complexity and, hence, of different type.



Ernst Zermelo, Abraham Fraenkel, and Thoralf Skolem

A related way to avoid unrestricted comprehension is consideration of *classes*, which is known today as **NGB theory**, introduced by John von Neumann, reformulated by Paul Bernays, and further simplified by Kurt Gödel. To summarize the idea of this theory without going into formal definitions, a class is a collection of objects which can be so large that "anything goes" for them. A class is a set if and only if it belongs to some other class. So, for example, Russell "set" R is a class which is not a set.


John von Neumann, Paul Bernays, and Kurt Gödel

Subset relation. Equality of two sets. A set A is a **subset** of a set B, written as $A \subseteq B$, if every element of A is also an element of B. This can be easy to directly check when the two sets contain only a few elements. For example, if $A = \{1, 2\}$ and $B = \{1, 2, 3\}$ then A is a subset of B.

One can show that A is a subset of B in general, even if the elements of the sets are not all explicitly listed, by showing the implication below

$$x \in A \quad \Rightarrow \quad x \in B$$

for any element x.

Exercise 17. Show that the relation $\subseteq$ is *transitive*, i.e. that

$$A \subseteq B \text{ and } B \subseteq C \text{ imply } A \subseteq C$$

Solution. Assume that $A \subseteq B$ and $B \subseteq C$ and let us show that $A \subseteq C$. So, we need to show that the implication $x \in A \Rightarrow x \in C$ holds for any x. Let x be an arbitrary element such that $x \in A$. Since $A \subseteq B$, we have that the implication $x \in A \Rightarrow x \in B$ holds. And, as $x \in A$, we can conclude that x is in B by Modus Ponens.

As $B \subseteq C$, we have that the implication $x \in B \Rightarrow x \in C$ holds. Since $x \in B$ holds, we can conclude that x is in C by Modus Ponens. So, we showed that x is an element of C which proves the implication needed for $A \subseteq C$.

Two sets are **equal** if they have the same elements. So, showing that sets A and B are equal (written $A = B$) boils down to showing the equivalence below

$$x \in A \quad \Leftrightarrow \quad x \in B$$

for any element x.

Many properties of sets can be shown by using tautologies.

Exercise 18. Show that

$$A = B \quad \text{if and only if} \quad A \subseteq B \text{ and } B \subseteq A$$

holds for any two sets A and B.

Solution. The needed equivalence can be shown as follows, using definitions and the appropriate tautology.

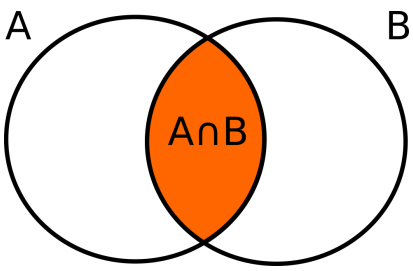
$$\begin{array}{lll} A = B & \Leftrightarrow & (\forall x)(x \in A \Leftrightarrow x \in B) \qquad \text{(by the definition of } = \text{)} \\ & \Leftrightarrow & (\forall x)\left((x \in A \Rightarrow x \in B) \wedge (x \in B \Rightarrow x \in A)\right) \qquad \text{(Biconditional law)} \\ & \Leftrightarrow & ((\forall x)(x \in A \Rightarrow x \in B)) \wedge ((\forall x)(x \in B \Rightarrow x \in A)) \qquad \text{(Moving } \forall \text{ through } \wedge\text{)} \\ & \Leftrightarrow & A \subseteq B \wedge B \subseteq A \qquad \text{(by the definition of } \subseteq\text{)} \end{array}$$

Having the relation $\subseteq$, one can define the strict subset relation $\subset$ by

$$A \subset B \quad \text{if} \quad A \subseteq B \text{ and } A \neq B.$$

For example, $\{1\}$ is strictly contained in $\{1, 2\}$ so we can write $\{1\} \subset \{1, 2\}$.

Operations on sets. The **intersection** $A \cap B$ of two sets A and B is a set consisting of elements which are in *both* sets. Thus,



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

Venn Diagrams can be used to represent operations on sets. The diagram representing the intersection of two sets is above.

Many set identities can be shown to hold by using corresponding tautologies. For example, showing commutativity for the intersection

$$A \cap B = B \cap A$$

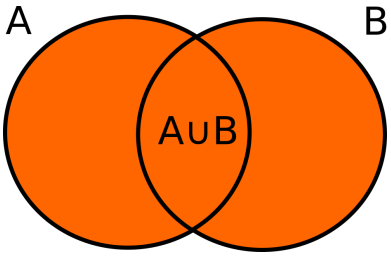
follows from commutativity of $\wedge$ as the following shows.

$$\begin{array}{rcll} x \in A \cap B & \Leftrightarrow & x \in A \wedge x \in B & \text{(by the definition of } \cap) \\ & \Leftrightarrow & x \in B \wedge x \in A & \text{(Commutativity of } \wedge) \\ & \Leftrightarrow & x \in B \cap A & \text{(by the definition of } \cap) \end{array}$$

The **union** $A \cup B$ of two sets A and B is a set consisting of elements which are in one or in the other set. Thus,

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

The diagram representing the union of two sets is on the right.



As $\vee$ is commutative and the union is defined via the disjunction, $A \cup B = B \cup A$ can be shown analogously to showing commutativity for the intersection. Since $\vee$ distributes to $\wedge$ and vice versa, the corresponding tautology and the definitions can be used to show distributivity of $\cup$ and $\cap$.

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C) \text{ and}$$
$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C).$$

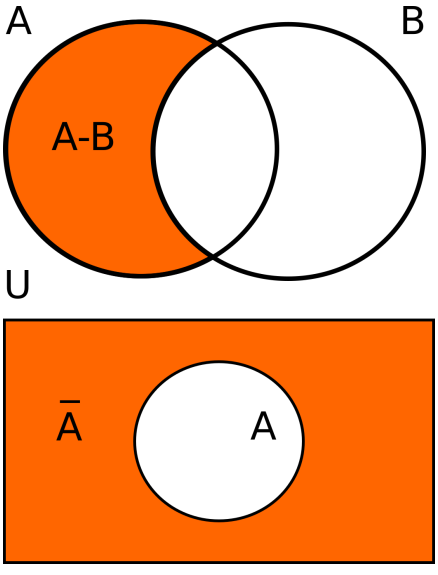
For example, the first formula above can be shown as follows.

$$\begin{array}{rcll} x \in A \cap (B \cup C) & \Leftrightarrow & x \in A \wedge x \in B \cup C & \text{(by the definition of } \cap) \\ & \Leftrightarrow & x \in A \wedge (x \in B \vee x \in C) & \text{(by the definition of } \cup) \\ & \Leftrightarrow & (x \in A \wedge x \in B) \vee (x \in A \wedge x \in C) & \text{(Distributivity of } \wedge \text{ and } \vee) \\ & \Leftrightarrow & x \in A \cap B \vee x \in A \cap C & \text{(by the definition of } \cap) \\ & \Leftrightarrow & x \in (A \cap B) \cup (A \cap C) & \text{(by the definition of } \cup) \end{array}$$

The **difference** $A - B$ of two sets A and B is a set consisting of elements which are in A but not in B. Thus,

$$A - B = \{x : x \in A \wedge x \notin B\}$$

If a set A is considered to be a subset of a set U (the notation U is used to implies that U is "universal" for A), the difference $U - A$ is the **complement** of A in U. We use notation $\overline{A}$ for the complement of A. The notations A^c and A' are also used for the complement. In practice, this universal set does not have to be explicitly given or mentioned – it is understood



that we are working within some general set of elements under our consideration. So, the set $\overline{A}$ effectively corresponds to the elements *not* in A and, thus, the operation of taking the complement corresponds to the *negation.*

Recall that De Morgan's laws specify how the negation moves through $\wedge$ and $\vee$. These laws can be used to show that

$$\overline{A \cap B} = \overline{A} \cup \overline{B} \text{ and}$$
$$\overline{A \cup B} = \overline{A} \cap \overline{B}.$$

For example, the first formula above can be shown as follows.

$$\begin{array}{rcll} x \in \overline{A \cap B} & \Leftrightarrow & \neg\, x \in A \cap B & \text{(by the definition of the complement)} \\ & \Leftrightarrow & \neg\, (x \in A \wedge x \in B) & \text{(by the definition of } \cap) \\ & \Leftrightarrow & \neg\, x \in A \vee \neg\, x \in B & \text{(by De Morgan's law)} \\ & \Leftrightarrow & x \in \overline{A} \vee x \in \overline{B} & \text{(by the definition of the complement)} \\ & \Leftrightarrow & x \in \overline{A} \cup \overline{B} & \text{(by the definition of } \cup) \end{array}$$

If the universal set U is considered as the set of all elements currently under consideration, then the formula $x \in U$ is considered to be true for any possible x and the identity

$$A \cup \overline{A} = U$$

corresponds to the law of the excluded middle. On the other hand, $A \cap \overline{A}$ consists of no elements as the sentence $p \wedge \neg p$ is a contradiction. We use $\emptyset$ to denote the set with no elements called **the empty set**. The notation $\{\}$ is also used for this set. So, we have that

$$A \cap \overline{A} = \emptyset$$

Since $x \in \emptyset$ is true for no elements x, showing that a certain set is equal to the empty set can often be shown by a **proof by contradiction**. To prove a certain statement P using a proof by contradiction, assume that P is false, derive a false statement out of it, and then conclude that, since $\neg P \Rightarrow \bot$, then $\neg P$ has to be false, so P is true. We illustrate this method in the next example.

Exercise 19. Show that $A \subseteq A - B$ is equivalent to $A \cap B = \emptyset$ for any two sets A and B.

Solution. As the statement we need to show is an equivalence, we need to show two directions, $A \subseteq A - B \Rightarrow A \cap B = \emptyset$ and $A \cap B = \emptyset \Rightarrow A \subseteq A - B$.

To show the direction ($\Rightarrow$), assume that $A \subseteq A - B$ and let us show that $A \cap B = \emptyset$. Assume, on the contrary, that there is $x \in A \cap B$. Then $x \in A$ and $x \in B$ are both true. As $x \in A$ and $A \subseteq A - B$, we have that $x \in A - B$. By definition of the difference, this means that $x \in A$ and $x \notin B$. So, we have now that both $x \in B$ and $x \notin B$ are true which is a contradiction (recall that $p \wedge \neg p$ is always false). Thus, our initial assumption that there is $x \in A \cap B$ is false, so $A \cap B$ contains no elements and, hence $A \cap B = \emptyset$. This finishes the proof of direction ($\Rightarrow$).

To show the direction ($\Leftarrow$), assume that $A \cap B = \emptyset$. We need to show that $A \subseteq A - B$. Let us use the proof by contradiction again. So, assume that it is not the case that $A \subseteq A - B$ which means that there is $x \in A$ which is not in $A - B$. As $x \notin A - B$, we have that the negation of the conjunction $x \in A \wedge x \notin B$ holds. By De Morgan's law, this means that the disjunction $x \notin A \vee x \in B$ holds. However, as x is in A the first term of this disjunction is false, so for the disjunction to be true, it is necessary that the second term $x \in B$ holds. Thus, we have that x is an element of both A and B and, hence, $x \in A \cap B$. This contradicts that $A \cap B$ is equal

to $\emptyset$. As we reached a contradiction, our assumption that $A \subseteq A - B$ is false cannot hold, so $A \subseteq A - B$ is true.

Note that all the operations and relations on sets can be completely paired up with logical connectives:

> *the operations* $\cap, \cup$, *and the complement correspond to* $\wedge, \vee$, *and* $\neg$ *and*
> *the relations* $=$ *and* $\subseteq$ *correspond to* $\Leftrightarrow$ *and* $\Rightarrow$.

Besides the set identities already given and paired up with corresponding tautologies, the table below lists some additional properties and their tautology counterparts.

set identity	**tautology**
$A \cap (B \cap C) = (A \cap B) \cap C$ $A \cup (B \cup C) = (A \cup B) \cup C$	associativity for $\wedge$ and $\vee$
$A \cap A = A$ $A \cup A = A$	idempotent laws for $\wedge$ and $\vee$
$\overline{\overline{A}} = A$	Double Negation law
$A = B \;\Leftrightarrow\; A \subseteq B \wedge B \subseteq A$	Biconditional law
$A \subseteq B \;\Leftrightarrow\; \overline{B} \subseteq \overline{A}$	Contrapositive
$A \subseteq B \;\Leftrightarrow\; \overline{A} \cup B = U$	Material Implication

Generalized intersection and union. An argument can be made that all of the above identities involve only up to three sets and Venn diagrams can be used for demonstrating their validity instead of definitions and tautologies. We adopted this more formal approach because it can be generalized to identities on intersection and union of possibly infinitely many sets.

So, let us consider I to be any set (we use I to indicate the *index set*) and let A_i be sets for any $i \in I$. The **generalized intersection**, denoted by $\bigcap_{i\in I} A_i$ is the set of all elements x which are in A_i for every $i \in I$. Thus,

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

The **generalized union**, denoted by $\bigcup_{i\in I} A_i$ is the set of all elements x which are in A_i for some $i \in I$. Thus,

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

If I is the set of natural numbers $I = \{1, 2, \ldots\}$, $\bigcap_{i\in I} A_i$ and $\bigcup_{i\in I} A_i$ are also written as

$$\bigcap_{i=1}^{\infty} A_i \quad \text{and} \quad \bigcup_{i=1}^{\infty} A_i$$

respectively.

Exercise 20. Show that

$$\overline{\bigcap_{i\in I} A_i} = \bigcup_{i\in I} \overline{A_i}$$

Solution.

$$\begin{array}{rcll} x \in \overline{\bigcap_{i\in I} A_i} & \Leftrightarrow & \neg\, x \in \bigcap_{i\in I} A_i & \text{(by the definition of the complement)} \\ & \Leftrightarrow & \neg\, (\forall i \in I)\; x \in A_i & \text{(by the definition of } \bigcap\text{)} \\ & \Leftrightarrow & (\exists i \in I)\; \neg\, x \in A_i & \text{(Distributing } \neg \text{ through } \forall\text{)} \\ & \Leftrightarrow & (\exists i \in I)\; x \in \overline{A_i} & \text{(by the definition of the complement)} \\ & \Leftrightarrow & x \in \bigcup_{i\in I} \overline{A_i} & \text{(by the definition of } \bigcup\text{)} \end{array}$$

The power set. If A is a set, the **power set** $\mathcal{P}(A)$ of A is the set which consists of all the subsets of A.

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

For example, if $A = \{1, 2\}$, then $\mathcal{P}(A)$ consists of four elements

$$\emptyset, \{1\}, \{2\}, \text{ and } \{1, 2\}.$$

Since the relations $\emptyset \subseteq A$ and $A \subseteq A$, hold for every set A (see the first practice problem below) $\emptyset$ and A are always elements of $\mathcal{P}(A)$. Note that in the case when $A = \emptyset$, $\mathcal{P}(A)$ has only one element $A = \emptyset$, so $\mathcal{P}(\emptyset) = \{\emptyset\}$.

The Cartesian product. If A and B are two sets, the **Cartesian product** $A \times B$ is the set of ordered pairs (a, b) where the first coordinate a is in A and the second b is in B.

$$A \times B = \{(a, b) : a \in A \wedge b \in B\}$$

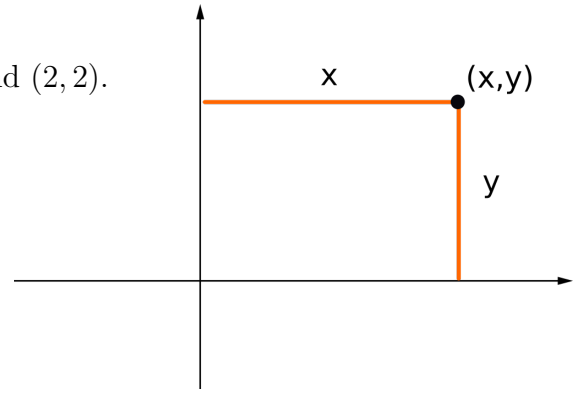
For example, if $A = \{1, 2\}$ and $B = \{\triangle, \square, \Diamond\}$, then $A \times B$ consists of six elements

$$(1, \triangle),\ (1, \square),\ (1, \Diamond)\ (2, \triangle),\ (2, \square),\ \text{and } (2, \Diamond)$$

and $A \times A$ consists of four elements

$$(1, 1),\ (1, 2),\ (2, 1),\ \text{and } (2, 2).$$

If $\mathbb{R}$ is used to denote the set of real numbers, then $\mathbb{R}\times\mathbb{R}$ is the set of points in xy-plane. Indeed, if we represent the first copy of $\mathbb{R}$ as numbers on the x-axis and the second copy of $\mathbb{R}$ as the numbers on the y-axis, then $\mathbb{R}\times\mathbb{R}$ consists of the ordered pairs (x, y) of real numbers which is exactly the content of the xy-plane.



By defining the product set via ordered pairs, we assumed a certain level of familiarity with the concept of an ordered pair of a reader. In the "epic search for truth" in which we are to build such a concept using sets only, an ordered pair (a, b), for a in some set A and b in some set B, can be defined as the element $\{\{a\}, \{a, b\}\}$ of $\mathcal{P}(\mathcal{P}(A \cup B))$. This definition enables one to deduce the difference between the first and the second entry of the element defining (a, b).

If n is a positive integer and $A_1, \ldots, A_n$ sets, one defines the Cartesian product $A_1 \times A_2 \times \ldots \times A_n$ as the set of n-tuples $(a_1, a_2, \ldots, a_n)$ such that $a_i \in A_i$ for every $i = 1, \ldots, n$. Thus,

$$A_1 \times A_2 \times \ldots \times A_n = \{(a_1, a_2, \ldots, a_n) : a_i \in A_i \text{ for every } i = 1, \ldots, n.\}$$

For example, if $A = \{1, 2\}$, $B = \{\triangle, \square, \Diamond\}$, and $C = \{c\}$ then $A \times B \times C$ consists of six elements

$$(1, \triangle, c),\ (1, \square, c),\ (1, \Diamond, c)\ (2, \triangle, c),\ (2, \square, c),\ \text{and } (2, \Diamond, c)$$

Note that $A \times B \times C$, $(A \times B) \times C$, and $A \times (B \times C)$ are all different sets. The second two consists of ordered pairs in which first or the second coordinate is an ordered pair itself, so they do not contain ordered triples. So, for example, $(1, \triangle, c)$ is an element of $A \times B \times C$ but not of $(A \times B) \times C$ nor $A \times (B \times C)$, $((1, \triangle), c)$ is an element of $(A \times B) \times C$ but not of $A \times B \times C$ nor $A \times (B \times C)$, and $(1, (\triangle, c))$ is an element of $A \times (B \times C)$ but not of $A \times B \times C$ nor $(A \times B) \times C$.

Cardinality. In all of our examples involving sets with "a few" elements, we made an intuitive reference to the **number of elements** of a set. For example, if $A = \{1, 2\}$, then the number of elements of A is two. Things are less clear if the number of elements of a set is not finite and the following questions may be relevant for our "epic search for truth".

(1) Do any two sets with infinitely many elements have the same number of elements?
(2) If not, how do we measure different infinities?
(3) What do we even mean by "the number of elements" if this number is not finite?
(4) If sets are to be the first step in building mathematics formally, what do we even mean by "a number"?

We shall be able to address all these questions, after introducing the concept of a *bijective correspondence* in section 5 and treat cardinality more rigorously in section 6.

Practice Problems 3.

(1) Show the following identities or statements in which $A, B, C,$ and D stand for arbitrary sets.
   (a) $\emptyset \subseteq A$
   (b) $A \subseteq A$
   (c) $A \cap B \subseteq A$
   (d) $A \subseteq A \cup B$
   (e) $A \subseteq B \;\Leftrightarrow\; \overline{B} \subseteq \overline{A}$
   (f) $A \times \emptyset = \emptyset \times A = \emptyset$
   (g) $A - B = A \cap \overline{B}$
   (h) $A \subseteq B \;\Leftrightarrow\; A \cap B = A$
   (i) $A \subseteq B \;\Leftrightarrow\; \mathcal{P}(A) \subseteq \mathcal{P}(B)$. When showing direction ($\Rightarrow$), you may need to use that the relation $\subseteq$ is transitive (see Exercise 17).
   (j) $A \subseteq B \;\wedge\; C \subseteq D \;\Rightarrow\; A \times C \subseteq B \times D$
   (k) $A \cup B = \emptyset \;\Leftrightarrow\; A = \emptyset \wedge B = \emptyset$
(2) Exhibit some sets A and B for which the following identities or statements hold.
   (a) $A - B \neq B - A$
   (b) $A \times B \neq B \times A$
(3) Determine $\bigcap_{n=1}^{\infty} A_n$ and $\bigcup_{n=1}^{\infty} A_n$ for given sets A_n where $n = 1, 2, \ldots$.
   (a) $A_n = \{n\}$
   (b) $A_n = \{1, 2, \ldots, n\}$,
   (c) $A_n = \{n, n+1, \ldots\}$
   (d) $A_n = \{\triangle\}$
   (e) $A_n = [0, n)$ where $[0, n)$ is the interval of real numbers between 0 and n including 0 (not including n).
(4) Let $A = \{1\}$ and $B = \{2, 3\}$. Determine the following sets.

$$\mathcal{P}(A),\;\; \mathcal{P}(B),\;\; \mathcal{P}(\mathcal{P}(A)),\;\; A \times B,\;\; \mathcal{P}(A \times B),\;\; \mathcal{P}(A) \times B,\;\; A \times \mathcal{P}(B),\;\; \mathcal{P}(A) \times \mathcal{P}(B).$$

Solutions. (1) (a) One needs to show that the implication $x \in \emptyset \Rightarrow x \in A$ holds for every x. Since the premise $x \in \emptyset$ is always false, the implication holds (recall that $\bot \Rightarrow p$ is true for any value of p).

(b) The implication $x \in A \Rightarrow x \in A$ is true since the sentence $p \Rightarrow p$ is a tautology.

(c)
$$\begin{array}{lll} A \subseteq B & \Leftrightarrow & (\forall x)(x \in A \Rightarrow x \in B) \quad \text{(by the definition of } \subseteq) \\ & \Leftrightarrow & (\forall x)(\neg x \in B \Rightarrow \neg x \in A) \quad \text{(by Contrapositive law)} \\ & \Leftrightarrow & (\forall x) x \in \overline{B} \Rightarrow x \in \overline{A} \quad \text{(by the definition of the complement)} \\ & \Leftrightarrow & \overline{B} \subseteq \overline{A} \quad \text{(by the definition of } \subseteq) \end{array}$$

(d) Assume that $x \in A \cap B$. Then $x \in A$ and $x \in B$, so $x \in A$ holds. This shows that the premise $x \in A \cap B$ implies $x \in A$. This shows that $A \cap B \subseteq A$.

(e) Assume that $x \in A$. Then the disjunction $x \in A$ or $x \in B$ is true, so $x \in A \cup B$. This shows that the premise $x \in A$ implies $x \in A \cup B$ so $A \subseteq A \cup B$.

(f) For any ordered pair (x, y), $(x, y) \in A \times \emptyset$ is equivalent with $x \in A$ and $y \in \emptyset$. Since the relation $y \in \emptyset$ is false, no such y exists, so no $(x, y) \in A \times \emptyset$ exists. This shows that $A \times \emptyset = \emptyset$. One shows that $\emptyset \times A = \emptyset$ similarly.

(g)
$$\begin{array}{lll} x \in A - B & \Leftrightarrow & x \in A \wedge \neg x \in B \quad \text{(by the definition of the difference)} \\ & \Leftrightarrow & x \in A \wedge x \in \overline{B} \quad \text{(by the definition of the complement)} \\ & \Leftrightarrow & x \in A \cap \overline{B} \quad \text{(by the definition of the intersection)} \end{array}$$

(h) Let us show the direction ($\Rightarrow$) first. Assume that $A \subseteq B$. Since $A \cap B \subseteq A$ (see problem 1c), to show $A \cap B = A$, it is sufficient to show that $A \subseteq A \cap B$. Assume that $x \in A$. Then x is also in B since $A \subseteq B$. So, the conjunction $x \in A$ and $x \in B$ is true. Thus, $x \in A \cap B$.
Let us show the direction ($\Leftarrow$) next. Assume that $A \cap B = A$ holds and let us show $A \subseteq B$. So, assuming $x \in A$, we need to show $x \in B$. If $x \in A$ then $x \in A \cap B$ since $A = A \cap B$. So, $x \in A$ and $x \in B$ both hold. In particular, $x \in B$ holds.

(i) To show the direction ($\Rightarrow$), assume that $A \subseteq B$ and let $C \in \mathcal{P}(A)$. Then $C \subseteq A$. So, we have that $C \subseteq A$ and that $A \subseteq B$. By transitivity of $\subseteq$, we have that $C \subseteq B$ so $C \in \mathcal{P}(B)$. This shows that $\mathcal{P}(A) \subseteq \mathcal{P}(B)$.
To show the direction ($\Leftarrow$), assume that $\mathcal{P}(A) \subseteq \mathcal{P}(B)$ and let us show that $A \subseteq B$. So, we need to show the implication $x \in A \Rightarrow x \in B$ for any x. Let $x \in A$. Thus, the set $\{x\}$ is a subset of A (because $x \in \{x\}$ is true and $x \in A$ is true so the implication $x \in \{x\} \Rightarrow x \in A$ is true). So, we have that $\{x\}$ is an element of $\mathcal{P}(A)$. As $\mathcal{P}(A) \subseteq \mathcal{P}(B)$, this implies that $\{x\}$ is an element of $\mathcal{P}(B)$. So, $\{x\}$ is a subset of B and, as x is in $\{x\}$ and the implication $x \in \{x\} \Rightarrow x \in B$ holds, we have that x is in B by Modus Ponens.

(j) Assume that $A \subseteq B$ and $C \subseteq D$ and show that $A \times C \subseteq B \times D$. So, we need to show that if $(a, c) \in A \times C$, then $(a, c) \in B \times D$. Assume that $(a, c) \in A \times C$, then $a \in A$ and $c \in C$. If $a \in A$ then $a \in B$ since $A \subseteq B$. If $c \in C$, then $c \in D$ since $C \subseteq D$. So, we have that $a \in B$ and $c \in D$ which implies that $(a, c) \in B \times D$.

(k)
$$\begin{array}{lll} A \cup B = \emptyset & \Leftrightarrow & \neg x \in A \cup B \quad \text{(by the definition of } \emptyset) \\ & \Leftrightarrow & \neg(x \in A \vee x \in B) \quad \text{(by the definition of } \cup) \\ & \Leftrightarrow & \neg x \in A \wedge \neg x \in B \quad \text{(by De Morgan's law)} \\ & \Leftrightarrow & A = \emptyset \wedge B = \emptyset \quad \text{(by the definition of } \emptyset) \end{array}$$

(2) (a) If $A = \{1, 2\}$ and $B = \{1\}$, for example, then $A - B = \{2\}$ and $B - A = \emptyset$. Another solution: if A is any nonempty set and $B = \emptyset$, then $A - B = A - \emptyset = A$ and $B - A = \emptyset - A = \emptyset$.

(b) Let $A = \{1\}$ and $B = \{2\}$. Then $A \times B = \{(1, 2)\}$ and $B \times A = \{(2, 1)\}$.

(3) (a) $\bigcap_{n=1}^{\infty} A_n = \{1\} \cap \{2\} \cap \{3\} \cap \ldots = \emptyset$ and $\bigcup_{n=1}^{\infty} A_n = \{1\} \cup \{2\} \cup \{3\} \cup \ldots = \{1, 2, 3, \ldots\}$.

(b) $\bigcap_{n=1}^{\infty} A_n = \{1\} \cap \{1, 2\} \cap \{1, 2, 3\} \cap \ldots = \{1\}$ and $\bigcup_{n=1}^{\infty} A_n = \{1\} \cup \{1, 2\} \cup \{1, 2, 3\} \cup \ldots = \{1, 2, 3, \ldots\}$.

(c) $\bigcap_{n=1}^{\infty} A_n = \{1, 2, 3, \ldots\} \cap \{2, 3, 4, \ldots\} \cap \ldots = \emptyset$ and $\bigcup_{n=1}^{\infty} A_n = \{1, 2, 3, \ldots\} \cup \{2, 3, 4, \ldots\} \cup \ldots = \{1, 2, 3, \ldots\}$.

(d) $\bigcap_{n=1}^{\infty} A_n = \{\triangle\} \cap \{\triangle\} \cap \ldots = \{\triangle\}$ and $\bigcup_{n=1}^{\infty} A_n = \{\triangle\} \cup \{\triangle\} \cup \ldots = \{\triangle\}$.

(e) $\bigcap_{n=1}^{\infty} A_n = [0, 1) \cap [0, 2) \cap [0, 3) \cap \ldots = [0, 1)$ and $\bigcup_{n=1}^{\infty} A_n = [0, 1) \cup [0, 2) \cup [0, 3) \cup \ldots [0, n) \cup \ldots = [0, \infty)$.

(4) If $A = \{1\}$, and $B = \{2, 3\}$, then

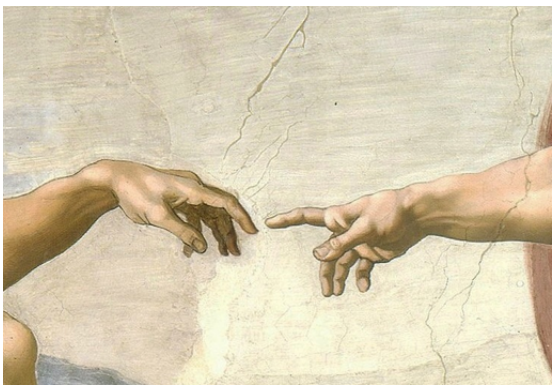
$$\mathcal{P}(A) = \{\emptyset, \{1\}\}, \quad P(B) = \{\emptyset, \{2\}, \{3\}, \{2, 3\}\}, \quad \mathcal{P}(\mathcal{P}(A)) = \{\emptyset, \{\emptyset\}, \{\{1\}\}, \{\emptyset, \{1\}\}\}.$$

$$A \times B = \{(1, 2), (1, 3)\}, \quad \mathcal{P}(A \times B) = \{\emptyset, \{(1, 2)\}, \{(1, 3)\}, \{(1, 2), (1, 3)\}\},$$

$$\mathcal{P}(A) \times B = \{(\emptyset, 2), (\emptyset, 3)(\{1\}, 2), (\{1\}, 3)\}, \quad A \times \mathcal{P}(B) = \{(1, \emptyset), (1, \{2\}), (1, \{3\}), (1, \{2, 3\})\}.$$

$$\mathcal{P}(A) \times \mathcal{P}(B) = \{(\emptyset, \emptyset), (\emptyset, \{2\}), (\emptyset, \{3\}), (\emptyset, \{2, 3\}), (\{1\}, \emptyset), (\{1\}, \{2\}), (\{1\}, \{3\}), (\{1\}, \{2, 3\})\}.$$

4. Relations



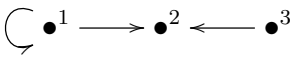
Binary relations. When introducing predicates and the sentences of predicate logic, we used a concept of a **relation**. Knowing the Cartesian product by now, we can make this concept more precise.

A **binary relation** R on sets A and B is any subset of $A \times B$. We write $(a, b) \in R$ as $R(a, b)$ or aRb and say that a and b are in the relation R. If $A = B$, we say that R is a **binary relation on** A.

For example, $=$ is a binary relation of any set A and (a, b) being in relation $=$ is written as $a = b$. As another example, $\subseteq$ is a binary relation on $\mathcal{P}(A)$ for any set A. If $\mathbb{R}$ is the set of real numbers, $\leq$ is a binary relation on $\mathbb{R}$.

A binary relation on a set A can be graphically represented by a **directed graph**: elements of A are the **vertices**, represented as points, of the graph and there is an **edge**, represented as an arrow connecting points, from the vertex representing $a \in A$ to the vertex representing $b \in A$ if aRb holds.

For example, if $A = \{1, 2, 3\}$ and R consists of the pairs $(1, 1), (1, 2), (3, 2)$, we can represent this relation by the graph below.



If n is a positive integer and $A_1, A_2, \ldots, A_n$ are sets, an **n-ary relation on** $A_1, A_2, \ldots, A_n$ is a subset of the set $A_1 \times A_2 \times \ldots \times A_n$. So, one can think of such a relation R as a property of some n-tuples.

For example, the relation R consisting of the triples of real numbers (x, y, z) such that $x + y = z$ is a ternary relation on $\mathbb{R}$.

If $n = 1$, the **unary relation** on a set A is any subset of A. So, one can think of an unary relation as distinguishing those elements of A which have some specific property. For example, the set of even integers constitutes an unary relation on the set of all integers and the set of positive real numbers is an unary relation on the set of all real numbers.

Because of their relevance for the definition of a function, we shall primary concentrate on binary relations. So, in what follows, by *a relation* we mean *a binary relation.*

An equivalence relation. As we shall see in sections 9 and 10, (binary) relations which "identify" the first and the second coordinate of the ordered pairs they contain are of relevance. To specify what we mean by "identify", we consider the following three properties of a relation R on a set A. Recall that we write aRb if the ordered pair (a, b) is in relation R.

(1) R is **reflexive** if aRa holds for every $a \in A$.
(2) R is **symmetric** if aRb implies bRa for every $a \in A$ and $b \in A$.
(3) R is **transitive** if aRb and bRc imply aRc for every $a \in A$, $b \in a$ and $c \in A$.

If R is a relation which has these three properties, we say that R is an **equivalence relation on** A.

The main example of an equivalence relation is the relation $=$ on any set A. It is clearly reflexive because $a = a$ holds for every a. It is symmetric because $a = b$ indeed implies $b = a$ and it is transitive because $a = b \wedge b = c \Rightarrow a = c$ holds.

When represented graphically, a relation is reflexive exactly when every vertex of its graph emits a *loop* $\bullet$⟲. A relation is symmetric exactly when for every edge from one vertex to the other one, there is an edge returning from the second to the first vertex $\bullet \rightleftarrows \bullet$. A relation is transitive exactly when there is a "direct route" for every path with a "layover": the bottom arrow has to exist if the two top arrows exist $\bullet \rightarrow \bullet \rightarrow \bullet$ and $\bullet \rightarrow \bullet$.

For example, if $A = \{1, 2, 3\}$ the graph below defines an equivalence relation

Below are further examples of equivalence relations.

Example 1. (1) Let $R = A \times A$ for any set A. Such a relation is called a **full relation** because it contains all possible ordered pairs. As R contains the "diagonal" $\{(a, a) : a \in A\}$, R is reflexive. Since R contains every possible ordered pair, both the premise and the conclusions of the implications defining symmetry and transitivity are true, so R is symmetric and transitive.

(2) Let $\mathbb{Z}$ be the set of integers and consider the relation $\equiv$ given by

$$m \equiv n \quad \text{if} \quad m - n \text{ is divisible by 2.}$$

As $m - m = 0$ and 0 is divisible by 2, this relation is reflexive. It is symmetric since if $n - m$ is even, then $m - n$ is also even, so $m \equiv n$ implies that $n \equiv m$. It is transitive since if $m \equiv n$ and $n \equiv k$, then both $m - n$ and $n - k$ are divisible by 2. Then, their sum $(m - n) + (n - k) = m - k$ is also divisible by 2.

There is nothing special about 2 in this example, so for any positive integer l, the relation on the set of integers given by $m \equiv n$ if $m - n$ is divisible by l is an equivalence relation. This shows that $m \equiv k$. This relation equates m and n **modulo l**.

(3) The relation **"being parallel to"** is an equivalence relation on the set of all planes in three dimensional space. Indeed, every plane is parallel to itself so this relation is reflexive. If a plane α is parallel to a plane β, then β is parallel to α also, so the relation is symmetric. If α is parallel to β and β is parallel to γ, then α is parallel to γ so the relation is transitive.

(4) Consider the set of nonnegative integers and let $\sim$ be the relation on this set given by

$$(k, l) \sim (m, n) \quad \text{if} \quad k + n = l + m.$$

Let us show that this relation is an equivalence relation.

Reflexivity. We need to show that $(k, l) \sim (k, l)$ for any nonnegative integers k and l.

$$\begin{aligned} (k, l) \sim (k, l) &\Leftrightarrow k + l = l + k \quad \text{(by the definition of } \sim) \\ &\Leftrightarrow k + l = k + l \quad \text{(by commutativity of } +) \end{aligned}$$

Since $k + l = k + l$ is true, we have that $(k, l) \sim (k, l)$ is also true.

Symmetry. Assume that $(k, l) \sim (m, n)$ for some $k, l, m, n \in \mathbb{N}$ and show that $(m, n) \sim (k, l)$.

$$\begin{aligned} (k, l) \sim (m, n) &\Leftrightarrow k + n = l + m \quad \text{(by the definition of } \sim) \\ &\Leftrightarrow m + l = n + k \quad \text{(by commutativity of } + \text{ and symmetry of } =) \\ &\Leftrightarrow (m, n) \sim (k, l) \quad \text{(by the definition of } \sim) \end{aligned}$$

Transitivity. Assume that $(k,l) \sim (m,n)$ and that $(m,n) \sim (o,p)$ and show that $(k,l) \sim (o,p)$.

$$\begin{aligned}
(k,l) \sim (m,n) \ \wedge \ (m,n) \sim (o,p) \ &\Leftrightarrow \ k+n = l+m \ \wedge \ m+p = n+o && \text{(by the definition of } \sim) \\
&\Rightarrow \ k+n+m+p = l+m+n+o && \text{(by adding the equations)} \\
&\Leftrightarrow \ k+p = l+o && \text{(by cancelling } n+m) \\
&\Leftrightarrow \ (k,l) \sim (o,p) && \text{(by the definition of } \sim)
\end{aligned}$$

This example may seem random right now, but it will be essential when forming integers from natural numbers in section 9. More generally, if you continue your study of mathematics, this type of relation is used when forming a *Grothendieck group* of a cancellative monoid.

We intend to use the symbol $\sim$ in larger generality than only in the previous example: we use it for a generic equivalence relation.

If $\sim$ is an equivalence relation on a set A, and $a \in A$, then the **equivalence class** $[a]$ of a consists of all elements of A which are in relation with a

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

So, one can think of $[a]$ as the set of all elements of A which $\sim$ *identifies* with a. Note that as $\sim$ is reflexive, $a \sim a$ for any $a \in A$ so $a \in [a]$ for any $a \in A$.

If $\sim$ is represented via graph, the equivalence class of an element a consists of all the elements whose vertices *connect* to the vertex labeled by a. For example, if $A = \{1,2,3\}$ and $\sim$ has the graph below,

then $[1] = \{1\}$ and $[2] = [3] = \{2,3\}$.

Exercise 21. Show that

$$[a] = [b] \quad \text{if and only if} \quad a \sim b.$$

Solution. If $[a] = [b]$ then $a \in [a] = [b]$, so $a \in [b]$ which implies that $b \sim a$ by definition of the equivalence class. Thus $a \sim b$ by symmetry. Conversely, if $a \sim b$, let us show that $[a] = [b]$. As $[a]$ and $[b]$ are sets, we need to show that $[a] \subseteq [b]$ and $[b] \subseteq [a]$ hold. To show $[a] \subseteq [b]$, assume that $c \in [a]$ and let us show $c \in [b]$.

The statement $c \in [a]$ means that $a \sim c$ by the definition of the equivalence class. And, as $a \sim b$, we have that $a \sim b$ and $a \sim c$ so $b \sim c$ by symmetry and transitivity. So, $c \in [b]$. This shows that $[a] \subseteq [b]$. The converse $[b] \subseteq [a]$ is shown analogously (fill the blanks for practice).

The set of all equivalence classes is the **quotient set** or the **factor set** $A/\sim$ of A with respect to $\sim$. Thus,

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

Thus, if one wishes to identify certain objects if they are "equal" in the eyes of a certain equivalence relation, then one can consider the set $A/\sim$ instead of the original set A. For example, if one is not interested in exact position of a plane in space, only in its "slope" (i.e the direction vector), then one can consider the quotient set of the set of all planes with respect to the equivalence "... is parallel to..." from part (3) of Example 1. This idea of "identifying" up to some equivalence appears when considering cardinality of sets, dimension of vector spaces, isomorphic groups, homeomorphic topological spaces, connected graphs, so it is rather fundamental for many areas of mathematics.

Let us consider the equivalence classes and the quotient sets of the set $A = \{1, 2, 3\}$ with respect to three different equivalence relations below.

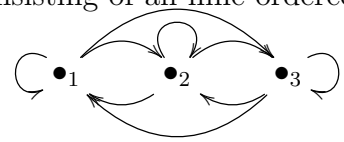
(1) The equality (i.e. the relation $\{(1, 1), (2, 2), (3, 3)\}$).

This relation identifies each element only with itself, so $[1] = \{1\}$, $[2] = \{2\}$ and $[3] = \{3\}$ and so the quotient set $A/\sim$ has three elements: $\{1\}, \{2\}$, and $\{3\}$.

(2) The relation $\sim$ given by

For this relation, $[1] = \{1\}$, $[2] = [3] = \{2, 3\}$ and so the quotient set $A/\sim$ consists of two elements $A/\sim = \{[1], [2]\} = \{\{1\}, \{2, 3\}\}$. Thus, the relation $\sim$ *identifies* 2 and 3 on A.

(3) The full relation $A \times A$ consisting of all nine ordered pairs in $A \times A$.



Here every element of A is in relation with any other element of A, so there is only one equivalence class $[1] = [2] = [3] = \{1, 2, 3\}$ and $A/\sim$ contains only one element $A/\sim = \{[1]\} = \{\{1, 2, 3\}\}$. Thus, the relation $\sim$ identifies all three elements of A.

(4) Let us describe the quotient set of the relation $\equiv$ from part (2) of Example 1. As all even integers are in relation $\equiv$, all odd numbers are in relation $\equiv$ with each other, and no even and odd integer are in this relation, we have that the equivalence class of any even integer $2n$ is equal to the equivalence class of 0 and it consists of all even integers. The equivalence class of any odd number $2n + 1$ is equal to the equivalence class of 1 and it consists of all odd integers.

Thus, $[0] = \{2n : n \in \mathbb{Z}\} = [2m]$ and $[1] = \{2n + 1 : n \in \mathbb{Z}\} = [2m + 1]$, for any nonegative integer m. So, all even numbers are identified with 0 and all odd numbers with 1 in the quotient set. As a result, the quotient set has two elements $[0]$ and $[1]$.

A partial order. If a *reflexive* and *transitive* relation R on a set A is also antisymmetric where

R is **antisymmetric** if aRb and bRa implies $a = b$ for every $a \in A$ and $b \in A$

then R is said to be a **partial order** on A and the set A is said to be a **poset** (to shorten "partially ordered set"). We use the symbol $\preceq$ to denote a relation which is a partial order.

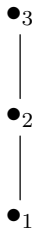
If a relation is represented via a directed graph, it is antisymmetric exactly when the loops are the only possible types of cycles (i.e. there are no cycles of length larger than 1). For example, the graph

defines a partial order on $A = \{1, 2, 3\}$ and the graph

does not define a partial order on A since the antisymmetry fails because of the presence of a cycle containing the vertices 1 and 2.

Another way to represent a relation which *is* a partial order is a type of diagram called a **Hasse diagram**. A Hasse diagram is an undirected graph in which a vertex corresponding to

a is graphed below a vertex corresponding to an element b if $a \preceq b$ and $a \neq b$. For example, if $A = \{1, 2, 3\}$, and $\preceq$ is defined by the first graph above, then $1 \preceq 2 \preceq 3$ holds, so its Hasse diagram is the graph below (much simpler than the directed graph representation).



Let us consider some other examples.

Example 2.
(1) The equality is a partial order on any set because it is reflexive and transitive and the implication $a = b \wedge b = a \Rightarrow a = b$ clearly holds.
(2) The relation $\subseteq$ on $\mathcal{P}(A)$ for any set A. The reflexivity holds since $B \subseteq B$ holds for any set B (see 1b in practice problems of section 3). The transitivity holds by Exercise 17 and the antisymmetry by Exercise 18.
(3) The relation $\leq$ on the set of real numbers $\mathbb{R}$. This relation is reflexive ($a \leq a$ indeed holds for any real number a) and transitive ($a \leq b$ and $b \leq c$ imply $a \leq c$). It is antisymmetric since $a \leq b$ and $b \leq a$ force a and b to be equal.
(4) The division relation $|$ on the set of positive integers is a partial order since n divides n for any positive integer n, if n divides k and k divides m, then n divides m, so it is reflexive and transitive. It is antisymmetric since if n divides k and k divides n, then they are necessarily equal.

Any partial order $\preceq$ on a set A defines a **strict partial order** $\prec$ by

$$a \prec b \quad \text{if} \quad a \preceq b \text{ and } a \neq b.$$

For example, the relation $\subseteq$ on $\mathcal{P}(A)$ for a set A gives rise to the relation $\subset$. For example, if $A = \{1, 2, 3\}$, then $\{1\} \subset \{1, 2\}$ and $\{1\} \subseteq \{1\}$ but $\{1\} \not\subset \{1\}$. The relation $\leq$ on $\mathbb{R}$ gives rise to the relation $<$ of "being strictly less than".

Greatest, least, maximal, and minimal elements, supremum and infimum. Let A be any set and $\preceq$ be a partial order on A. We introduce the following types of elements.

(1) $a \in A$ is **a greatest element** if $b \preceq a$ for every $b \in A$. Dually, $a \in A$ is **a least element** if $a \preceq b$ for every $b \in A$.

Let us show that a is a greatest element, then it is *unique* so that we can say that a is "the greatest element". Indeed, assume that both a_1 and a_2 are greatest elements of a set A partially ordered by $\preceq$. Thus, we have that $b \preceq a_1$ holds for every $b \in A$. So, by taking a_2 for b, we have that $a_2 \preceq a_1$. As a_2 is also a greatest element, $b \preceq a$ for every $b \in A$. By taking a_1 for b, we have that $a_1 \preceq a_2$. Thus, both $a_1 \preceq a_2$ and $a_2 \preceq a_1$ hold and so, as $\preceq$ is antisymmetric, we have that $a_1 = a_2$.

Analogous claim holds for a least element: if it exists, it is unique.

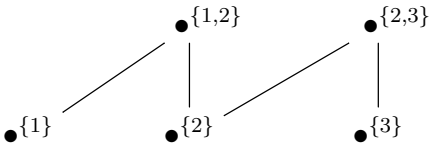
For example, A is the greatest element of $\mathcal{P}(A)$ considered with the partial order $\subseteq$ for any set A. The empty set is the least element of $\mathcal{P}(A)$.

Let us consider another example. The element 0 is the least and 1 is the greatest element of the closed interval $[0,1]$ of real numbers. On the other hand, the open interval $(0,1)$ does not have the greatest nor the least element because for every element of this open interval, say ε, there is a larger and a smaller element. For example, $\frac{\varepsilon}{2}$ is smaller than ε (and still larger than 0 since $\varepsilon > 0$) and $\varepsilon + \frac{1-\varepsilon}{2}$ is larger than ε (and still smaller than 1 since $\varepsilon + \frac{1-\varepsilon}{2} = \frac{1+\varepsilon}{2} < 1$ as $1 + \varepsilon < 1 + 1 = 2$).

(2) An element $a \in A$ is **a maximal element** of A if there is no element $b \in A$ which is strictly larger than a. To write this requirement by a formula, recall that $a \prec b$ stands for $a \preceq b$ and $a \neq b$. So, this requirement can be written as $\neg(\exists b \in A)(a \preceq b \wedge a \neq b)$. By passing negation through the quantifier and the connectives, we have that the condition is equivalent with $(\forall b \in A)(a \preceq b \Rightarrow a = b)$.

Dually, $a \in A$ is **a minimal element** of A if there is no element $b \in A$ which is strictly smaller than a. Equivalently, for all $b \in A$ if $b \preceq a$ then $a = b$.

As opposed to the greatest and the least elements, a maximal element and a minimal element are not necessarily unique. For example, let $A = \{1,2,3\}$ and B be a subset of $\mathcal{P}(A)$ consisting of $\{1\}, \{2\}, \{3\}, \{1,2\}$ and $\{2,3\}$. The relation $\subseteq$ is a partial order on B and the Hasse diagram for the poset B is below.



Thus, B has two maximal and three minimal elements and no greatest and no least elements. This example also shows that a maximal element does not have to be the greatest and a minimal element the least. Exercise 22 below explores the converse.

If $A = \{1,2,3\}$ and the partial order is $\leq$, on the other hand, then 1 is both the least and a minimal element and 3 is the greatest and a maximal element. As another example, if A is any set, then the greatest element A of $\mathcal{P}(A)$ is also a maximal element and $\emptyset$ is a minimal element. The open interval $(0,1)$, considered with $\leq$ does not have a maximal or a minimal element.

Exercise 22. For every set A with a partial order $\preceq$, if the greatest element exists, then it is also a maximal element. Dually, if the least element exists, then it also a minimal element.

Solution. If $a \in A$ is the greatest element, then $b \preceq a$ holds for any $b \in A$. Let us show that a is a maximal element by showing that $(\forall b \in A)(a \preceq b \Rightarrow a = b)$ holds.

So, let b be an arbitrary element of A and let us assume that $a \preceq b$ holds. As $b \preceq a$ also holds by the requirement that a is the greatest element, we have that $a = b$ by the antisymmetry.

The second sentence of the exercise can be shown analogously.

(3) If $B \subseteq A$, $a \in A$ is an **upper bound** of B if $b \preceq a$ for every $b \in B$. Note that such a may not be an element of B.

Dually, $a \in A$ is a **lower bound** of B if $a \preceq b$ for every $b \in B$.

For example, if $A = \{1,2,3\}$ and B is the subset of $\mathcal{P}(A)$ ordered by $\subseteq$ so that the Hasse diagram of B is the last figure above, then the set $\{1,2,3\}$ is an upper bound of B.

For another example, let A be the set of real numbers and B be the interval $(0,1)$. Then 2 is an upper bound of $(0,1)$ because 2 is larger than or equal to any element of $(0,1)$ and so are

3, π, $\sqrt{5}$ or any number larger than or equal to 1. The least upper bound, 1, of all these upper bounds have a special significance.

(4) If $B \subseteq A$, $a \in A$ is a **supremum** of B if a is the least element of the set of the upper bounds of B and $a \in A$ is an **infimum** of B if a is the greatest element of the set of the lower bounds of B.

As a supremum is the least element of certain set, if it exists it is unique. An infimum is also unique if it exists.

For example, 1 is the supremum of $(0, 1)$, ordered by $\leq$ and 0 is the infimum. This example illustrate the significance of supremum and infimum: they may exist even when a maximum and a minimum do not exist.

Total order. A partial order $\preceq$ on a set A enables us to establish a certain hierarchy between the set of elements which are in relation $\preceq$. However, we may not be able to "compare" every two elements of A. For example, if $A = \{\square, \triangle\}$ and then $\subseteq$ is a partial order on $\mathcal{P}(A)$ but the sets $\{\square\}$ and $\{\triangle\}$ are not "comparable" because neither is a subset of the other. This example contrasts the partial

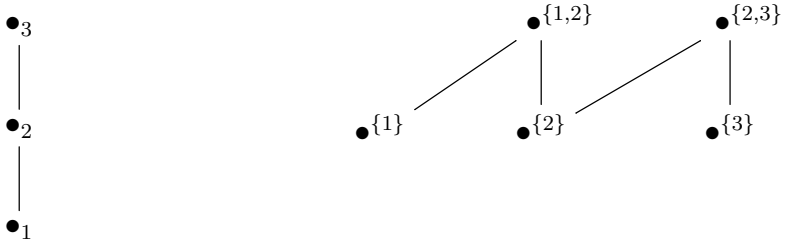
order $\leq$ on the set of real numbers because for any two real numbers a and b either $a \leq b$ or $b \leq a$ so one can "compare" any two such numbers. Partial orders with this property are called *total orders*.

More precisely, if a partial order $\preceq$ on a set A is such that

$$a \preceq b \text{ or } b \preceq a$$

holds for any $a \in A$ and $b \in A$, then $\preceq$ is a **total order.**

We have seen that $\subseteq$ may not be a total order and that $\leq$ is a total order on the set of real numbers. Similarly, the poset given by the first diagram below is a total order and the poset given by the second diagram below is not (neither $\{1, 2\}$ and $\{2, 3\}$ can be compared nor any pair of $\{1\}, \{2\}$ and $\{3\}$).



Practice Problems 4. (1) For a given set A and a relation $\sim$ on it, check whether the given equation $\sim$ is an equivalence relation. If it is, determine the quotient set.

(a) $A = \{1, 2, 3\}$ and $\sim$ consists of the ordered pairs $(1, 1), (2, 2), (3, 3), (1, 2), (2, 1)$, $(2, 3)$, $(3, 2)$.

(b) $A = \{1, 2, 3\}$ and $\sim$ consists of the ordered pairs $(1, 1), (2, 2), (3, 3), (1, 2), (2, 1)$, $(2, 3)$, $(1, 3)$, $(3, 1)$.

(c) A is the set of real numbers and $\sim$ is given by $a \sim b$ if $a^2 = b^2$.
(d) A is the set of integers and $\equiv$ is given by $m \equiv n$ if $m - n$ is divisible by 5.
(e) A is the set of positive integers and $\sim$ is given by $m \sim n$ if n is divisible by m.

(2) For a given set A and a relation $\preceq$ on it, determine whether $\preceq$ is a partial order. If it is, represent it by a Hasse diagram and determine whether it is a total order. Then, determine the greatest, the smallest elements, minimal and maximal elements, if any of those exist.
(a) $A = \{1, 2, 3\}$ and $\preceq$ consists of the ordered pairs $(1, 1), (2, 2), (3, 3), (1, 2), (2, 3)$.
(b) $A = \{1, 2, 3\}$ and $\preceq$ consists of the pairs $(1, 1), (2, 2), (3, 3), (1, 2), (2, 3), (3, 2), (1, 3)$.
(c) $A = \mathcal{P}(\{1, 2, 3\})$ and $\preceq$ consists of the pairs $(\{1\}, \{1\})$, $(\{2\}, \{2\})$, $(\{3\}, \{3\})$.
(d) $A = \{\{1\}, \{2\}, \{3\}\}$ and $\preceq$ consists of the pairs $(\{1\}, \{1\})$, $(\{2\}, \{2\})$, $(\{3\}, \{3\})$.
(e) $A = \{\{1\}, \{2\}, \{3\}\}$ and $\preceq$ consists of the pairs $(\{1\}, \{1\})$, $(\{2\}, \{2\})$, $(\{1\}, \{2\})$, $(\{3\}, \{3\})$.

(3) If R is a relation on a set A which is reflexive and transitive, show that the relation $\sim$ given by

$$a \sim b \quad \text{if} \quad aRb \text{ and } bRa$$

is an equivalence relation.

(4) Let A and B be any sets and let $\preceq$ be a partial order on A and $\precsim$ is a partial order on B. Let us define $\precapprox$ on $A \times B$ by

$$(a, b) \precapprox (c, d) \quad \text{if and only if} \quad a \preceq c \text{ and } b \precsim d.$$

Show that $\precapprox$ is a partial order on $A \times B$.

(5) For the given poset A of the set of real numbers $\mathbb{R}$, consider both A and $\mathbb{R}$ to be partially ordered by the relation $\leq$. Determine the greatest, the smallest elements, minimal and maximal elements, and suprema and infima of A, if any of those exist.
(a) $A = \{1\}$
(b) $A = [0, 1)$.
(c) A is the set of positive integers.
(d) $A = (0, 1) \cup (1, 2)$
(e) $A = \bigcup_{n=1}^{\infty} [0, n)$

(6) Show that if a binary relation R defined on a nonempty set A is both symmetric and antisymmetric, then it is the equality relation, that is

$$aRb \quad \Rightarrow \quad a = b$$

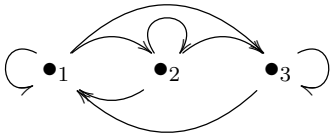
for every $a, b \in A$.

In addition, if R is also reflexive, then the converse $a = b \Rightarrow aRb$ also holds.

Solutions. (1) (a) The relation is reflexive ($1 \sim 1, 2 \sim 2$, and $3 \sim 3$ all hold) and symmetric ($1 \sim 2$ and $2 \sim 1$ both holds an $2 \sim 3$ and $3 \sim 2$ both hold) but not transitive: $1 \sim 2$ and $2 \sim 3$ hold, but not $1 \sim 3$.
The following oriented graph represents $\sim$ can also be used to reach the same conclusion since there are arrows from 1 to 2 and from 2 to 3 but not from 1 to 3.

(b) The relation is reflexive ($1 \sim 1, 2 \sim 2$, and $3 \sim 3$ all hold), but neither symmetric nor transitive. It is not symmetric since $2 \sim 3$ holds but not $3 \sim 2$. It is not transitive since $3 \sim 1$ and $1 \sim 2$ hold, but not $3 \sim 2$.

The following oriented graph represents $\sim$ can also be used to reach the same conclusion: for both symmetry and transitivity there should be an arrow from 3 to 2.



(c) The relation is reflexive since $a^2 = a^2$ holds. It is symmetric since $a^2 = b^2$ implies that $b^2 = a^2$ and transitive since $a^2 = b^2$ and $b^2 = c^2$ imply that $a^2 = c^2$.
Note that $a^2 = b^2$ if and only if $b = \pm a$. So, the equivalence class $[a]$ of any real number a consists of two elements a and $-a$ for $a \neq 0$ and $[0] = \{0\}$. Thus, the quotient set is the set of the sets $\{a, -a\}$ where $a \in \mathbb{R}$. As each negative number $-a$ is "identified" to its opposite a, the quotient set can be represented as the set of nonnegative real numbers.

(d) *Reflexivity.* Since $m - m = 0$ and 0 is divisible by 5, $m \equiv m$ holds.
Symmetry. If $n - m$ is divisible by 5, then $m - n = -(n - m)$ is also divisible by 5, so $m \equiv n$ implies that $n \equiv m$.
Transitivity. If $m \equiv n$ and $n \equiv k$, then both $m - n$ and $n - k$ are divisible by 5. Then, their sum $(m - n) + (n - k) = m - k$ is also divisible by 5. This shows that $m \equiv k$.
Quotient set: two integers are in relation, if they have the same remainder when dividing by 5. As the possible remainders are $0, 1, 2, 3$, and 4, there are five different equivalence classes $[0], [1], [2], [3]$, and $[4]$ (the class $[2]$, for example, consists of all integers of the form $5k + 2$ for $k \in \mathbb{Z}$). The quotient set consists of five elements $A/\equiv = \{[0], [1], [2], [3], [4]\}$.

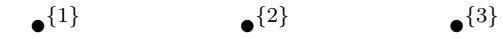
(e) This is not an equivalence relation since it is not symmetric (it is antisymmetric, in fact). Indeed, while 1 divides 2, 2 does not divide 1.

(2) (a) The relation $\preceq$ is reflexive and antisymmetric but not transitive as we have that $1 \preceq 2$ and $2 \preceq 3$ but 1 is not in the relation with 3.

(b) The relation $\preceq$ is reflexive and transitive but not antisymmetric as we have that $2 \preceq 3$ and $3 \preceq 2$ but $2 \neq 3$.

(c) The relation is not reflexive: $\{1, 2\}$ is an element of A but $(\{1, 2\}, \{1, 2\})$ is not an element of $\preceq$.

(d) The relation is reflexive since every element of A is in the relation with itself. The relation is antisymmetric: the premise of the implication ($a \preceq b$ and $b \preceq a \Rightarrow a = b$) is never true if $a \neq b$. The implication is also transitive since the premise of the implication ($a \preceq b$ and $b \preceq c \Rightarrow a \preceq c$) is never true if $a \neq b$ and $b \neq c$ and it trivially holds when $a = b$ or $b = c$. The Hasse diagram of $\preceq$ is below.



The partial order is not total since there are incomparable elements (actually any two different elements are incomparable with each other). There are no greatest or smallest elements and every element of A is both maximal and minimal element.

(e) The relation is reflexive since every element of A is in the relation with itself. The relation is antisymmetric: the premise of the implication ($a \preceq b$ and $b \preceq a \Rightarrow a = b$) is never true if $a \neq b$. The implication is also transitive since the premise of the implication ($a \preceq b$ and $b \preceq c \Rightarrow a \preceq c$) is never true if $a \neq b$ or $b \neq c$ and it trivially

holds when $a = b$ or $b = c$. The Hasse diagram of $\preceq$ is below.

The partial order is not total since $\{1\}$ and $\{3\}$ are incomparable (as are $\{2\}$ and $\{3\}$). There are no greatest or smallest elements, $\{1\}$ and $\{3\}$ are minimal and $\{2\}$ and $\{3\}$ are maximal elements.

(3) *Reflexivity.* We need to show that $a \sim a$ holds for any $a \in A$.

$$\begin{array}{rcll} a \sim a & \Leftrightarrow & aRa \ \wedge \ aRa & \text{(by the definition of } \sim) \\ & \Leftrightarrow & aRa & \text{(by idempotence of } \wedge) \\ & \Leftrightarrow & \top & \text{(by reflexivity of } R) \end{array}$$

Symmetry. Assume that $a \sim b$ holds and show that $b \sim a$ holds.

$$\begin{array}{rcll} a \sim b & \Leftrightarrow & aRb \ \wedge \ bRa & \text{(by the definition of } \sim) \\ & \Leftrightarrow & bRa \ \wedge \ aRb & \text{(by commutativity of } \wedge) \\ & \Leftrightarrow & b \sim a & \text{(by the definition of } \sim) \end{array}$$

Transitivity. Assume that $a \sim b$ and $b \sim c$ hold and show that $a \sim c$ holds,

$$\begin{array}{rcll} a \sim b \wedge b \sim c & \Leftrightarrow & (aRb \ \wedge \ bRa) \wedge (bRc \ \wedge \ cRb) & \text{(by the definition of } \sim) \\ & \Leftrightarrow & (aRb \ \wedge \ bRc) \wedge (cRb \ \wedge \ bRa) & \text{(by commutativity of } \wedge) \\ & \Leftrightarrow & aRc \ \wedge \ cRa & \text{(by transitivity of } R) \\ & \Leftrightarrow & a \sim c & \text{(by the definition of } \sim) \end{array}$$

(4) *Reflexivity.* We need to show that $(a, b) \precsim (a, b)$ holds for any $a \in A$ and any $b \in B$.

$$\begin{array}{rcll} (a,b) \precsim (a,b) & \Leftrightarrow & a \preceq a \ \wedge \ b \precsim b & \text{(by the definition of } \precsim) \\ & \Leftrightarrow & \top \ \wedge \ \top & \text{(since } \preceq \text{ and } \precsim \text{ are reflexive)} \\ & \Leftrightarrow & \top & \text{(by the definition of } \wedge) \end{array}$$

Antisymmetry. Assume that $(a, b) \precsim (c, d)$ and that $(c, d) \precsim (a, b)$ for some $a, c \in A$ and $b, d \in B$ and show that $(a, b) = (c, d)$.

$$\begin{array}{rcll} (a,b) \precsim (c,d) \wedge (c,d) \precsim (a,b) & \Leftrightarrow & (a \preceq c \ \wedge \ b \precsim d) \wedge (c \preceq a \ \wedge \ d \precsim b) & \text{(by the definition of } \precsim) \\ & \Leftrightarrow & (a \preceq c \ \wedge \ c \preceq a) \wedge (b \precsim d \ \wedge \ d \precsim b) & \text{(by commutativity of } \wedge) \\ & \Rightarrow & a = c \ \wedge \ b = d & \text{(since } \preceq \text{ and } \precsim \text{ are antisymmetric)} \\ & \Leftrightarrow & (a,b) = (c,d) & \text{(by the definition of an ordered pair)} \end{array}$$

Transitivity. Assume that $(a, b) \precsim (c, d)$ and $(c, d) \precsim (e, f)$ for some $a, c, e \in A$ and $b, d, f \in B$ and show that $(a, b) \precsim (e, f)$.

$$\begin{array}{rcll} (a,b) \precsim (c,d) \wedge (c,d) \precsim (e,f) & \Leftrightarrow & (a \preceq c \ \wedge \ b \precsim d) \wedge (c \preceq e \ \wedge \ d \precsim f) & \text{(by the definition of } \precsim) \\ & \Leftrightarrow & (a \preceq c \ \wedge \ c \preceq e) \wedge (b \precsim d \ \wedge \ d \precsim f) & \text{(by commutativity of } \wedge) \\ & \Rightarrow & a \preceq e \ \wedge \ b \precsim f & \text{(since } \preceq \text{ and } \precsim \text{ are transitive)} \\ & \Leftrightarrow & (a,b) \precsim (e,f) & \text{(by the definition of } \precsim) \end{array}$$

(5) (a) If $A = \{1\}$, greatest, the smallest elements, minimal and maximal elements (each unique), and suprema and infima of A are all equal and equal to 1.

(b) If $A = [0, 1)$ neither the greatest element nor a maximal element exist. The supremum exist and it is 1. 0 is the smallest, a minimal element (which is unique) and the infimum of A.

(c) A is the set of positive integers, i.e. the set $\{1, 2, 3, \ldots\}$. Then 1 is the smallest element, unique minimal element and the infimum of A. There is no greatest, no maximal element and no supremum.

(d) $A = (0, 1) \cup (1, 2)$. The fact that 1 is not an element of A does not make a big difference in this case and the elements in question for A are the same as for $(0, 2)$: there are no smallest nor greatest elements, no minimal and maximal elements and 0 is the infimum and 2 is the supremum of A.

(e) As any nonnegative real number is smaller than some positive integer n, A is the interval $[0, \infty)$. Thus, 0 is the smallest element, a unique minimal element and the infimum and there is no greatest element, no maximum and no supremum.

(6) The problem is asking us to show the implication $aRb \Rightarrow a = b$ for any $a, b \in A$. So, assume that a and b are elements of A such that aRb holds. As R is symmetric, we have that bRa holds. Thus, the premise of the implication $aRb \wedge bRa \Rightarrow a = b$ is true and the implication itself is true because R is antisymmetric. Hence, the conclusion $a = b$ is also true.

If R is reflexive, then aRa holds for any $a \in A$. So, if $a = b$ holds, then aRa is aRb and it holds. This shows the converse implication $a = b \Rightarrow aRb$.

5. Functions

Maps, domains, codomains. A function is a relation which satisfies some further properties. In particular, if A and B are sets, a binary relation f on $A \times B$ is a **function** or a **mapping** A **to** B, if the following two conditions hold:

(1) For every $a \in A$, there is $b \in B$ such that (a, b) is in f. Thus, every element of A should appear in the first coordinate of at least one of the ordered pairs.
(2) For every $a \in A$, $b \in B$ such that (a, b) is in f is unique. Thus, no element of A should appear twice in the first coordinate of any two ordered pairs.

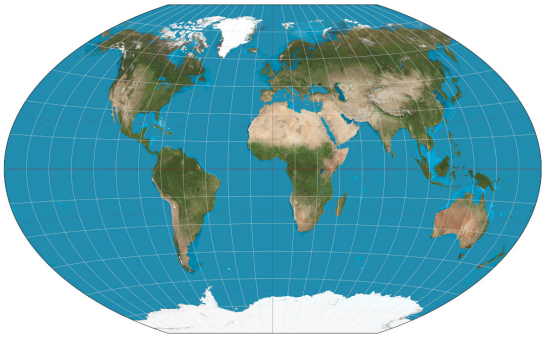
In this case, we say that f **maps** A to B and we write $f : A \to B$ and if $(a, b) \in f$ for some $a \in A$ and $b \in B$, we write

$$f(a) = b$$

and say that b is the **image** of a.

The two conditions above can be written as follows.

(1) For every $a \in A$, there is $b \in B$ such that $f(a) = b$.
(2) If $a_1 = a_2$, then $f(a_1) = f(a_2)$ for every $a_1, a_2 \in A$.

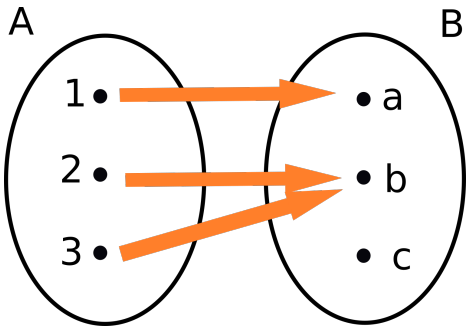


The set A is called **the domain** of f and the set B is **the codomain** of f. A function can be represented by arrows **mapping** the elements of A to elements of B. For example, if

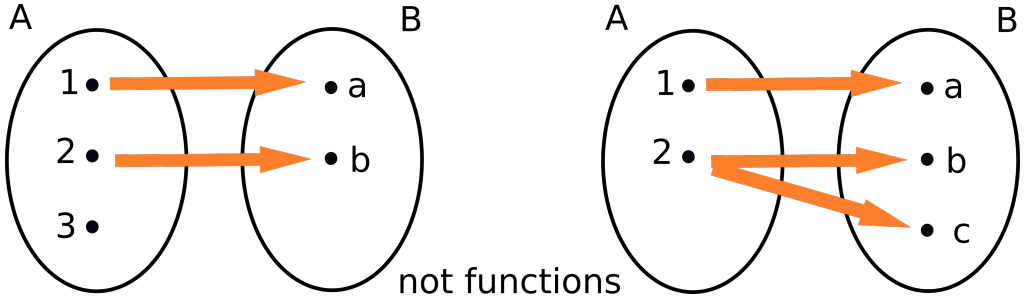
$A = \{1, 2, 3\}$ and $B = \{a, b, c\}$, the relation consisting of

$$(1, a), (2, b), \text{ and } (3, b)$$

is a function (every element of A indeed appears in the first coordinate and no element of A appears twice in the first coordinate of any of the ordered pairs). This function can be written as $f(1) = a$, $f(2) = b$, and $f(3) = b$ and represented by the diagram on the right.

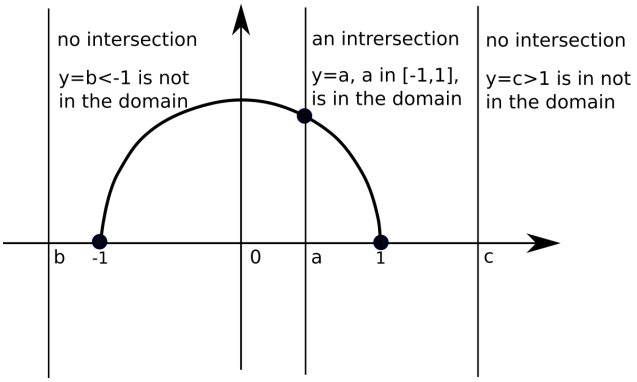


This type of representation can be used to check whether a given relation is a function. The relation on the first diagram below is not a function since the first condition fails (the element 3 of A is mapped to no element of B) and the relation on the second diagram below is not a function since the second condition fails (the element 2 is mapped to two different elements of B).



A relation on a subset A of the set of real numbers $\mathbb{R}$ is a function can be represented by a **graph** in the xy-plane. The two requirements for the relation to be a function can be checked by **the vertical line test**: any vertical line passing any element of A (represented on the x-axis) should intersect the graph at least and at most once (i.e. exactly once). For example, $y = x^2$ is a function with the domain $\mathbb{R}$.

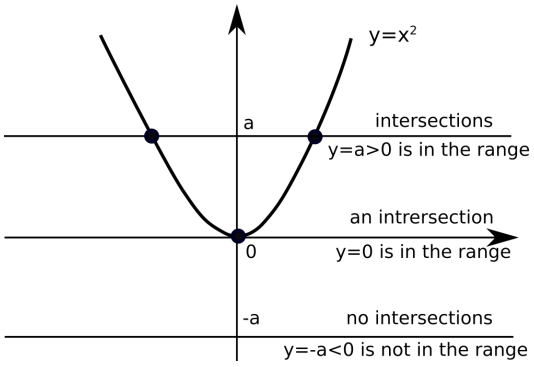
The upper arc of the unit circle $y = \sqrt{1 - x^2}$ is a function with the domain $[-1, 1]$, but it is not a function on entire $\mathbb{R}$ because a vertical line passing any number outside of the interval $[-1, 1]$ does not intersect the graph so the vertical line test fails. The entire unit circle $x^2 + y^2 = 1$ fails the vertical line test inside $[-1, 1]$ also, so this is not a function neither on $[-1, 1]$ nor on $\mathbb{R}$.



If f is a function mapping A to B, the set of all elements of B which are images of some element of A is called the **image** or the **range** of f and is denoted by $\mathrm{Im}f$ or, simply, $f(A)$. Thus,

$$f(A) = \{f(a) : a \in A\} = \{b \in B : b = f(a) \text{ for some } a \in A\}.$$

For example, the image of the very first function we considered (see the first figure of this section) is $\{a, b\}$. The image of $y = x^2$ considered on the domain $\mathbb{R}$ is the set of nonnegative real numbers, the interval $[0, \infty)$. Note that this can be determined by considering all y-values such that a *horizontal line at that point intersects the graph*. The figure on the right illustrates this for $y = x^2$ function.



In the special case when the domain A of some function $f : A \to B$ is of the form $A_1 \times A_2 \times \ldots A_n$, one can consider f to be a **function of n variables**. For example, the formula $z = x^2 + y^2$ defines a function f on two variables mapping an ordered pair (x, y) from $\mathbb{R} \times \mathbb{R}$ onto the element $x^2 + y^2$ of $\mathbb{R}$. So, $f : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$.

Injective, surjective and bijective functions. A function $f : A \to B$ is

(1) is **onto** or **surjective** if

$$\text{for every } b \in B, \text{ there is } a \in A \text{ such that } f(a) = b,$$

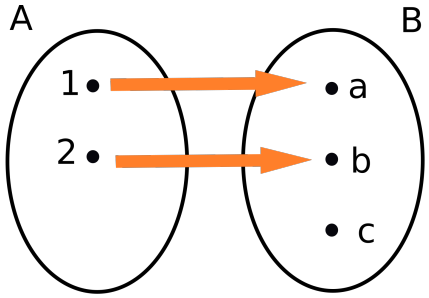
i.e. if the image $f(A)$ of A is the entire set B. Thus, for an onto function, every element of the codomain is the image of some element of the domain, i.e. $f(A) = B$. Represented graphically, every element of B is hit by an arrow originating in A.

(2) A function $f : A \to B$ is **one-to-one** or **injective** if

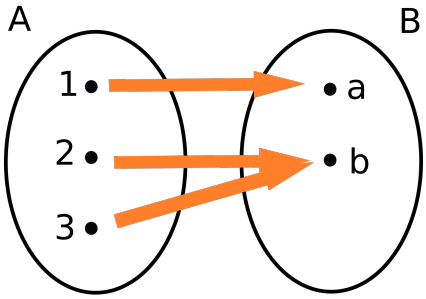
$$f(a_1) = f(a_2) \text{ implies that } a_1 = a_2$$

for any $a_1, a_2 \in A$. Thus, a function is one-to-one if the *converse* of the second condition in the definition of the function holds. Represented graphically, no element of B receives two arrows.

For example, the first function we considered in this section (see the first figure with sets A and B in this section) is not onto since $c \in B$ is not in the image of f – it does not receive an arrow from A. This function is not one-to-one since $b \in B$ is in the image of two different elements – it receives two arrows from A.



one-to-one and not onto



onto and not one-to-one

In some cases, it is easier to check the *contrapositive*

$$a_1 \neq a_2 \quad \Rightarrow \quad f(a_1) \neq f(a_2)$$

of the implication $f(a_1) = f(a_2) \quad \Rightarrow \quad a_1 = a_2$ to check that a function is one-to-one. Note that f is *not* one-to-one if there are $a_1, a_2 \in A$ such that

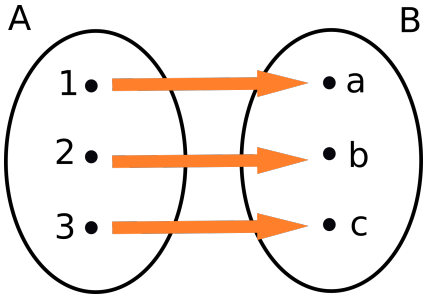
$$a_1 \neq a_2 \quad \text{and} \quad f(a_1) = f(a_2).$$

If a function f on a subset A of $\mathbb{R}$ is represented graphically, it is one-to-one if it passes horizontal line test on its image: a horizontal line at any element of $f(A)$ (positioned on the y-axis) does not intersects the graph more than once. If $f(A) = \mathbb{R}$, the function is onto $\mathbb{R}$ and a horizontal line at any point of the y-axis intersects the graph.

For example, the image of $y = x^2$ is the interval $[0, \infty)$ and this function is not injective: 2 and -2, for example, have the same image 4. The function $y = x^3$ is both one-to-one and onto: the horizontal line at any point on the y-axis intersects the graph (so it is onto) and it intersects it exactly once (so it is one-to-one).

If a function $f : A \to B$ is both one-to-one and onto, we say that it is a **bijection** and that A and B are in a bijective correspondence.

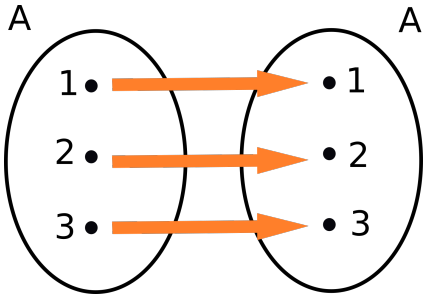
For example, the function given by the diagram on the right is a bijection. The function $y = x^3$ is a bijection mapping $\mathbb{R}$ onto $\mathbb{R}$. If $y = x^2$ is considered only on the interval $[0, \infty)$ it maps this interval bijectively onto itself, so it is a bijection $[0, \infty) \to [0, \infty)$.



An important example of a bijection is the **identity function** on a set A. This function, usually denoted by id_A or 1_A, maps every element $a \in A$ identically onto itself, so it is given by

$$\mathrm{id}_A(a) = a$$

for every $a \in A$. For example, the function $y = x$ is the identity function on the set of real numbers.



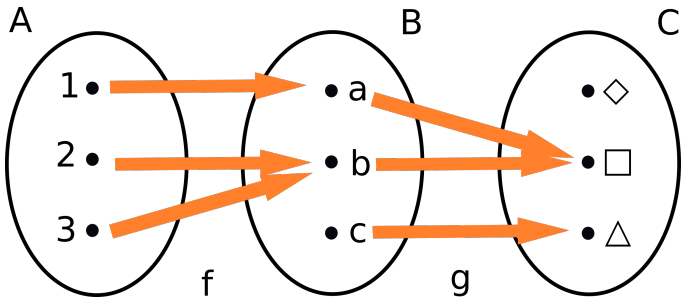
Composition of functions. If A, B, and C are some sets and $f : A \to B$ and $g : B \to C$ are functions, a **composition** $g \circ f$ is the function mapping A to C given by

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

for $a \in A$.

For example, if $A = \{1, 2, 3\}, B = \{a, b, c\}$, and $C = \{\Diamond, \Box, \triangle\}$, and $f : A \to B$ and $g : B \to C$ are defined as on the figure below, then

$$(g \circ f)(1) = g(f(1)) = g(a) = \Box, \quad (g \circ f)(2) = g(f(2)) = g(b) = \Box, \text{ and}$$
$$(g \circ f)(3) = g(f(3)) = g(b) = \Box.$$



If f and g are real-valued functions of $\mathbb{R}$ given by some formulas, a formula for the composite $g \circ f$ is obtained by replacing every x in $g(x)$ by the formula for $f(x)$. In this case, we think of f as the *inner* and g as the *outer* function. You may remember the composite of the functions requiring the *Chain Rule* when differentiating a composite in Calculus 1.

For example, if $f(x) = 3x + 5$ and $g(x) = x^2 + 2x$, then

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

Before the next exercise showing some properties of a composite, note that to show that two functions f_1 and $f_2 : A \to B$ are equal, one needs to show that they map an arbitrary element of A to the same element of B, i.e. that

$$f_1(a) = f_2(a) \text{ for every } a \in A.$$

Exercise 23. If $f : A \to B$, $g : B \to C$, and $h : C \to D$ are functions, show the following properties.

(1) Associativity holds for the composite.
$$(h \circ g) \circ f = h \circ (g \circ f)$$
(2) The identity function is a neutral element for the composite.
$$f \circ \mathrm{id}_A = f \quad \text{and} \quad \mathrm{id}_B \circ f = f$$
(3) If f and g are injections, then $g \circ f$ is an injection.
(4) If f and g are surjections, then $g \circ f$ is a surjection.
(5) If f and g are bijections, then $g \circ f$ is a bijection.
(6) If $g \circ f$ is an injection, then f is an injection.
(7) If $g \circ f$ is a surjection, then g is a surjection.

If $A = B = C$, exhibit some set A and functions f and g on A such that

$$f \circ g \neq g \circ f.$$

Solution. (1) Let $a \in A$ be arbitrary. We have that

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

and that

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

This shows that $((h \circ g) \circ f)(a) = (h \circ (g \circ f))(a)$ for any $a \in A$ and so $(h \circ g) \circ f = h \circ (g \circ f)$.

(2) Let $a \in A$ be arbitrary. We have that $(f \circ \mathrm{id}_A)(a) = f(\mathrm{id}_A(a)) = f(a)$. Thus $f \circ \mathrm{id}_A = f$.
To show the second identity, note that $\mathrm{id}_B(f(a)) = f(a)$ by the definition of id_B. Thus, for any $a \in A$, $(\mathrm{id}_B \circ f)(a) = \mathrm{id}_B(f(a)) = f(a)$, which shows that $\mathrm{id}_B \circ f = f$.

(3) Assume that f and g are injections. To show that $g \circ f$ is injective, assume that $g \circ f(a_1) = g \circ f(a_2)$ for $a_1, a_2 \in A$, and show that $a_1 = a_2$.

$$\begin{array}{lcll} g \circ f(a_1) = g \circ f(a_2) & \Leftrightarrow & g(f(a_1)) = g(f(a_2)) & \text{(by the definition of } \circ) \\ & \Rightarrow & f(a_1) = f(a_2) & \text{(since } g \text{ is injective)} \\ & \Rightarrow & a_1 = a_2 & \text{(since } f \text{ is injective)} \end{array}$$

(4) Assume that f and g are surjections. We need to show that $g \circ f$ is a surjection, i.e. that for every $c \in C$, there is $a \in A$ such that $(g \circ f)(a) = c$.
Let $c \in C$ be arbitrary. As g is a surjection, there is $b \in B$ such that $g(b) = c$. Since f is also surjective, for b there is $a \in A$ such that $f(a) = b$. Hence,

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

(5) If f and g are bijections, then they are both injective and surjective. The composite $g \circ f$ is injective by part (3) and surjective by part (4), so it is a bijection.

(6) Assume that $g \circ f$ is an injection. To show that f is an injection, we need to show the implication $f(a_1) = f(a_2) \Rightarrow a_1 = a_2$ for arbitrary $a_1, a_2 \in A$.

$$\begin{array}{lcll} f(a_1) = f(a_2) & \Rightarrow & g(f(a_1)) = g(f(a_2)) & \text{(since } g \text{ is a function)} \\ & \Leftrightarrow & g \circ f(a_1) = g \circ f(a_2) & \text{(by the definition of } \circ) \\ & \Rightarrow & a_1 = a_2 & \text{(since } g \circ f \text{ is injective)} \end{array}$$

(7) Assume that $g \circ f$ is surjective. To show that g is surjective, we need to show that $(\forall c \in C)(\exists b \in B) g(b) = c$. So, let $c \in C$. As $g \circ f$ is surjective, there is $a \in A$ such that $(g \circ f)(a) = c$. Thus, $g(f(a)) = c$. By taking b to be $f(a)$, we have that $g(b) = c$.

To show that the composite is not commutative, almost any set with nonidentity functions different from one another will do. For example if $A = \mathbb{R}$, $f(x) = 3x + 5$ and $g(x) = x^2 + 2x$, then

$$(g \circ f)(x) = g(f(x)) = g(3x+5) = (3x+5)^2 + 2(3x+5) = 9x^2 + 30x + 25 + 6x + 10 = 9x^2 + 36x + 35,$$

$$(f \circ g)(x) = f(g(x)) = g(x^2 + 2x) = 3(x^2 + 2x) + 5 = 3x^2 + 6x + 5.$$

For $x = 0$, for example, $(g \circ f)(0) = 35 \neq 5 = (f \circ g)(0)$ and so $g \circ f \neq f \circ g$.

Inverse function. A function $f : A \to B$ has an **inverse function** $g : B \to A$ if

$$g \circ f = \mathrm{id}_A \quad \text{and} \quad f \circ g = \mathrm{id}_B .$$

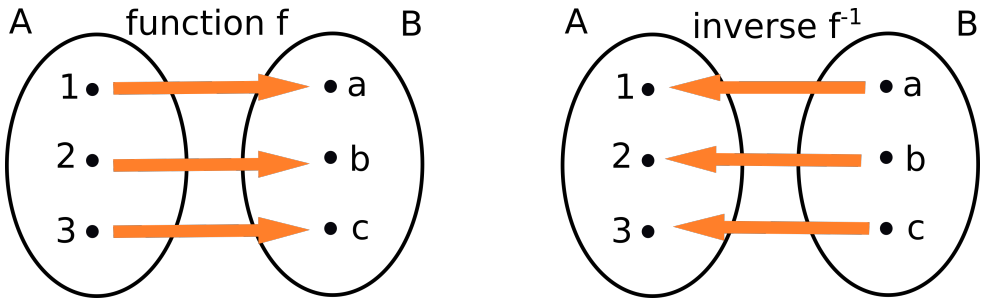
If an inverse function exists, it is **unique**. To show this, assume that both $g : B \to A$ and $h : B \to A$ are inverses of $f : A \to B$ and let us show that $g = h$. This holds since

$$\begin{array}{rcll} g & = & \mathrm{id}_A \circ g & \text{by property (2) of Exercise 23} \\ & = & (h \circ f) \circ g & \text{since } h \text{ is an inverse to } f \\ & = & h \circ (f \circ g) & \text{by property (1) of Exercise 23} \\ & = & h \circ \mathrm{id}_B & \text{since } g \text{ is an inverse to } f \\ & = & h & \text{by property (2) of Exercise 23.} \end{array}$$

As an inverse function is unique, we can use a fixed notation for such function and we use f^{-1}. Hence, if $f : A \to B$ has an inverse, it is $f^{-1} : B \to A$ and

$$f^{-1} \circ f = \mathrm{id}_A \quad \text{and} \quad f \circ f^{-1} = \mathrm{id}_B .$$

In this case, we say that f is **an invertible function.**



Exercise 24. Show that $f : A \to B$ is invertible if and only if f is a bijection.

Solution. Let us show the direction ($\Rightarrow$). So, let us assume that f is invertible. Thus, f^{-1} exists. As the identity functions id_A and id_B are bijections, we have that $f^{-1} \circ f = \mathrm{id}_A$ is injective and that $f \circ f^{-1} = \mathrm{id}_B$ is surjective. The injectivity of $f^{-1} \circ f$ then implies that f is injective by part (6) of Exercise 23. The surjectivity of $f \circ f^{-1}$ then implies that f is surjective by part (7) of Exercise 23. Hence, f is both one-to-one and onto so it is a bijection.

To show the direction ($\Leftarrow$), let us assume that f is bijective. As f is onto, $(\forall b \in B)(\exists a \in A) f(a) = b$ and as f is one-to-one, $f(a_1) = f(a_2) \Rightarrow a_1 = a_2$ for any $a_1, a_2 \in A$ Thus, if we define a function $g : B \to A$ by $g(b) = a$ if $f(a) = b$, we have that two requirements for g to be a function hold so our definition of g is valid and it indeed defines a function (one says that the function g is *well-defined* in this case. Indeed, $(\forall b \in B)(\exists a \in A) f(a) = b$ becomes equivalent to $(\forall b \in B)(\exists a \in A) g(b) = a$ showing that the first requirement for g to be a function holds. The second requirement holds since if $b_1 = b_2$ for $b_1, b_2 \in B$ and if $b_1 = f(a_1)$ and $b_2 = f(a_2)$ for $a_1, a_2 \in A$ which exists since f is onto, then $f(a_1) = b_1 = b_2 = f(a_2)$ holds and this implies that $a_1 = a_2$ since f is one-to-one. Thus, we have that $g(b_1) = a_1 = a_2 = g(b_2)$.

To show that $g = f^{-1}$, it is sufficient to show that $g \circ f = \mathrm{id}_A$ and $f \circ g = \mathrm{id}_B$. The first relation holds since for any $a \in A$ and $b \in B$ such that $f(a) = b$ (thus $g(b) = a$) we have that

$$(g \circ f)(a) = g(f(a)) = g(b) = a = \mathrm{id}_A(a).$$

The second relation holds by a similar argument

$$(f \circ g)(b) = f(g(b)) = f(a) = b = \mathrm{id}_B(b).$$

Inverse images of a function. If $f : A \to B$ is any function, possibly not bijective, and $C \subseteq A$ and $D \subseteq B$, we define the **image of** C as

$$f(C) = \{b \in B : b = f(c) \text{ for some } c \in C\}$$

and the **inverse image of** D as

$$f^{-1}(D) = \{a \in A : f(a) \in D\}.$$

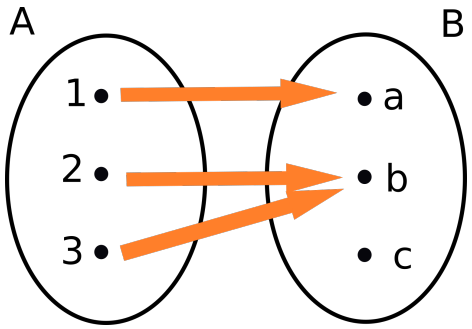
Note that $f(C) \subseteq B$ and that $f^{-1}(D) \subseteq A$ by the above definitions. Also note that the inverse image of a subset of B should not be confused with the inverse function and it should be clear from context in which sense the notation f^{-1} is used.

For example, if $A = \{1, 2, 3\}, B = \{a, b, c\}$ and f is given as on the figure on the right, then

$$f(\{1, 2\}) = \{a, b\} \text{ and } f(\{2, 3\}) = \{b\}$$

for example. And

$$f^{-1}(\{a, b\}) = \{1, 2, 3\} \text{ and } f^{-1}(\{b, c\}) = \{2, 3\}.$$



Exercise 25. Show the following properties of a function $f : A \to B$, $C \subseteq A$, and $D \subseteq B$.

(1) $C \subseteq f^{-1}(f(C))$
(2) $f(f^{-1}(D)) \subseteq D$
(3) If f is one-to-one, then $C = f^{-1}(f(C))$.
(4) If f is onto, then $f(f^{-1}(D)) = D$.
(5) If D_1, D_2 are subsets of B then

$$f^{-1}(D_1 \cap D_2) = f^{-1}(D_1) \cap f^{-1}(D_2).$$

(6) If C_1, C_2 are subsets of A, show that

$$f(C_1 \cap C_2) \subseteq f(C_1) \cap f(C_2).$$

Show that the converse holds if f is injective and exhibit and example showing that the converse does not show in general.

Solution. (1) Assume that $c \in C$. Then $f(c) \in f(C)$ by the definition of $f(C)$ so $c \in f^{-1}(f(C))$ by the definition of the inverse image of $f(C)$.

(2) Assume that $d \in f(f^{-1}(D))$ and show that $d \in D$. As $d \in f(f^{-1}(D))$, there is $a \in f^{-1}(D)$ such that $d = f(a)$. Since $a \in f^{-1}(D)$, we have that $f(a)$ is in D. Hence $d = f(a) \in D$.

(3) As $C \subseteq f^{-1}(f(C))$ holds by part (1), it is sufficient to show the inclusion $f^{-1}(f(C)) \subseteq C$.
Assume that $c \in f^{-1}(f(C))$ and let us show that $c \in C$. As $c \in f^{-1}(f(C))$, we have that $f(c) \in f(C)$. Hence, there is $c_1 \in C$ such that $f(c) = f(c_1)$. Since f is one-to-one, this implies that $c = c_1$ and as $c_1 \in C$, we have that c is in C.

(4) As $f(f^{-1}(D)) \subseteq D$ holds by part (2), it is sufficient to show that $D \subseteq f(f^{-1}(D))$.
Let $d \in D$. As $D \subseteq B$, $d \in B$. Since f is onto, there is $c \in A$ such that $f(c) = d \in D$ so that $c \in f^{-1}(D)$. This implies that $d = f(c) \in f(f^{-1}(D))$.

(5) Let $a \in A$.

$$\begin{aligned} a \in f^{-1}(D_1 \cap D_2) &\Leftrightarrow f(a) \in D_1 \cap D_2 && \text{(by the definition of the inverse image)} \\ &\Leftrightarrow f(a) \in D_1 \ \wedge \ f(a) \in D_2 && \text{(by the definition of the intersection)} \\ &\Leftrightarrow a \in f^{-1}(D_1) \wedge a \in f^{-1}(D_2) && \text{(by the definition of the inverse image)} \\ &\Leftrightarrow a \in f^{-1}(D_1) \cap f^{-1}(D_2) && \text{(by the definition of the intersection)} \end{aligned}$$

(6)

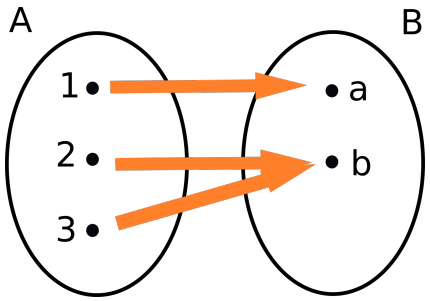
(7) Let $b \in B$.

$$\begin{aligned} b \in f(C_1 \cap C_2) &\Leftrightarrow (\exists a \in A)(b = f(a) \wedge a \in C_1 \cap C_2) \ \text{(by the definition of the image)} \\ &\Leftrightarrow (\exists a \in A)(b = f(a) \wedge a \in C_1 \wedge a \in C_2) \ \text{(by the definition of } \cap) \\ &\Leftrightarrow (\exists a \in A)(b = f(a) \wedge a \in C_1 \wedge b = f(a) \wedge a \in C_2) \ \text{(by idempotence of } \wedge) \\ &\Rightarrow (\exists a \in A)(b = f(a) \wedge a \in C_1) \wedge (\exists a \in A)(b = f(a) \wedge a \in C_2) \\ &\quad \text{(by passing } \exists \text{ through } \wedge) \\ &\Leftrightarrow b \in f(C_1) \wedge b \in f(C_2) \ \text{(by the definition of the inverse image)} \\ &\Leftrightarrow b \in f(C_1) \cap f(C_2) \ \text{(by the definition of } \cap). \end{aligned}$$

Let us assume now that f is injective and let us show the converse. So, let us assume that $b \in f(C_1) \cap f(C_2)$ so that $b = f(a_1)$ for some $a_1 \in C_1$ and $b = f(a_2)$ for some $a_2 \in C_2$. Thus, we have that $f(a_1) = b = f(a_2)$ and from these relations we can deduce that $a_1 = a_2$ because f is injective. So, as $a_1 \in C_1$, $a_2 \in C_2$, and $a_1 = a_2$, we have that $a_1 \in C_1 \cap C_2$. Since $b = f(a_1)$, we obtain that $b \in f(C_1 \cap C_2)$.

When exhibiting of a non-injective function f and the sets C_1 and C_2 for which the converse of the given inclusion fails, start by taking a simple non-injective function and play with various options for C_1 and C_2 to check if some of them would work.

For example, let A, B and f be as on the figure on the right. As the function values of 2 and 3 make f not one-to-one, try taking $C_1 = \{2\}$ and $C_2 = \{3\}$. Then $C_1 \cap C_2 = \emptyset$ so $f(C_1 \cap C_2) = \emptyset$. On the other hand, $f(C_1) = \{f(2)\} = \{b\}$ and $f(C_2) = \{f(3)\} = \{b\}$, so $f(C_1) \cap f(C_2) = \{b\} \cap \{b\} = \{b\}$. As $\{b\}$ is not a subset of $\emptyset$, this shows that $f(C_1) \cap f(C_2)$ is not necessarily a subset of $f(C_1 \cap C_2)$.



The inverse images of sets in the codomain of a function are important when defining the concept of a continuous function. For example, for a real-valued function f on $\mathbb{R}$ equipped with concepts of open subsets (see Practice problems 2 problem (9)), one say that f is continuous if *the inverse image of every open set is open.* When open sets are introduced using the absolute value function, this definition specializes to the epsilon-delta definition of continuity considered at the end of section 2.

Practice Problems 5. (1) Exhibit an example of a function $f : \mathbb{R} \to \mathbb{R}$ which is one-to-one but not onto.

(2) Show that the following properties of functions hold.

(a) If $f : A \to B$ and $g : B \to C$ are invertible, then

$$(g \circ f)^{-1} = f^{-1} \circ g^{-1}.$$

(b) If $f : A \to B$ is invertible, show that f^{-1} is invertible first and then show that

$$(f^{-1})^{-1} = f.$$

(3) If a function $f : A \to B$ is one-to-one, then for any nonempty set C and any two functions $g, h : C \to A$

$$f \circ g = f \circ h \Rightarrow g = h.$$

(4) Let $f : A \to B$ be a function mapping a set A to set B. Show the following statements.
(a) If D_1, D_2 are subsets of B then

$$f^{-1}(D_1 \cup D_2) = f^{-1}(D_1) \cup f^{-1}(D_2).$$

(b) If C_1, C_2 are subsets of A, then

$$f(C_1 \cup C_2) = f(C_1) \cup f(C_2).$$

(5) If f is onto, show that

$$g_1 \circ f = g_2 \circ f \text{ implies that } g_1 = g_2$$

for every $C \neq \emptyset$ and every functions $g_1, g_2 : B \to C$.

(6) Let $f : A \to B$ be a function mapping a set A to set B. Show the converse of part (3) Exercise 25: if $C = f^{-1}(f(C))$ holds for every subset C of A, then f is one-to-one.

(7) If U is any set and $A \subseteq U$, the **characteristic function** $\chi_A : A \to \{0, 1\}$ of A is defined by

$$\chi_A(x) = \begin{cases} 1 & x \in A \\ 0 & x \notin A \end{cases}$$

Show that the following identities hold for any $A, B \subseteq U$.
(a) $\chi_{A \cup B} = \chi_A + \chi_B - \chi_A \cdot \chi_B$
(b) $\chi_{A \cap B} = \chi_A \cdot \chi_B$
(c) $\chi_{\overline{A}} = 1 - \chi_A$

Solutions. (1) Try to think of a graph which has no horizontal line intersecting it more than once but with some horizontal lines not intersecting it at all. For example, e^x has such a graph: a horizontal line passing a positive y-value on the y-axis intersects the graph of e^x exactly once and a horizontal line passing a negative y-value on the y-axis does not intersect the graph of e^x. This shows that e^x is one-to-one (no horizontal line intersects it twice), but not onto (some horizontal lines do not intersect it at all. A graph of $\tan^{-1}(x)$ has the same property.

(2) (a) As an inverse function of $g \circ f$ is unique, the required equality holds if we show that $f^{-1} \circ g^{-1}$ is also an inverse of $g \circ f$. This amounts to showing that $f^{-1} \circ g^{-1}$ composed with $g \circ f$ on the left produces id_C and composed with $g \circ f$ on the right produces id_A. These identities hold as

$$\begin{aligned}
(g \circ f) \circ (f^{-1} \circ g^{-1}) &= g \circ ((f \circ f^{-1}) \circ g^{-1}) && \text{(by the associativity of } \circ) \\
&= g \circ (\mathrm{id}_B \circ g^{-1}) && \text{(since } f^{-1} \text{ is the inverse of } f) \\
&= g \circ g^{-1} && \text{(since } \mathrm{id}_B \circ g^{-1} = g^{-1}) \\
&= \mathrm{id}_C && \text{(since } g^{-1} \text{ is the inverse of } g)
\end{aligned}$$

and

$$\begin{array}{rcll}(f^{-1}\circ g^{-1})\circ(g\circ f) & = & f^{-1}\circ((g^{-1}\circ g)\circ f) & \text{(by the associativity of } \circ) \\ & = & f^{-1}\circ(\mathrm{id}_B\circ f) & \text{(since } g^{-1} \text{ is the inverse of } g) \\ & = & f^{-1}\circ f & \text{(since } \mathrm{id}_B\circ f = f) \\ & = & \mathrm{id}_A & \text{(since } f^{-1} \text{ is the inverse of } f)\end{array}$$

(b) If $f : A \to B$ is invertible, then there is a function f^{-1} such that $f^{-1}\circ f = \mathrm{id}_A$ and $f\circ f^{-1} = \mathrm{id}_B$. As id_A is onto, $f^{-1}\circ f$ is onto so f^{-1} is onto by part (7) of Exercise 23. As id_B is injective, $f\circ f^{-1}$ is injective, so f^{-1} is injective by part (6) of Exercise 23. This shows that f^{-1} is both injective and surjective so it is a bijection by Exercise 24. This shows the first part of the problem.
To show the second part, note that the first part implies that there is the inverse $(f^{-1})^{-1}$ of f^{-1}. So, the relations $(f^{-1})^{-1}\circ f^{-1} = \mathrm{id}_B$ and $f^{-1}\circ(f^{-1})^{-1} = \mathrm{id}_A$ hold. Hence

$$(f^{-1})^{-1} = (f^{-1})^{-1}\circ\mathrm{id}_A = (f^{-1})^{-1}\circ\left(f^{-1}\circ f\right) = \left((f^{-1})^{-1}\circ f^{-1}\right)\circ f = \mathrm{id}_B\circ f = f.$$

(3) Assume that $f : A \to B$ is one-to-one that $C \neq \emptyset$ and that $f\circ g = f\circ h$ for some $g, h : C \to A$. To show that $g = h$, let $c \in C$ and let us show that $g(c) = h(c)$. As $f\circ g = f\circ h$, we have that $f(g(c)) = f(h(c))$. Since f is injective, this implies that $g(c) = h(c)$.

(4) (a) Let $D_1, D_2 \subseteq B$ and let $a \in A$.

$$\begin{array}{rcll}a \in f^{-1}(D_1\cup D_2) & \Leftrightarrow & f(a)\in D_1\cup D_2 & \text{(by the definition of the inverse image)} \\ & \Leftrightarrow & f(a)\in D_1 \text{ or } f(a)\in D_2 & \text{(by the definition of the union)} \\ & \Leftrightarrow & a\in f^{-1}(D_1) \text{ or } a\in f^{-1}(D_2) & \text{(by the definition of the inverse image)} \\ & \Leftrightarrow & a\in f^{-1}(D_1)\cup f^{-1}(D_2) & \text{(by the definition of the union).}\end{array}$$

(b) Let $b \in B$.

$$\begin{array}{rcl}b\in f(C_1\cup C_2) & \Leftrightarrow & (\exists a\in A)(b=f(a)\wedge a\in C_1\cup C_2) \quad \text{(by the definition of the image)} \\ & \Leftrightarrow & (\exists a\in A)(b=f(a)\wedge(a\in C_1\vee a\in C_2)) \quad \text{(by the definition of } \cup) \\ & \Leftrightarrow & (\exists a\in A)((b=f(a)\wedge a\in C_1)\vee(b=f(a)\wedge a\in C_2)) \quad \text{(by distributivity)} \\ & \Leftrightarrow & (\exists a\in A)(b=f(a)\wedge a\in C_1)\vee(\exists a\in A)(b=f(a)\wedge a\in C_2) \\ & & \text{(by passing } \exists \text{ through } \vee) \\ & \Leftrightarrow & b\in f(C_1)\vee b\in f(C_2) \quad \text{(by the definition of the inverse image)} \\ & \Leftrightarrow & b\in f(C_1)\cup f(C_2) \quad \text{(by the definition of } \cup).\end{array}$$

(5) Assume that f is onto and that $g_1\circ f = g_2\circ f$ for some $C \neq \emptyset$ and $g_1, g_2 : B \to C$. We need to show that $g_1 = g_2$ which means that we have to show that $g_1(b) = g_2(b)$ for every $b \in B$. Let $b \in B$. Since f is onto, there is $a \in A$ such that $b = f(a)$.

Since $g_1\circ f = g_2\circ f$, we have that $g_1\circ f(a) = g_2\circ f(a)$ and so $g_1(b) = g_1(f(a)) = g_1\circ f(a) = g_2\circ f(a) = g_2(f(a)) = g_2(b)$.

(6) Let $f : A \to B$ and assume that $C = f^{-1}(f(C))$ for every $C \subseteq A$. We need to show that f is one-to-one so let us show that $f(a_1) = f(a_2)$ implies that $a_1 = a_2$ for any $a_1, a_2 \in A$.

By the assumption $\{a_1\} = f^{-1}(f(\{a_1\}))$ which means that a_1 is the only element of

$$f^{-1}(f(\{a_1\})) = \{a\in A : f(a)\in f(\{a_1\})\} = \{a\in A : f(a) = f(a_1)\}$$

and an analogous statement holds for a_2. Thus,

$$f(a_1) = f(a_2) \Rightarrow f(\{a_1\}) = f(\{a_2\}) \Rightarrow f^{-1}f(\{a_1\}) = f^{-1}(f(\{a_2\})) \Rightarrow \{a_1\} = \{a_2\} \Rightarrow a_1 = a_2.$$

(7) (a) For any $x \in U$, we show that $\chi_{A\cup B}(x) = \chi_A(x)+\chi_B(x)-\chi_A(x)\cdot\chi_B(x)$ by discussing the four cases below.
  (i) $x \in A$ and $x \in B$. In this case, the left side $\chi_{A\cup B}(x)$ is 1 and the right side $\chi_A(x) + \chi_B(x) - \chi_A(x) \cdot \chi_B(x)$ is $1 + 1 - 1 = 1$.
  (ii) $x \in A$ and $x \notin B$. In this case, the left side $\chi_{A\cup B}(x)$ is 1 and the right side $\chi_A(x) + \chi_B(x) - \chi_A(x) \cdot \chi_B(x)$ is $1 + 0 - 0 = 1$.
  (iii) $x \notin A$ and $x \in B$. In this case, the left side $\chi_{A\cup B}(x)$ is 1 and the right side $\chi_A(x) + \chi_B(x) - \chi_A(x) \cdot \chi_B(x)$ is $0 + 1 - 0 = 1$.
  (iv) $x \notin A$ and $x \notin B$. In this case, the left side $\chi_{A\cup B}(x)$ is 0 and the right side $\chi_A(x) + \chi_B(x) - \chi_A(x) \cdot \chi_B(x)$ is $0 + 0 - 0 = 0$.

  (b) For any $x \in U$, we show that $\chi_{A\cap B}(x) = \chi_A(x) \cdot \chi_B(x)$ by discussing the two cases below.
  (i) $x \in A \cap B$. In this case, the left side $\chi_{A\cap B}(x)$ is 1 and the right side $\chi_A(x) \cdot \chi_B(x)$ is $1 \cdot 1 = 1$.
  (ii) $x \notin A \cap B$. In this case, the left side $\chi_{A\cap B}(x)$ is 0 and the right side $\chi_A(x) \cdot \chi_B(x)$ is either $1 \cdot 0, 0 \cdot 1$ or $0 \cdot 0$ so it is 0 in either case.

  (c) For any $x \in U$, we show that $\chi_{\bar{A}}(x) = 1 - \chi_A(x)$ by discussing the two cases below.
  (i) $x \in A$. In this case, the left side $\chi_{\bar{A}}(x)$ is 0 because $x \notin \bar{A}$ and the right side $1 - \chi_A(x)$ is $1 - 1 = 0$.
  (ii) $x \notin A$. In this case, the left side $\chi_{\bar{A}}(x)$ is 1 because $x \in \bar{A}$ and the right side $1 - \chi_A(x)$ is $1 - 0 = 1$.

6. Counting and cardinality

Cardinality. In this section, we make the concept of the **number of elements** of a set more formal. After such formal treatment, we will be able to answer the questions from the end of section 3.

(1) Do any two sets with infinitely many elements have the same number of elements?
(2) If not, how do we measure different infinities?
(3) What do we even mean by "the number" of elements if this number is not finite?
(4) If sets are to be the first step in building mathematics formally, what do we even mean by "a number"?

The concept of a bijection is crucial for answering these questions.

Two sets A and B are **equipotent (or equinumerous)** if there is a bijection $A \to B$. We write $A \approx B$ in this case. If $A \approx B$, we say that they have the same **cardinality**. For example, the sets $A = \{1, 2, 3\}$ and $B = \{a, b, c\}$ are equipotent because f given by $1 \mapsto a, 2 \mapsto b, 3 \mapsto c$ is a bijection. We are aiming to assign the cardinal number 3 to the cardinality of A and B.

Exercise 26. Show that the relation $\approx$ is reflexive, symmetric and transitive.

Solution. Since id_A is a bijection $A \to A$, we have that $A \approx A$, so $\approx$ is reflexive.

If $A \approx B$, then there is a bijection $f : A \to B$. As f is a bijection, there is the inverse $f^{-1} : B \to A$ which is also a bijection (by Exercise 24). This shows that $B \approx A$ and so $\approx$ is symmetric.

If $A \approx B$ and $B \approx C$, then there are bijections $f : A \to B$ and $g : B \to C$. By part (5) of Exercise 23, $g \circ f : A \to C$ is a bijection, so $A \approx C$. Thus, $\approx$ is transitive.

The exercise above shows that $\approx$ can be considered as an equivalence relation on the class of all sets (note: this class is not a set). So, we can talk about the equivalence class of a set A, the class consisting of all sets which are equipotent to A.

Cardinal numbers (or **cardinals** for short) are these equivalence classes. This formal way of introducing cardinals captures the intuitive approach of introducing the cardinality of A as the *number of its elements* (and the number of elements of every other set equipotent to A). While the informal approach leaves questions from the beginning of this section without an answer, we can answer them all using this formal approach. We use $|A|$ for the cardinal number corresponding to the set A. Using this notation, the relation $\approx$ can also be written as

$$A \approx B \quad \Leftrightarrow \quad |A| = |B|.$$

We would like to select convenient **representatives** of each of the equivalence classes and introduce a notation for the "first few" cardinals which agrees with intuitive concepts.

(0) We use 0 to denote the equivalence class which contains the empty set. We also pick $\emptyset$ as the representative of this class (no other choice here if you think about it). So, we

can write

$$0 = |\emptyset|.$$

Thus, 0 describes the intuitive concept of **nothingness**.

(1) We choose the set $\{\emptyset\}$ to represent all the sets which are in a bijective correspondence with this set. So, the cardinality of $\{1\}, \{55\}, \{a\}, \{\square\}$, for example, is represented as the cardinality of $\{\emptyset\}$ and we use symbol 1 to represent this cardinality.

$$1 = |\{\emptyset\}|$$

Thus, 1 corresponds to the intuitive concept of **oneness**.

Note that the representative $\{\emptyset\}$ can be obtained as the union of the previous representative $\emptyset$ and the set containing the previous representative.

$$\{\emptyset\} = \emptyset \cup \{\emptyset\}.$$

(2) Continue the process by picking the next representative to be the union of the previous representative $\{\emptyset\}$ and the set which contains it $\{\{\emptyset\}\}$.

$$\{\emptyset, \{\emptyset\}\} = \{\emptyset\} \cup \{\{\emptyset\}\}.$$

The symbol 2 is used to denote the equivalence class of the sets in a bijective correspondence with this representative set.

$$2 = |\{\emptyset, \{\emptyset\}\}|.$$

So, 2 corresponds to the intuitive concept of **twoness**.

Continuing in this manner, we introduce $3, 4, \ldots$ as follows. that

$$3 = |\{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}|$$

$$4 = |\{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}, \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}\}| \text{ etc.}$$

The equivalence classes $0, 1, 2, \ldots$ and the representative sets $\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}, \ldots$ can also be *identified* (this approach is used when the cardinals are introduced via *ordinals* in a course focused on Set Theory exclusively). We use the ellipsis to write the list of the cardinals introduced in this way as $0, 1, 2, \ldots$ and we denote the set of all such cardinals by ω.

$$\omega = \{0, 1, 2, \ldots\}$$

Let us also introduce the **successor function** $S : \omega \to \omega$ given as follows: for a cardinal $n \in \omega$, we define its **successor** $n + 1$ as

$$n + 1 = n \cup \{n\}.$$

As n is represented by the set $\{0, 1, \ldots, n-1\}$, the union $n \cup \{n\}$ is equal to $\{0, 1, \ldots, n\}$ which represents the next cardinal $n + 1$.

A total order of cardinals. One can introduce a partial order on the class of cardinalities of sets by

$$|A| \leq |B| \quad \text{if there is an injection } A \to B.$$

As id_A is injective and the composition of two injective functions is injective (see part (3) of Exercise 23), the relation $\leq$ is reflexive and transitive. The statement that $\leq$ is antisymmetric is known as the *Schröder–Bernstein Theorem*. So, $\leq$ is a partial order on the class of all cardinals and it turns out that each two cardinals can be compared, so $\leq$ is a *total order*.

One can introduce the strict order $<$ as follows

$$|A| < |B| \quad \text{if } |A| \leq |B| \text{ and } A \not\approx B.$$

This order corresponds to the (expected) order of cardinals

$$0 < 1 < 2 < \dots$$

and, also, to the order of the representatives

$$\emptyset \subsetneq \{\emptyset\} \subsetneq \{\emptyset, \{\emptyset\}\} \subsetneq \dots$$

Moreover, every nonempty subset of ω has the least element (such a total order is said to be a *well-order*).

Finite and infinite sets, Cantor's Theorem. While we use ω to denote the set $\{0, 1, 2, \dots\}$, the symbol $\aleph_0$ is used to denote the **cardinality of** ω**.** So, we can write

$$\omega = \{0, 1, 2, \dots\} \text{ and } \aleph_0 = |\omega|.$$

The cardinality $\aleph_0$ is strictly larger than of any of the elements of ω. For example, the inclusion of $\{\emptyset, \{\emptyset\}\}$ into ω ensures that $2 \leq \aleph_0$. As ω contains $0, 1$ and 2 any function mapping ω to 2 has to have at least one of these three different elements mapped to the same element of 2 (0 or 1). Thus, such a function cannot be injective. As a result, there is no bijection between ω and 2 so $\aleph_0$ is strictly larger than 2.

A set is said to be **finite** if its cardinality is strictly less than $\aleph_0$ (thus it is one of $0, 1, 2, \dots$). A set is **infinite** otherwise. The above argument shows that ω is infinite. It can be shown that $\aleph_0$ is **the smallest infinite cardinal** and the subscript zero in the notation $\aleph_0$ indicates that. Any set with cardinality smaller than or equal to $\aleph_0$ is said to be **countable** and any set that is not countable is **uncountable**.

A natural question is: are there any cardinals strictly larger than $\aleph_0$? That is: are there uncountable sets? And the statement below implies that the answer is "yes, plenty".

Theorem 1. (Cantor's Theorem) *For any set A and its power set $\mathcal{P}(A)$,*

$$|A| < |\mathcal{P}(A)|.$$

The proof of the strict inequality between the two cardinalities above resembles the argument leading to Russell Paradox.

Proof. The relation $|A| \leq |\mathcal{P}(A)|$ holds because the function $A \to \mathcal{P}(A)$ given by $a \mapsto \{a\}$ is injective ($\{a\} = \{b\}$ indeed implies that $a = b$). Thus, to show that $|A|$ is strictly less than $|\mathcal{P}(A)|$, we need to show that $\mathcal{P}(A)$ and A are not equipotent, i.e. that there is no bijection $A \to \mathcal{P}(A)$.

Assume, on the contrary, that there is a bijection $f : A \to \mathcal{P}(A)$. In that case, consider the set $A_f = \{a \in A : a \notin f(a)\}$. By the definition of A_f, $A_f \subseteq A$, so $A_f \in \mathcal{P}(A)$. As f is onto, there is $a_f \in A$ such that $f(a_f) = A_f$. For such a_f we have that one of the two possibilities hold: either $a_f \in A_f$ or $a_f \notin A_f$. In the first case, we have that $a_f \notin f(a_f)$ by the definition of A_f. So, we have that both $a_f \in A_f$ and $a_f \notin f(a_f) = A_f$ hold which is a contradiction. In the second case, we have that $a_f \in f(a_f)$ by the definition of A_f. So, we have that both $a_f \notin A_f$ and $a_f \in f(a_f) = A_f$ hold which is also a contradiction.

This shows that our assumption that f is a bijection cannot be correct, so no such bijection f exists showing that $|A| \neq |\mathcal{P}(A)|$. This finishes the proof of $|A| < |\mathcal{P}(A)|$. □

Applied to the set $\omega = \{0, 1, 2, \ldots\}$, Cantor's theorem shows that $\aleph_0$ is strictly less that the cardinality of $\mathcal{P}(\omega)$. Continuing this argument, we obtain an infinite and strictly increasing chain of infinite cardinals.

$$|\omega| < |\mathcal{P}(\omega)| < |\mathcal{P}(\mathcal{P}(\omega))| < |\mathcal{P}(\mathcal{P}(\mathcal{P}(\omega)))| < \ldots$$

This shows that there are *infinitely many infinite cardinals* all mutually different from each other. Note that for a finite cardinal n, the cardinality of $\mathcal{P}(n)$ is 2^n (this can be shown by considering 2^n as the cardinal of the set of all functions from n considered as the set $\{0, 1, \ldots, n-1\}$ to the set 2 considered as the set $\{0, 1\}$). The formula $|\mathcal{P}(n)| = 2^n$ continue to hold for infinite cardinals also (more Set Theory is needed for a more formal argument) so we write $2^{\aleph_0}$ for the cardinality of the set $\mathcal{P}(\omega)$.

Continuum Hypothesis. The cardinal $\aleph_0$ is the smallest infinite cardinal (we would need a bit more on ordinals to be able to formally prove this statement which is intuitively clear). As we know that there is a strictly larger cardinal, the first next cardinal we call $\aleph_1$. The first next larger cardinal is $\aleph_2$ so we continue this sequence and have the chain below.

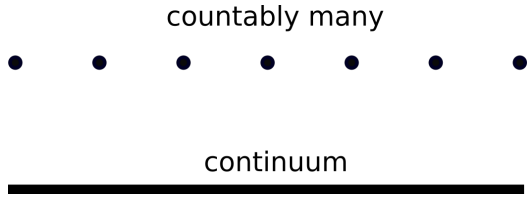
$$\aleph_0 < \aleph_1 < \aleph_2 < \ldots$$

As $\aleph_0 = |\omega| < |\mathcal{P}(\omega)| = 2^{\aleph_0}$, we know that $2^{\aleph_0}$ is equal to one of the alephs strictly larger than $\aleph_0$ but we cannot readily (or at all?) tell which aleph is equal to $2^{\aleph_0}$. Unable to show that there is any other cardinality between $\aleph_0$ and $2^{\aleph_0}$, Cantor conjectured that $2^{\aleph_0}$ is equal to the first next cardinal $\aleph_1$. This conjecture of Cantor is known as the

Continuum Hypothesis.

$$2^{\aleph_0} = \aleph_1$$

The name of this hypothesis comes from the statement we show in section 10: the cardinality of the set of real numbers, known as the **continuum** $\mathfrak{c}$, is equal to $2^{\aleph_0}$.



Cantor tried to prove this hypothesis for a long period of time. David Hilbert placed the question whether this hypothesis is true as the very first question on the list of 23 open questions he considered to be most crucial for the state of mathematics circa 1900. He presented 10 of the 23 problems at the International Congress of Mathematicians in Paris in 1900. At the moment, there are only 3 problems still unresolved (and two problems on the list are considered to vague to be solved). However, out of 18 solved problems, as many as 10 are solved in a way which still causes some controversy in mathematical community. The question whether the Continuum Hypothesis holds is one of them because the answer is

> neither "Yes, $2^{\aleph_0}$ is indeed equal to $\aleph_1$"
> nor "No, $2^{\aleph_0}$ is strictly larger than $\aleph_1$".

In 1940, Kurt Gödel proved that the second statement *cannot be proven* within the ZFC set theory. In 1964, Paul Cohen showed that the first statement *also cannot be proven* within the ZFC theory. Thus, the answer to the Hilbert's first problem is that

> both statements "$2^{\aleph_0} = \aleph_1$" and "$2^{\aleph_0} > \aleph_1$" can be neither proved nor disproved withing the ZFC theory – they are **independent** from the ZFC theory. So, the continuum hypothesis is **undecidable.**

This means that we can continue to build the set theory by either assuming $2^{\aleph_0} = \aleph_1$ or $2^{\aleph_0} > \aleph_1$ as one of the **axioms** of the new, larger theory we want to build.

Such position of the continuum hypothesis is not unique in mathematics – the Euclid's Fifth Postulate (recall that this postulate was discussed at the beginning of the section 1) cannot be proven from other axioms of geometry so either its statement or its negation can be taken to be the axioms. If the Fifth Postulate is assumed, one ends up with Euclidean Geometry. With its negation, we arrive either to elliptic (if there are no parallel lines) or hyperbolic geometries (if there are infinitely many lines passing a given point which do not intersect the given line).

After hearing about undecidability of the continuum hypothesis within ZFC, one may make an argument: so can we use another theory as a foundation of mathematics, possibly stronger than ZFC?

The answer to this question came from Kurt Gödel in the form of two statements known today as **Gödel's Incompleteness Theorems**. The first incompleteness theorem states that no consistent extension of ZF is decidable (so there is a statement which we cannot prove nor disprove within this system). The second incompleteness theorem, an extension of the first, states that the consistency of any extension of ZF cannot be proven using the methods within such extension.

At first this may seem like "bad news" for axiomatization of mathematics. However, one can interpret these results as only saying that a system capable of proving its own consistency is too simple to describe something as complex and as vast as entire arithmetic or set theory, let alone entire mathematics.

Addition and multiplication of cardinals. When wanting to determine the cardinal which would correspond to the cardinality of one set "plus" cardinality of the other, one may think of the cardinality of the union. However, if $A = \{1, 2, 3\}$ and $B = \{1, 2\}$, then the union has only three elements and not 3+2=5 elements and this discrepancy happens every time the two sets have *nonempty intersection*. So, before considering the union, one needs to *make the sets disjoint first*. This is obtained by considering any two different objects, for example, 1 and 2, or a and b, or $\square$ and $\triangle$. Then one would cross the first set with the one-element set containing the first of the two newly chosen elements and the second set with the one-element set containing the second of the two newly chosen elements. As the two sets obtained in this way have the same cardinality as the original sets but they are *disjoint*, their *union* has the cardinality which represents the sum of the two initial cardinalities.

For example, if A and B denote the two initial set and we use $\square$ and $\triangle$ for the two different objects, we form $A \times \{\square\}$ and $B \times \{\triangle\}$. Note that $|A| = |A \times \{\square\}|$ because the function $A \to A \times \{\square\}$ such that $a \mapsto (a, \square)$ is a bijection. And, similarly, $|B| = |B \times \{\triangle\}|$. The sets $A \times \{\square\}$ and $B \times \{\triangle\}$ are disjoint because no element of $A \times \{\square\}$ has $\triangle$ in the second coordinate. This enables us to define

$$|A| + |B| \text{ as } |(A \times \{\square\}) \cup (B \times \{\triangle\})|.$$

For example, if $A = \{1, 2, 3\}$ and $B = \{1, 2\}$, then $(A \times \{\square\}) \cup (B \times \{\triangle\}) = \{(1, \square), (2, \square), (3, \square), (1, \triangle), (2, \triangle)\}$ and this set has exactly five elements.

If the sets A and B are disjoint to start with, one does not necessarily have to consider their cross products with the two different objects because $A \cup B$ has the same cardinality as $(A \times \{\square\}) \cup (B \times \{\triangle\})$. For example, if A is the cardinal n (recall that we can identify the cardinal n with the representative set $\{0, 1, \ldots, n-1\}$, and B is $\{n\}$, then $A \cap B = \emptyset$ and

$$n + 1 = |A| + |B| = |A \cup B| = |n \cup \{n\}|.$$

This shows that the cardinality of $n \cup \{n\}$ corresponds to the **successor function** mapping n to $n + 1$.

The **product** of the cardinals corresponding to two sets A and B is the cardinality of the product $A \times B$.

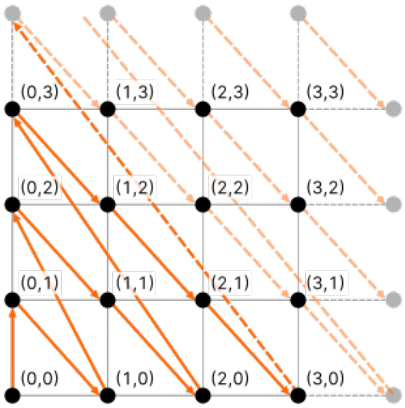
$$|A| \cdot |B| = |A \times B|$$

For example, if $A = \{1, 2, 3\}$ and $B = \{1, 2\}$, then $A \times B = \{(1, 1), (2, 1), (3, 1), (1, 2), (2, 2), (3, 2)\}$ and this set has exactly $3 \cdot 2 = 6$ elements.

If A and B are countable sets, we show that $A \times B$ is countable. We first show this claim for $A = \omega$ and $B = \omega$.

Claim 2. $|\omega \times \omega| = |\omega|$

Proof. To show the claim, we need to exhibit a bijection of $\omega \times \omega$ and ω. One such bijection $\omega \to \omega \times \omega$ can be obtained by "zigzagging" as on the figure on the right. So, $0 \mapsto (0, 0), 1 \mapsto (1, 0), 2 \mapsto (0, 1), 3 \mapsto (2, 0)$ etc. Such map is clearly injective and it is onto because the orange arrow on the figure passes every ordered pair. □



We can write the equation in the above claim as

$$\aleph_0 \cdot \aleph_0 = \aleph_0.$$

The claim and the practice problem (4b) below imply that if $|A| = \aleph_0$ and $|B| = \aleph_0$ then

$$|A \times B| = \aleph_0 \cdot \aleph_0 = \aleph_0.$$

So, if A and B are infinitely countable, then $A \times B$ is also infinitely countable. We utilize this fact when we determine the cardinality of the set of integers and the set of rationals in section 9. Section 9 also uses the following claim.

Let A be nonempty and finite and B be infinitely countable, say $|A| = n$ and $|B| = \aleph_0$. We claim that $|A \times B| = \aleph_0$. To see this, note that $|B| = |\{a\} \times B|$ for any $a \in A$. As $\{a\} \times B \subseteq A \times B$, we have that $\aleph_0 = |B| \leq |A \times B|$. On the other hand, we have that $|A| < \aleph_0$ so $|A| \cdot |B| < \aleph_0 \cdot \aleph_0 = \aleph_0$. Thus, we "sandwiched" $|A \times B|$ between two $\aleph_0$

$$\aleph_0 \leq |A \times B| \leq \aleph_0,$$

so $|A \times B| = \aleph_0$. We write this fact as

$$n \cdot \aleph_0 = \aleph_0$$

for any $n \in \omega, n \neq 0$. Similar arguments can be used for any infinite cardinal α

$$n \cdot \alpha = \alpha \text{ and } \alpha \cdot \alpha = \alpha.$$

Claim 3. *If A is an infinite set, a_0 an element of A, and b an element not in A, then*

$$|A| = |A \cup \{b\}| = |A - \{a_0\}|$$

This claim shows that an infinite set has the same cardinality as the set obtained by adding an element or taking one element out. Thus, none of these two processes change the cardinality of an infinite set.

Proof. As A is infinite, $|A| \geq |\omega|$. Thus, there is an injection $f : \omega \to A$. Let us define a bijection $g : A \to A \cup \{b\}$ by

$$g(a) = \begin{cases} b & a = f(0) \\ f(n-1) & a = f(n) \text{ for } n > 0 \\ a & a \neq f(n) \text{ for any } n \end{cases}$$

This map is clearly injective and it is onto because every element of A is either of the form $f(n)$ for some n or it is not of this form.

If A is infinite, then $A - \{a_0\}$ is infinite because if $|A - \{a_0\}| = n$ would imply that $|A| = n + 1$ which is strictly less than $|\omega|$ so we would reach a contradiction. Thus, the relation $|A| = |A - \{a_0\}|$ follows from $|A \cup \{b\}| = |A|$ applied to the infinite set $A - \{a_0\}$. □

Iterating the process described above, we have that

$$|A| = |A \cup \{b_0, b_1, \ldots, b_n\}| = |A - \{a_0, a_1, \ldots, a_n\}|$$

for an infinite set A, $n \in \omega$, $a_0, a_1, \ldots, a_n \in A$, and $b_0, b_1, \ldots, b_n$ elements not in A. We prove this using induction in one of the practice problems at the end of next section.

The relation $|A| = |A \cup \{b_0, b_1, \ldots, b_n\}|$ shows that if A is any infinite set, then

$$|A| + n = |A|.$$

In particular, $\aleph_0 + n = \aleph_0$.

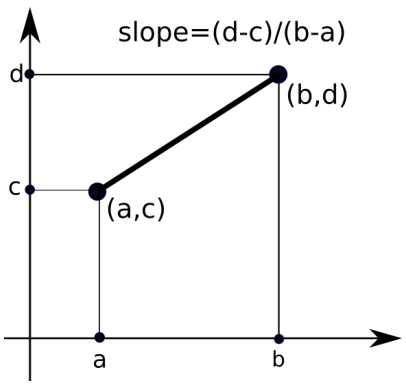
It also holds that $\aleph_0 + \aleph_0 = \aleph_0$ and we present a less formal argument for that. Let E be the set of even nonnegative integers and O be the set of odd positive integers. E and O are disjoint sets whose union is ω, so $|E| + |O| = |\omega| = \aleph_0$. Each set has cardinality $\aleph_0$ since $n \mapsto 2n$ is a bijection of $\omega \to E$ and $n \mapsto 2n + 1$ is a bijection $\omega \to O$. Hence $|E| = |O| = |\omega| = \aleph_0$.

If α is any infinite cardinal, one shows analogously that $\alpha + \alpha = \alpha$. So, we have that

$$n \cdot \alpha = \alpha \text{ and } \alpha \cdot \alpha = \alpha.$$

When intervals of real numbers are considered, one should not assume their *length* to be a measure of their cardinality. In fact, while (a, b) and (c, d) have different length when $b - a \neq d - c$, they have *the same cardinality* for any a, b, c, d such that $a < b$ and $c < d$.

To see this, note that finding the linear function which passes the points (a, c) and (b, d)



maps the interval (a, b) bijectively onto (c, d) as the figure above illustrates. See the first practice problem below for details on showing that such a linear function is bijective.

Practice Problems 6. (1) Show that the following pairs of sets have the same cardinality by explicitly producing a bijection between them.
   (a) The set of all positive integers and the set of even positive integers.
   (b) The interval $(5, 9)$ and the interval $(1, 7)$.
   (c) The interval $[5, 9]$ and the interval $[1, 7]$.

(2) Consider the following sets.

$$\mathcal{P}(A),\ \ \mathcal{P}(B),\ \ A \times B,\ \ \mathcal{P}(A \times B),\ \ \mathcal{P}(A) \times B,\ \ A \times \mathcal{P}(B),\ \text{ and }\ \mathcal{P}(A) \times \mathcal{P}(B)$$

Determine the cardinality of the above sets given the cardinalities of A and B. Express your answers in terms of the given cardinalities of A and B.
   (a) $|A| = 3$ and $|B| = 2$.
   (b) $|A| = \aleph_0$ and $|B| = 2$.

(3) Let $A_n = \omega - \{0, 1, 2, \ldots, n\}$ for $n \in \omega$. Determine the cardinality of the following sets.

$$A_n, \qquad A_n - A_{n+1}, \qquad \omega - A_n, \qquad \bigcap_{n\in\omega} A_n \qquad , \bigcup_{n\in\omega} A_n$$

(4) If A, B, C, and D are sets such that $|A| = |C|$ and $|B| = |D|$, show that the following holds.
   (a) $|A| + |B| = |C| + |D|$
   (b) $|A| \cdot |B| = |C| \cdot |D|$.

   This implies that the addition and multiplication of cardinals is *well-defined*.

(5) Show the following properties of the cardinal addition and multiplication.
   (a) $|A| + 0 = 0 + |A| = |A|$
   (b) $|A| + |B| = |B| + |A|$
   (c) $|A| \cdot 1 = 1 \cdot |A| = |A|$
   (d) $|A| \cdot |B| = |B| \cdot |A|$

Solutions. (1) (a) Let $A = \{1, 2, 3, \ldots\}$ and $B = \{2, 4, 6, \ldots\}$ be the two sets as required. Then $f : A \to B$ mapping n onto $2n$ is a function. Its inverse $g : B \to A$ can be defined by mapping an even positive integer of the form $2n$ onto n. Then for any n, we have that $g(f(n)) = g(2n) = n$ so $g \circ f$ is the identity on A and $f(g(2n)) = f(n) = 2n$, so $f \circ g$ is the identity on B. Thus, f is invertible and, hence, a bijection.

   (b) Any linear function mapping the endpoints of the interval onto the endpoints of the interval can be used. For example, we can take the linear function with the slope $\frac{7-1}{9-5} = \frac{6}{4} = \frac{3}{2}$ such that $y = 1$ when $x = 5$. Thus, $y - 1 = \frac{3}{2}(x - 5) \Rightarrow y = \frac{3}{2}x - \frac{13}{2}$. Thus, let $f : (5, 9) \to (7, 1)$ be given by $f(x) = \frac{3}{2}x - \frac{13}{2}$. The formula for the inverse can be obtained by solving $y = \frac{3}{2}x - \frac{13}{2}$ for $x : y + \frac{13}{2} = \frac{3}{2}x \Rightarrow x = \frac{2}{3}y + \frac{13}{3}$, so let $g : (7, 1) \to (5, 9)$ be given by $g(x) = \frac{2}{3}x + \frac{13}{3}$. Both compositions $g \circ f$ and $f \circ g$ are identity maps:

$$g(f(x)) = g\left(\frac{3}{2}x - \frac{13}{2}\right) = \frac{2}{3}\left(\frac{3}{2}x - \frac{13}{2}\right) + \frac{13}{3} = x - \frac{13}{3} + \frac{13}{3} = x \text{ and}$$

$$f(g(x)) = f\left(\frac{2}{3}x + \frac{13}{3}\right) = \frac{3}{2}\left(\frac{2}{3}x + \frac{13}{3}\right) - \frac{13}{2} = x + \frac{13}{2} - \frac{13}{2} = x$$

(c) Since f and g from the previous solution map the endpoints of the intervals onto the endpoints of the intervals, the same functions can be used.

(2) (a) If $|A| = 3$ and $|B| = 2$, then $|\mathcal{P}(A)| = 2^3 = 8$, $|\mathcal{P}(B)| = 2^2 = 4$, $|A \times B| = 3 \cdot 2 = 6$, $|\mathcal{P}(A \times B)| = 2^6 = 64$, $|\mathcal{P}(A) \times B| = 8 \cdot 2 = 16$, $|A \times \mathcal{P}(B)| = 3 \cdot 4 = 12$, and $|\mathcal{P}(A) \times \mathcal{P}(B)| = 8 \cdot 4 = 32$.

(b) If $|A| = \aleph_0$ and $|B| = 2$, then $|\mathcal{P}(A)| = 2^{\aleph_0}$, $|\mathcal{P}(B)| = 2^2 = 4$, $|A \times B| = \aleph_0 \cdot 2 = \aleph_0$, $|\mathcal{P}(A \times B)| = 2^{\aleph_0}$, $|\mathcal{P}(A) \times B| = 2^{\aleph_0} \cdot 2 = 2^{\aleph_0}$, $|A \times \mathcal{P}(B)| = \aleph_0 \cdot 4 = \aleph_0$, and $|\mathcal{P}(A) \times \mathcal{P}(B)| = 2^{\aleph_0} \cdot 4 = 2^{\aleph_0}$.

(3) If $A_n = \omega - \{0, 1, 2, \ldots, n\} = \{n+1, n+2, \ldots\}$, then $|A_n| = \aleph_0$. $A_n - A_{n+1} = \{n+1, n+2, \ldots\} - \{n+2, n+3, \ldots\}) = \{n+1\}$ so $|A_n - A_{n+1}| = 1$. $\omega - A_n = \omega - \{n+1, n+2, \ldots\} = \{0, 1, \ldots, n\}$, so $|\omega - A_n| = n + 1$.

Note that $A_0 = \{1, 2, \ldots\}, A_1 = \{2, 3, \ldots\}, A_2 = \{3, 4, \ldots\} \ldots$, so $\bigcap_{n\in\omega} A_n = \emptyset$ and $|\bigcap_{n\in\omega} A_n| = 0$. We also have that $\bigcup_{n\in\omega} A_n = \{1, 2, 3, \ldots\}$ so $|\bigcup_{n\in\omega} A_n| = |\omega| = \aleph_0$.

(4) As $|A| = |C|$ and $|B| = |D|$, there are bijections $f : A \to C$ and $g : B \to D$.

(a) Since $|A| + |B|$ is defined as $|(A \times \{\square\}) \cup (B \times \{\triangle\})|$ and $|C| + |D|$ is defined as $|(C \times \{\square\}) \cup (D \times \{\triangle\})|$, we need to show that

$$|(A \times \{\square\}) \cup (B \times \{\triangle\})| = |(C \times \{\square\}) \cup (D \times \{\triangle\})|$$

so we need to construct a bijection $F : (A \times \{\square\}) \cup (B \times \{\triangle\}) \to (C \times \{\square\}) \cup (D \times \{\triangle\})$. Let us define F by $(a, \square) \mapsto (f(a), \square)$ and $(b, \triangle) \mapsto (g(b), \triangle)$.
One can check directly that this function is one-to-one and onto. However, it may be shorter to show that if f^{-1} and g^{-1} are the inverses of f and g respectively, then the function $G : (C \times \{\square\}) \cup (D \times \{\triangle\}) \to (A \times \{\square\}) \cup (B \times \{\triangle\})$ given by $(c, \square) \mapsto (f^{-1}(c), \square)$ and $(d, \triangle) \mapsto (g^{-1}(d), \triangle)$ is the inverse of F. This holds since

$$(G \circ F)(a, \square) = G(F(a, \square)) = G(f(a), \square) = (f^{-1}(f(a)), \square) = (a, \square),$$

$$(G \circ F)(b, \triangle) = G(F(b, \triangle)) = G(g(b), \triangle) = (g^{-1}(g(b)), \triangle) = (b, \triangle),$$

$$(F \circ G)(c, \square) = F(G(c, \square)) = F(f^{-1}(c), \square) = (f(f^{-1}(c)), \square) = (c, \square),$$

$$(F \circ G)(d, \triangle) = F(G(d, \triangle)) = F(g^{-1}(d), \triangle) = (g(g^{-1}(d)), \triangle) = (d, \triangle)$$

which shows that $G \circ F$ is the identity on $(A \times \{\square\}) \cup (B \times \{\triangle\})$ and that $F \circ G$ is the identity on $(C \times \{\square\}) \cup (D \times \{\triangle\})$. Hence, F and G are inverse to each other and so F (and G) are bijections by Exercise 24.

(b) Since $|A| \cdot |B|$ is defined as $|A \times B|$ and $|C| \cdot |D|$ is defined as $|C \times D|$, we need to show that $|A \times B| = |C \times D|$. This means that we need to define a function $F : A \times B \to C \times D$ which will turn out to be a bijection. Let us define such a function $F : A \times B \to C \times D$ by $(a, b) \mapsto (f(a), g(b))$. If f^{-1} and g^{-1} are the inverses of f and g respectively, then let us also define $G : C \times D \to A \times B$ by $(c, d) \mapsto (f^{-1}(c), g^{-1}(d))$. Check that both $G \circ F$ and $F \circ G$ are the identities.

$$(G \circ F)(a, b) = G(F(a, b)) = G(f(a), g(b)) = (f^{-1}(f(a)), g^{-1}(g(b))) = (a, b) \text{ and}$$

$$(F \circ G)(c, d) = F(G(c, d)) = F(f^{-1}(c), g^{-1}(d)) = (f(f^{-1}(c)), g(g^{-1}(d))) = (c, d).$$

Thus, F and G are bijections by Exercise 24, so $|A \times B| = |C \times D|$ holds.

(5) (a) Note that $|A|+0$ is the cardinality of the set $(A\times\{\square\})\cup(\emptyset\times\{\triangle\})$. Since $\emptyset\times\{\triangle\} = \emptyset$, the above union is $A \times \{\square\}$. This set has the same cardinality as A since the function $f : A \to A \times \{\square\}$ given by $a \mapsto (a, \square)$ is one-to-one ($(a_1, \square) = (a_2, \square)$ implies $a_1 = a_2$) and onto (a is the original of $(a, \square)$).

One can show $0 + |A| = |A|$ similarly or, after having part (b), this relation follows from (b) and $|A| + 0 = |A.|$

(b) The function $f : (A \times \{\square\}) \cup (B \times \{\triangle\}) \to (B \times \{\square\}) \cup (A \times \{\triangle\})$ given by $(a, \square) \mapsto (a, \triangle)$ and $(b, \triangle) \mapsto (b, \square)$ is inverse to itself (check that $f(f(a, \square) = (a, \square)$ and $f(f(b, \triangle)) = (b, \triangle)$), so this shows that it is a bijection

(c) Let us use $\{0\}$ to represent 1. Checking that the function $f : A \to A \times \{0\}$ given by $a \mapsto (a, 0)$ is a bijection since $(a_1, 0) = (a_2, 0)$ implies $a_1 = a_2$ and a is the original of $(a, 0)$. This shows that $|A| \cdot 1 = |A|$. The relation $1 \cdot |A| = |A|$ can be shown analogously. Alternatively, it follows from part (b) and the relation $|A| \cdot 1 = |A|$.

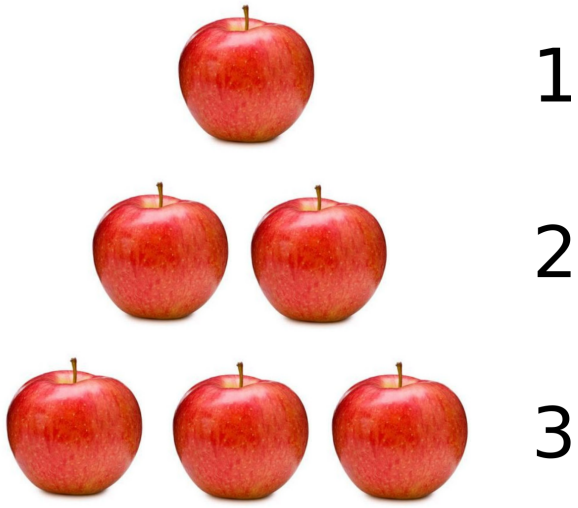
(d) The function $f : A \times B \to B \times A$ given by $(a, b) \mapsto (b, a)$ is inverse to itself since

$$f(f(a, b)) = f(b, a) = (a, b).$$

So, it is invertible and, hence, a bijection by Exercise 24. This shows that $|A \times B| = |B \times A|$ and so $|A| \cdot |B| = |B| \cdot |A|$.

7. Natural numbers and induction

Counting. Let us consider the finite cardinals $0, 1, 2, \ldots$. As the intent was when we were introducing them, the elements $0, 1, 2, \ldots$ correspond exactly to the outcome of *counting finitely many objects* (with zero representing the number of no objects at all) and they are called the **natural numbers**. The set of natural numbers is usually denoted by $\mathbb{N}$. Because 0 is, technically, not the outcome of counting any number of physical objects, 0 is sometimes not considered to be a natural number. However, as 0 is also a finite cardinal, just as $1, 2, \ldots$ are, in many cases 0 *is* considered to be a natural number and we adopt such treatment of zero.



Note that the set $\mathbb{N}$ is the same set as ω from the previous section. The notation $\mathbb{N}$ is used when considered the elements of ω as objects of arithmetic and the elements of larger number sets we will be considering in the following section. The notation ω is used when considering the natural numbers as representative sets of finite cardinalities.

Addition and multiplication. The multiplication and addition defined in the previous section can be shown to correspond to the well-known addition and multiplication of natural numbers. These two operations can also be defined **inductively**, using the **successor function** S (introduced in section 6) as follows. If m is any natural number, we are defining $m + n$ for any other natural number n by specifying that

$$\begin{aligned} m + 0 &= m \\ m + S(n) &= S(m + n) \end{aligned}$$

The first line of this definition specifies how to add zero to any natural number m. The second line of this definition specifies how to add $n + 1$ to m assuming that we know how to add n to m. So, the above two specifications are enough for us to be able to compute the sum of any two natural numbers. For example, we compute 3+2 as follows.

$$3 + 2 = S(3 + 1) = S(S(3 + 0)) = S(S(3)).$$

The multiplication can be also **inductively** defined as follows. If m is any natural number, we are defining $m \cdot n$ for any other natural number n by specifying that

$$\begin{aligned} m \cdot 0 &= 0 \\ m \cdot S(n) &= m \cdot n + m \end{aligned}$$

Thus, this specifies that we can $3 \cdot 2$, for example, as follows.

$$3 \cdot 2 = 3 \cdot 1 + 3 = 3 \cdot 0 + 3 + 3 = 0 + 3 + 3$$

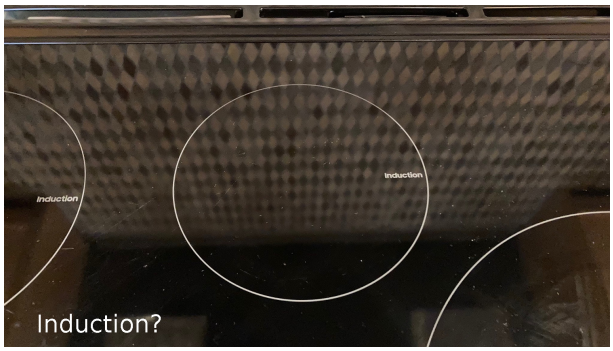
which shows that considering 3 twice is exactly the same thing as the sum 0+3+3. One would have to convince themselves that we do not have to write parenthesis for addition and multiplication so that these operations are **associative**. Note that we already used this fact when writing $(0 + 3) + 3$ as $0 + 3 + 3$.

These inductive definitions are not the first appearance of inductive definitions in this text: the definitions of sentences in both propositional and predicate logic are also inductive.

Mathematical induction. The induction is used whenever we write the ellipsis: when we write $0, 1, 2, \ldots$, for example, we are implicitly stating that if we know the initial element of the list and if we know how to proceed from the initial to the second element in the list and from the second to the third, that we will be able to form the fourth element using the third, and the fifth using the fourth and so on: knowing the n-th term, we can create the $(n+1)$-st term.

The above argument gives rise to a general method of proving statements about natural numbers called **mathematical induction:** to prove that a statement $P(n)$ holds for any natural number n, one proves the following two steps.

1. $P(0)$ holds.
2. If $P(n)$ holds, then $P(n+1)$ holds.



Example 3. Show the distributivity of addition and multiplication using induction: for any three natural numbers k, m, and n, show that

$$(k+m)\cdot n = k\cdot n + m\cdot n.$$

Solution. Let us fix the natural numbers k and m. The induction method states that the above statement holds if we manage to show that 1 and 2 below hold.

1. $(k+m)\cdot 0 = k\cdot 0 + m\cdot 0$
2. If $(k+m)\cdot n = k\cdot n + m\cdot n$, then $(k+m)\cdot(n+1) = k\cdot(n+1) + m\cdot(n+1)$.

Using the first step of definition of multiplication and addition,

$$(k+m)\cdot 0 = 0 = 0+0 = k\cdot 0 + m\cdot 0$$

which shows that 1 holds. Assume now that $(k+m)\cdot n = k\cdot n + m\cdot n$ holds. We show 2 as follows.

$$\begin{aligned}
(k+m)\cdot(n+1) &= (k+m)\cdot n + k + m && \text{(by step 2 of the definition of } \cdot) \\
&= k\cdot n + m\cdot n + k + m && \text{(by the induction assumption)} \\
&= k\cdot n + k + m\cdot n + m && \text{(by commutativity of } +, \\
& && \text{see practice problem 2b of section 6)} \\
&= k\cdot(n+1) + m\cdot(n+1) && \text{(by step 2 of the definition of } \cdot).
\end{aligned}$$

For a natural number m, let us define the **power function** $n \mapsto m^n$ by

$$\begin{aligned}
m^0 &= 1 \\
m^{n+1} &= m^n \cdot m
\end{aligned}$$

As it is customary, we suppress writing $\cdot$ sign for every multiplication and we shorten $m\cdot n$ to mn. Occasionally and for emphasis, we continue to write mn as $m\cdot n$.

Exercise 27. For natural numbers k and m, show that the statements below hold for every natural number n.

(1) $(km)^n = k^n m^n$
(2) $k^{m+n} = k^m k^n$
(3) $(k^m)^n = k^{mn}$

Solution. (1) Step 1 is to show that $(km)^0 = k^0 m^0$. As $(km)^0$, k^0, and m^0 are all equal to 1 and $1 = 1 \cdot 1$, we have that $(km)^0 = 1 = 1 \cdot 1 = k^0 m^0$.

To show step 2 assume that $(km)^n = k^n m^n$ holds and show that $(km)^{n+1} = k^{n+1} m^{n+1}$.

$$\begin{array}{rcll} (km)^{n+1} & = & (km)^n \, km & \text{(by step 2 of the definition of the power function)} \\ & = & k^n m^n \, km & \text{(by the induction assumption)} \\ & = & k^n k \, m^n m & \text{(by commutativity of } \cdot\text{)} \\ & & & \text{see practice problem 2d of section 6)} \\ & = & k^{n+1} m^{n+1} & \text{(by step 2 of the definition of the power function).} \end{array}$$

(2) Step 1 is to show that $k^{m+0} = k^m k^0$. This holds since $k^{m+0} = k^m = k^m \cdot 1 = k^m k^0$. To show step 2, assume that $k^{m+n} = k^m k^n$ holds and show that

$$\begin{array}{rcll} k^{m+n+1} & = & k^{m+n} \, k & \text{(by step 2 of the definition of the power function)} \\ & = & k^m k^n \, k & \text{(by the induction assumption)} \\ & = & k^m k^{n+1} & \text{(by step 2 of the definition of the power function).} \end{array}$$

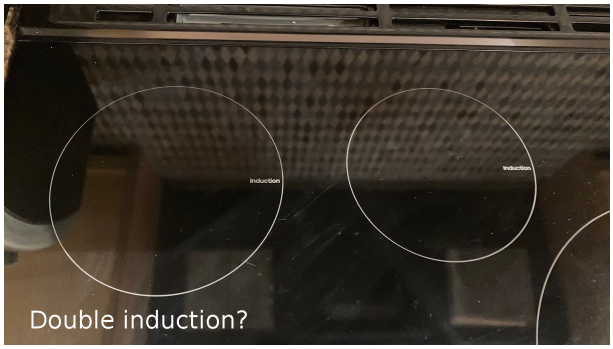
(3) Step 1 is to show that $(k^m)^0 = k^{m \cdot 0}$. This holds since $(k^m)^0 = 1 = k^0 = k^{m \cdot 0}$. To show step 2, assume that $(k^m)^n = k^{mn}$ holds and show that

$$\begin{array}{rcll} (k^m)^{n+1} & = & (k^m)^n \, k^m & \text{(by step 2 of the definition of the power function)} \\ & = & k^{mn} k^m & \text{(by the induction assumption)} \\ & = & k^{mn+m} & \text{(by the previous property we showed)} \\ & = & k^{m(n+1)} & \text{(by step 2 of the definition of } \cdot\text{).} \end{array}$$

Double induction. Double induction can be used to show that statements of the form $P(m, n)$ hold for all natural numbers m and n.

The method has the following form.

1. Show that $P(0, n)$ holds by showing
   1a. $P(0, 0)$ holds.
   1b. If $P(0, n)$, then $P(0, n + 1)$ holds.
2. Assuming that $P(m, n)$ holds, show that $P(m + 1, n)$ holds.



Let us illustrate this method by showing the statement from the following exercise.

Exercise 28. For any two natural numbers m and n,

if $m \leq n$, then there is unique k such that $m + k = n$.

Solution. Let $P(m, n)$ stand for the statement "if $m \leq n$, then there is unique k such that $m + k = n$".

When $m = n = 0$, the statement reduces to a true implication since the premise $0 \leq 0$ is true and the conclusion is true for $k = 0$. Such $k = 0$ is unique because if $0 + k' = 0$, then $k' = 0$ (because $0 + k' = k'$).

Assuming that $P(0, n)$ holds, let us show that $P(0, n+1)$ holds. So, assume that the premise $0 \leq n + 1$ of $P(0, n + 1)$ holds. Taking $n + 1$ for k, we have that $0 + k = k = n + 1$. To show uniqueness, if $0 + k' = n + 1$, then $k' = n + 1$ since $0 + k' = k'$. This concludes the proof of the first step.

To show the second step, assume that $P(m,n)$ holds and let us show $P(m+1,n)$. Assume that the assumption $m+1 \leq n$ of $P(m+1,n)$ holds. Hence $m < m+1 \leq n$ holds so the assumption $m \leq n$ of $P(m,n)$ also holds. So, there is unique l such that $m+l=n$. Since $m<n$, such l is strictly larger than zero (assuming otherwise $l=0$ leads to a contradiction $m=m+0=n$). As $l>0$, l is a successor of its predecessor, so $l=k+1$ for some natural number k. We have that $(m+1)+k=m+(k+1)$ by associativity and commutativity of $+$, so

$$(m+1)+k=m+(k+1)=m+l=n$$

where the last equality holds by the induction hypothesis. Such k is unique since $(m+1)+k'=n$ implies that $m+(k'+1)=n$ which implies $k'+1=l$ by the uniqueness in the induction hypothesis. This means that k and k' have the same successor and so $k=k'$.

The above exercise enables us to define a partial operation **subtraction** $-$ as follows

$$n-m=k \quad \text{if} \quad n=k+m$$

This operation is a *partial* operation since $n-m$ is defined only when $m \leq n$. For example, $2-3$ is not defined.

As corollary of the above exercise, the addition is **cancellative** and **monotonous**.

Exercise 29. For a natural number k, show that the following statements hold for any natural numbers m and n.

(1) (cancellativity of $+$) If $m+k=n+k$, then $m=n$.
(2) (monotony of $+$) If $m \leq n$, then $m+k \leq n+k$.

Solution. (1) We can show this statement by using the previous exercise. Assume that $m+k=n+k$. As natural numbers are totally ordered, we have that $m \leq n$ or $n \leq m$ hold. If $m \leq n$, there is a unique l such that $n=m+l$. Hence $m+k=n+k=m+l+k$. Since 0 is the unique natural number such that $m+k+0=m+k$, we have that $l=0$. Thus, the relation $n=m+l$ becomes the required $m=n$.

(2) Let $P(m,n)$ stands for the statement "if $m \leq n$, then $m+k \leq n+k$".

When $m=n=0$, the statement reduces to a true implication since the premise $0 \leq 0$ is true and the conclusion $0+k=k \leq k=0+k$ is also true. Assuming that $P(0,n)$ holds, let us show that $P(0,n+1)$ holds. Assume that the premise $0 \leq n+1$ of $P(0,n+1)$ holds (which is, in fact, true for any natural number n) and let us show that $0+k \leq n+1+k$. As $0 \leq n$, the premise of $P(0,n)$ holds, so the conclusion $0+k \leq n+k$ also holds.

As $\leq$ is transitive and the successor of a natural number is strictly larger than that natural number, we have that

$$0+k \leq n+k \leq (n+k)+1=n+1+k.$$

This shows that $P(0,n+1)$ holds and concludes the proof of the first step.

To show the second step, assume that $P(m,n)$ holds and show that $P(m+1,n)$ holds. Assume that the premise $m+1 \leq n$ of $P(m+1,n)$ holds and let us show the conclusion $m+1+k \leq n+k$. Since $m+1 \leq n$ and $m<m+1$, we have that $m<n$. By $P(m,n)$, this implies that $m+k \leq n+k$. We claim that $m+k<n+k$. Indeed, assuming that $m+k=n+k$, we have that $m=n$ by cancellation and this is a contradiction with $m<n$. Hence, $m+k<n+k$. This implies that the successor $m+k+1$ of $m+k$ is less than or equal to $n+k$.

One can show analogous statements for multiplication. For every m and n such that $0 < m \leq n$, there are unique k and $l < m$ such that

$$n = km + l$$

We say that k is the **quotient** and l is the **remainder**. This enables us to define a partial operation : which we call division, by

$$n : m = k \quad \text{if} \quad n = k \cdot m$$

Just as subtraction, division is only a *partial* operation since it is not defined for every pair of natural numbers. For example, $2 : 3$ is not defined. It can also be shown that the multiplication is cancellative and monotonous in the following sense.

(cancellativity of $\cdot$) If $mk = nk$ and $k \neq 0$, then $m = n$.
(monotony of $\cdot$) If $m \leq n$, then $mk \leq nk$.

Limited induction. In some cases, we may wish to prove a statement $P(n)$ on all natural numbers n such that $n \geq k$ for a natural number k. In cases like this, the two steps modify as follows.

1. $P(k)$ holds.
2. If $P(n)$ holds for $n \geq k$, then $P(n+1)$ holds.

Exercise 30. Show that the following statements hold for all $n \geq 3$.

(1) $2n > 2 + n$ (2) $2^n > 2n$

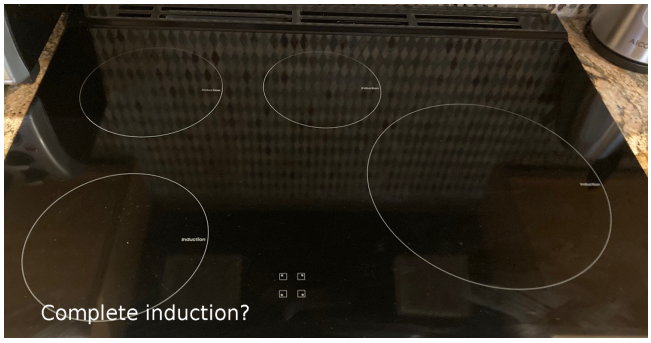
Solution. (1) The first step is to show that this statement holds for $n = 3$. This holds as $2(3) = 6 > 5 = 2 + 3$. Assuming that $2n > 2 + n$ holds for $n \geq 3$, let us show that $2(n+1) > 2 + n + 1$. This holds since $2(n+1) = 2n + 2 > 2 + n + 2$ by the induction hypothesis. As $2 > 1$, we have that $2 + n + 2 > 2 + n + 1$, so $2(n+1) = 2n + 2 > 2 + n + 2 > 2 + n + 1$ as needed.

(2) The statement holds for $n = 3$ since $2^3 = 8 > 6 = 2(3)$. Assume that it holds for $n \geq 3$. Then, we have that

$$\begin{aligned} 2^{n+1} &= 2^n \cdot 2 && \text{(by step 2 of the definition of the power function)} \\ &> 2n \cdot 2 && \text{(by the induction hypothesis and the monotony of } \cdot) \\ &> 2n + 2 && \text{(by part (1) for } 2n, \text{ applicable since } n \geq 3 \text{ so that } 2n > n + 2 > n \geq 3) \\ &= 2(n+1) && \text{(by distributivity).} \end{aligned}$$

Complete induction. Complete (or strong) induction is a variant of the induction method for proving that a statement of the form $P(n)$ holds for all n by showing the steps below.

1. $P(0)$ holds.
2. If $P(k)$ holds for all $k \leq n$, then $P(n+1)$ holds.



The assumption of the second step is stronger than the assumption of the second step in the basic induction format, so this is why this method is referred to as the strong induction. However, this method is, in fact, equivalent, to the basic method.

Complete induction is used for finding an explicit formula for a sequence a_n given by a recursive equation which describes a_{n+1} in terms of more than one previous term. The next example illustrates such scenario.

Example 4. Show that the sequence given by the **recursive equation** below

$$a_{n+1} = 2a_n - a_{n-1}, \qquad a_0 = 0, \;\; a_1 = 1$$

produces all natural numbers and can be defined also by $a_n = n$.

Solution. The sequence starts with $a_0 = 0$ which matches the formula $a_n = n$ for $n = 0$. Assuming that $a_k = k$ for all natural numbers $k \leq n$, let us show that $a_{n+1} = n + 1$. The induction hypothesis implies that $a_n = n$ and $a_{n-1} = n - 1$ so we have that

$$a_{n+1} = 2a_n - a_{n-1} = 2n - (n - 1) = 2n - n + 1 = n + 1.$$

This method can be applied when checking that an explicit formula $a_n = f(n)$ (also called the **closed form** of the sequence) is producing the elements of a sequence a_n given by a recursive formula

$$a_{n+1} = F(a_0, a_1, \ldots, a_n).$$

The next example displays another scenario when complete induction can be used.

Example 5. Show that for every nonzero natural number n there are natural numbers k and l such that

$$n = 2^k(2l + 1).$$

Solution. Let $P(n)$ be the statement "$n = 2^k(2l+1)$ for some natural numbers k and l". The assumption that n is nonzero makes us start the induction by showing that $P(1)$ holds. It does since $1 = 2^0(2(0) + 1)$ so we can take $k = l = 0$.

Note that assuming that $n = 2^k(2l + 1)$ does not seem to help with representing $n + 1 = 2^k(2l+1)+1$ as a product of the power of 2 and an odd number. However, using the induction hypothesis for some conveniently chosen natural number smaller than $n+1$ and larger or equal to 1 may be more effective than using the hypothesis for $n-1$. This is why we choose to use the complete induction here. Hence, let us assume that any number less or equal to n and greater or equal to 1 can be represented in the required format and let us consider $n + 1$.

If $n + 1$ is even, then $n + 1 = 2m$ where m is smaller than n (because $n + 1 \geq 2$ in this case so "half" of $n + 1$ is larger than or equal to 1). Using the induction hypothesis for m produces k and l such that $m = 2^k(2l + 1)$. Then we have that

$$n + 1 = 2m = 2 \cdot 2^k(2l + 1) = 2^{k+1}(2l + 1).$$

If $n + 1$ is odd then n is even and we have that $n = 2l$ for some l. Then we can take k to be zero and have

$$n + 1 = 2^0(2l + 1).$$

Mathematical induction is often used for showing **identities** involving sums of finitely many terms on one side and compact formulas containing only one term on the other side. The first practice problem contains some examples.

Mathematical induction is also often used for showing statements on **divisibility** of positive integers. The second practice problem contains some examples.

A third type of problems often shown using induction are problems involving **inequalities**. The third practice problem contains examples.

Practice Problems 7. (1) Use induction to show that the following formulas hold for every natural number.

(a)
$$0 + 1 + 2 + \ldots + n = \frac{n(n+1)}{2}$$

(b)
$$1 + 3 + 5 + \ldots + (2n+1) = (n+1)^2$$

(c) For every real number $x \neq 1$,
$$1 + x + x^2 + \ldots + x^n = \frac{1 - x^{n+1}}{1 - x}$$

(d) If $|A| = n$, then $|\mathcal{P}(A)| = 2^n$.

(e) If A is an infinite set, n a natural number, $a_0, a_1, \ldots, a_n$ elements of A and $b_0, b_1, \ldots, b_n$ elements not in A, then
$$|A| = |A \cup \{b_0, b_1, \ldots, b_n\}| = |A - \{a_0, a_1, \ldots, a_n\}|.$$

(2) Show the following statements on divisibility using induction.

(a) $n^3 + 2n$ is divisible by 3 for any natural number n.

(b) $6^n - 1$ is divisible by 5 for any natural number $n > 0$.

(3) The factorial function $f(n) = n!$ which you may have encountered in Calculus 2, is usually introduced by the formula $n! = 1 \cdot 2 \cdot 3 \cdot \ldots \cdot n$. The use of ellipsis indicate an inductive argument. Without using ellipsis, the function can be defined recursively as
$$0! = 1, \qquad (n+1)! = n! \cdot (n+1).$$
Using this definition, show that the factorial function is increasing faster than the exponential function:
$$n! > 2^n \text{ for all } n \geq 4.$$

(4) Show that the n-th derivative of $f(x) = \frac{1}{1-x}$ is $f^{(n)}(x) = \frac{n!}{(1-x)^{n+1}}$ for $n = 0, 1, 2, \ldots$

Deduce that $f^{(n)}(0) = n!$ holds for any natural number n. This may explain the Calculus 3 formula $\frac{1}{1-x} = \sum_{n=0}^{\infty} x^n$ for the power series expansion of $f(x)$ at $x = 0$.

(5) Show the monotony of the power function: for any natural number $k \geq 1$ and natural numbers m and n,
$$\text{if } m \leq n, \text{ then } k^m \leq k^n.$$

(6) Show that the given formulas of the form $a_n = f(n)$ are closed forms of the given recursive sequences.

(a) Recursive definition: $a_{n+1} = a_n + 5, a_1 = 3.$ Closed form: $a_n = 5n - 2.$

(b) Recursive definition: $a_{n+1} = 2a_n - a_{n-1}, a_0 = 2, a_1 = 5.$ Closed form: $a_n = 3n + 2.$

(c) Recursive definition: $a_{n+1} = 4a_n - 4a_{n-1}, a_0 = 0, a_1 = 2.$ Closed form: $a_n = n2^n.$

Solutions. (1) (a) The formula holds for $n = 0$ since the left side consists of a single term 0 and the right side is $\frac{0(0+1)}{2} = 0$. Assume the formula holds for n and let us show it for $n + 1$. By induction hypothesis, the first equality below holds.
$$0 + 1 + 2 + \ldots + n + (n+1) = \frac{n(n+1)}{2} + (n+1) = \frac{n(n+1)}{2} + \frac{2(n+1)}{2} =$$

$$\frac{n(n+1)+2(n+1)}{2} = \frac{(n+1)(n+2)}{2}.$$

(b) The formula holds for $n = 0$ since the left side consists of a single term $2(0)+1 = 1$ and the right side is $(0+1)^2 = 1$. Assume the formula holds for n and let us show it for $n+1$. By induction hypothesis, the first equality below holds.

$$1+3+5+\ldots+(2n+1)+2(n+1)+1 = (n+1)^2+2(n+1)+1 =$$

$$n^2+2n+1+2n+2+1 = n^2+4n+4 = (n+2)(n+2) = (n+2)^2.$$

(c) Let x be a real number $x \neq 1$. The formula holds for $n = 0$ since the left side consists of a single term 1 and the right side is $\frac{1-x^{0+1}}{1-x} = \frac{1-x}{1-x} = 1$. Assume the formula holds for n and let us show it for $n+1$. By induction hypothesis, the first equality below holds.

$$1+x+x^2+\ldots+x^n+x^{n+1} = \frac{1-x^{n+1}}{1-x}+x^{n+1} = \frac{1-x^{n+1}}{1-x}+\frac{x^{n+1}(1-x)}{1-x} =$$

$$\frac{1-x^{n+1}+x^{n+1}1-x^{n+2}}{1-x} = \frac{1-x^{n+2}}{1-x}.$$

(d) If $|A| = 0$, then A is the empty set and $\mathcal{P}(A) = \{\emptyset\}$. Hence $|\mathcal{P}(A) = 1 = 2^0$. Assuming the formula holds for sets with n elements, let us show it for a set A with $n+1$ element. Pick arbitrary $a \in A$ and let $B = A - \{a\}$. Then B has n elements so $|\mathcal{P}(B)| = 2^n$. Every subset of A is either a subset C of B or is of the form $C \cup \{a\}$ for a subset C of B. The number of such subsets C is 2^n by the induction hypothesis. So, the total number of subsets of A is the number $C \subseteq B$ plus the number of $C \cup \{a\}$ for $C \subseteq B$. Hence, it is

$$2^n + 2^n = 2^n(1+1) = 2^n \cdot 2 = 2^{n+1}.$$

(e) We show the two equalities $|A| = |A \cup \{b_0, b_1, \ldots, b_n\}|$ and $|A| = |A - \{a_0, a_1, \ldots, a_n\}|$. If $n = 0$, both hold by Claim 3. Let us show the first one by induction. As we already have the induction base, let us assume the claim holds for n and consider the elements $b_0, b_1, \ldots, b_n, b_{n+1}$ not in A. If h is a bijection $A \to A \cup \{b_0, b_1, \ldots, b_n\}$ and g a bijection $A \cup \{b_0, b_1, \ldots, b_n\} \to A \cup \{b_0, b_1, \ldots, b_n, b_{n+1}\}$ constructed as in the proof of Claim 2, their composition is a bijection $A \to A \cup \{b_0, b_1, \ldots, b_n, b_{n+1}\}$. The second equality follows from the first by considering the infinite set $A - \{a_0, a_1, \ldots, a_n\}$ and adding to it the elements $a_0, a_1, \ldots, a_n$.

(2) (a) If $n = 0$, then $n^3 + 2n = 0$ and 0 is divisible by 3. Assume that $n^3 + 2n$ is divisible by 3. Recall that this means that $n^3 + 2n = 3k$ for some natural number k. Let us show that $(n+1)^3 + 2(n+1)$ is also divisible by 3. Try to write this last expression as a sum of $n^3 + 2n$, so that we can use the induction hypothesis, and another term which is a multiple of 3 and, hence, divisible by 3. Foil $(n+1)^3$ to get $n^3 + 3n^2 + 3n + 1$ so that we have the following.

$$(n+1)^3 + 2(n+1) = n^3 + 3n^2 + 3n + 1 + 2n + 2 = n^3 + 2n + 3n^2 + 3n + 3 =$$

$$(n^3 + 2n) + 3(n^2 + n + 1) = 3k + 3(n^2 + n + 1) = 3(k + n^2 + n + 1)$$

The last expression is divisible by 3 since it is a multiple of 3.

(b) Since $n > 0$, we start the induction at $n = 1$. For $n = 1$, $6^n - 1 = 6 - 1 = 5$ and it is divisible by 5. Assume that $6^n - 1$ is divisible by 5 and write $6^n - 1 = 5k$ for some natural number k. Let us show that $6^{n+1} - 1$ is divisible by 5. Note that $6^{n+1} - 1 = 6 \cdot 6^n - 1$. From the induction hypothesis $6^n - 1 = 5k$, we have that $6^n = 5k + 1$. Substituting $5k + 1$ for 6^n in the inductive step, we have the following.

$$6^{n+1} - 1 = 6 \cdot 6^n - 1 = 6(5k + 1) - 1 = 30k + 6 - 1 = 30k + 5 = 5(6k + 1)$$

This last expression is divisible by 5 since it is a multiple of 5.

(3) Use the limited induction starting with $n = 4$. The formula $n! > 2^n$ holds for $n = 4$ since it becomes $4! = 24 > 16 = 2^4$. Assume the formula to be true for n and let us show it for $n + 1$. Note that $n + 1 > 2$ for any $n \geq 4$ because $n + 1$ is taking values $5, 6, 7, \ldots$ and they are all larger than 2. So, we have that

$$(n + 1)! = n! \cdot (n + 1) > 2^n \cdot (n + 1) > 2^n \cdot 2 = 2^{n+1}$$

where the first relation holds by the recursive definition of the factorial, the second relation holds by the inductive hypothesis and the third relation holds by the observation that $n + 1 > 2$ for $n \geq 4$.

(4) As the zeroth derivative is just the function itself, the formula $f^{(n)}(x) = \frac{n!}{(1-x)^{n+1}}$ holds for $n = 0$ since $\frac{0!}{(1-x)^{0+1}} = \frac{1}{1-x} = f(x)$. Assuming the formula holds for n, differentiate both sides of $f^{(n)}(x) = \frac{n!}{(1-x)^{n+1}}$ to get that

$$f^{(n+1)}(x) = \frac{d}{dx}\left(\frac{n!}{(1-x)^{n+1}}\right) = \frac{d}{dx}\left(n!(1-x)^{-(n+1)}\right) = n!(-(n+1))(1-x)^{-(n+1)-1}(-1) =$$

$$n!(n+1)(1-x)^{-n-2} = (n+1)!(1-x)^{-(n+2)} = \frac{(n+1)!}{(1-x)^{n+2}}.$$

This shows the required formula. Plugging 0 for x in it produces

Deduce that $f^{(n)}(0) = \frac{n!}{(1-0)^{n+1}} = \frac{n!}{1} = n!$ and substituting this in the formula $f(x) = \sum_{n=0}^{\infty} \frac{f^{(n)}(0)}{n!} x^n$ for the Taylor series expansion at $x = 0$ produces $\frac{1}{1-x} = \sum_{n=0}^{\infty} \frac{n!}{n!} x^n = \sum_{n=0}^{\infty} x^n$.

(5) Let $P(m, n)$ stands for the statement "if $m \leq n$, then $k^m \leq k^n$".

When $m = n = 0$, the statement reduces to a true implication since the premise $0 \leq 0$ is true and the conclusion $k^0 = 1 \leq 1 = k^0$ is also true. Assuming that $P(0, n)$ holds, let us show that $P(0, n+1)$ holds. Assume that the premise $0 \leq n+1$ of $P(0, n+1)$ holds (which is, in fact, true for any natural number n) and let us show that $k^0 \leq k^{n+1}$. As $0 \leq n$, the premise of $P(0, n)$ holds, so the conclusion $k^0 \leq k^n$ also holds. By monotony of the multiplication, we have that the induction hypothesis $k^0 \leq k^n$ and $1 \leq k$ imply that $k^0 \cdot 1 \leq k^n \cdot k$. So, we have that

$$k^0 = 1 = 1 \cdot 1 \leq k^n \cdot k = k^{n+1}.$$

This shows that $P(0, n + 1)$ holds and concludes the proof of the first step.

To show the second step, assume that $P(m, n)$ holds and show that $P(m+1, n)$ holds. Assume that the premise $m+1 \leq n$ of $P(m+1, n)$ holds and let us show the conclusion $k^{m+1} \leq k^n$. Since $m + 1 \leq n$ and $m < m + 1$, we have that $m < n$. By $P(m, n)$, this implies that $k^m \leq k^n$. We also know that $1 \leq k$ so multiplying the last two relations produces

$$k^m \leq k^n \cdot k = k^{n+1}.$$

(6) (a) As the initial term is given with $n = 1$, use limited induction and show the claim for all $n \geq 1$.
The closed form matches the recursive equation for $n = 1$ since $a_1 = 3$ and $5(1)-2 = 3$. Assuming the closed form and the recursive formula to agree for n, let us show that they agree for $n + 1$. On one hand, $a_{n+1} = a_n + 5 = 5n - 2 + 5 = 5n + 3$. On the other hand, $a_{n+1} = 5(n + 1) - 2 = 5n + 5 - 2 = 5n + 3$. Thus, the two formulas match.

(b) The closed form matches the recursive equation for $n = 0$ since $a_0 = 2$ and $3(0)+2 = 2$. Use complete induction, so assume the two formulas to match for all $k \leq n$ and show that $a_{n+1} = 3(n + 1) + 2 = 3n + 5$ using the recursive formula. This holds by the argument below.

$$a_{n+1} = 2a_n - a_{n-1} = 2(3n + 2) - (3(n - 1) + 2) = 6n + 4 - 3n + 3 - 2 = 3n + 5.$$

(c) The closed form matches the recursive equation for $n = 0$ since $a_0 = 0$ and $(0)2^0 = 0$. Use complete induction, so assume the two formulas to agree for all $k \leq n$ and show that $a_{n+1} = (n + 1)2^{n+1}$.

$$a_{n+1} = 4a_n - 4a_{n-1} = 4n2^n - 4(n - 1)2^{n-1} = 4 \cdot 2^{n-1}(n \cdot 2 - (n - 1)) =$$
$$2^2 \cdot 2^{n-1}(2n - n + 1) = 2^{n+1}(n + 1) = (n + 1)2^{n+1}.$$

8. Fundamentals of Modern Algebra

If A is a set, a function of two variables $* : A \times A \to A$ is said to be a **binary operation** on A and one writes $*(a, b)$ shorter as $a * b$.

Multiplication and addition on various number sets (natural numbers, integers, rationals, reals), addition of vectors in a vectors space, and multiplication of square matrices of the same size, are just some of the examples you may have already encountered. By considering an arbitrary set A and any binary (or n-ary) operation $*$ on A, one can study properties of this very general set up and then draw conclusions on properties of a variety of specific binary operation without necessarily studying each one of them. This idea of studying generalized operations instead of specific ones is the underlying idea of the area of mathematics know as **Abstract** or **Modern Algebra.** If you take the course bearing the same name, you will learn about **groups** which generalize a set with an associative operation with identity in which every element is invertible, **rings** which generalizes some common examples of sets with both addition and multiplication, and **fields** which generalize common examples of sets with + and commutative $\cdot$ in which every nonzero element has a multiplicative inverse.

A group

A ring

A field

Homomorphisms – operations on sets meet the functions. If A and B are two sets, each with a binary operation, one would prefer to consider functions $A \to B$ which are *compatible* with the two operations. This brings us to the concept of a *homomorphism.*

If $*$ is a binary operation on a set A and $\cdot$ is a binary operation on a set B, $f : A \to B$ is a **homomorphism** if it is compatible with the two binary operations that is if

$$f(a * b) = f(a) \cdot f(b)$$

for any $a, b \in A$. If such a homomorphism is a bijection, then it is said to be an **isomorphism**. In case when A and B are finite and we present operations on them by "multiplication" tables, then the table for A will match exactly the table for B if one lists the elements of $f(A)$ using the corresponding order of the elements of A. The first example below illustrates this.

The terms monomorphism and endomorphisms are used for injective and surjective homomorphisms respectively.

Example 6.

(1) If no operations on two sets A and B are considered, a homomorphism is any function $A \to B$ and an isomorphism is any bijection $A \to B$. Thus, if A and B have different cardinalities, then there is no bijection $A \to B$ so there is no isomorphism $A \to B$ regardless of a possible presence of any operations on the two sets.

(2) If two vector spaces V_1 and V_2 (say over real numbers) are considered together with addition, any linear transformation $T : V_1 \to V_2$ is a homomorphism (recall that the identity $T(v+w) = T(v)+T(w)$ for every $v, w \in V_1$ is a part of the definition of a linear transformation). Any linear transformation which is bijective is an isomorphism.

(3) Let $2\mathbb{Z}$ denote the set of even integers $\{\ldots,-4,-2,0,2,4,\ldots\}$. We can consider this set under addition coming from the addition in $\mathbb{Z}$. This makes the inclusion $i : 2\mathbb{Z} \to \mathbb{Z}$ (given by $2n \mapsto 2n$ for any $n \in \mathbb{Z}$) a homomorphism because

$$i(2m + 2n) = 2m + 2m = i(2m) + i(2n).$$

The inclusion i is clearly injective. This map is not onto (1, for example is not in the image of i), so this is an example of a homomorphism which is not an isomorphism.

(4) Let $\mathbb{Z}/\equiv$ denote the quotient set of $\mathbb{Z}$ with respect to the equivalence $\equiv$ from part (2) of Example 1. Recall that this set has two elements

$$\ldots = [-4] = [-2] = [0] = [2] = [4] = \ldots \text{ and } \ldots = [-3] = [-1] = [1] = [3] = [5] = \ldots.$$

Let us consider addition on this set governed by the rule that a sum of two even or two numbers is even and that the sum of an even and an odd number is odd. This corresponds to

$+$	$[0]$	$[1]$
$[0]$	$[0]$	$[1]$
$[1]$	$[1]$	$[0]$

. On the other hand, let $\mathbb{Z}_2$ denotes the set $\{0,1\}$ together with operation $+$ given by addition modulo 2. So, 1+1=2 is considered modulo 2 and, as 2 has remainder zero when divided by 2, we have that 1+1=0. Thus, the table is

$+$	0	1
0	0	1
1	1	0

. If f is a function $\mathbb{Z}/\equiv \to \mathbb{Z}_2$ given by $[0] \mapsto 0$ and $[1] \mapsto 1$, then f is an isomorphism: it is clearly bijective and if one compares the tables defining $+$, they match in the sense that the addition on $\mathbb{Z}_2$ is exactly given by

$+$	$f([0])$	$f([1])$
$f([0])$	$f([0])$	$f([1])$
$f([1])$	$f([1])$	$f([0])$

.

(5) Let R be the set containing the following two symmetry operations on the set of points in the xy-plane: the identity operation $\mathrm{id} : (x,y) \to (x,y)$ and the reflection r with respect to the y-axis $(x,y) \mapsto (-x,y)$. As $r \circ r = \mathrm{id}$, the multiplication table for R when this set is considered together with the composition $\circ$ is

$\circ$	id	r
id	id	r
r	r	id

. Comparing this table with the table of $\mathbb{Z}_2$, we conclude that $g : \mathbb{Z}_2 \to R$ given by $0 \mapsto \mathrm{id}$ and $1 \mapsto r$ is an isomorphism. This also implies that $g \circ f : \mathbb{Z}/\equiv \to R$ is also an isomorphism.

Congruences – operations meet the relations. If A is a set with an operation $*$ and an equivalence relation $\sim$, then $\sim$ is a **congruence** on A if it is compatible with the operation $*$ in the following sense.

$$a \sim c \text{ and } b \sim d \text{ implies that } a * b \sim c * d.$$

Example 7. (1) The identity relation is a congruence on any set A with any operation since $a = c$ and $b = d$ implies that $a * b = c * d$ because $*$ is a well-defined function of two variables.

(2) If $\equiv$ is the relation on $\mathbb{Z}$ from part (2) of Example 1 (and part (4) of Examples 6), then it is a congruence because

- If a, c are both even or both odd and b, d are both even or both odd, then $a + b$ and $c + d$ are also both even or both odd.
- If a, c are both even or both odd and one of b and d is even and another is odd, then one of $a + b$ and $c + d$ is even and another one is odd.

Similar arguments can be used in the remaining two cases.

(3) If $T : V_1 \to V_2$ is a linear transformation on two vector spaces (say over real numbers), then the relation on V_1 given by

$$v \sim_T w \text{ if } T(v - w) = 0$$

is a congruence: if $v \sim_T w$ and $v' \sim_T w'$, then $T(v - w) = 0$ and $T(v' - w') = 0$ so

$$T((v + v') - (w + w')) = T((v - w) + (v' - w')) = T(v - w) + T(v' - w') = 0 + 0 = 0$$

which shows that $v + v' \sim_T w + w'$.

The importance of congruences lies in the following: if $\sim$ is a congruence of a set A with operation $*$, then $*$ gives rise to a related operation on the quotient set $A/\sim$. This new operation, which we call also $*$, can be defined by

$$[a] * [b] = [a * b]$$

for any $a, b, c, d \in A$. The condition that $\sim$ is a congruence implies that this is a *well-defined* binary operation on $A/\sim$ meaning that if

$$[a] = [c] \text{ and } [b] = [d] \text{ then } [a] * [b] = [c] * [d].$$

This indeed holds since if $[a] = [c]$ and $[b] = [d]$, then $a \sim c$ and $b \sim d$, so the assumption that $\sim$ is a congruence implies that $a * b \sim c * d$ which implies that

$$[a * b] = [c * d] \text{ so that } [a] * [b] = [c] * [d].$$

For example, the addition of integers gives rise to the addition on the quotient set $\mathbb{Z}/\equiv$ formed with respect to the congruence $\equiv$ from part (2) of the previous example. This addition is exactly the addition given by

$+$	$[0]$	$[1]$
$[0]$	$[0]$	$[1]$
$[1]$	$[1]$	$[0]$

from Example 6.

Note that the congruence $\equiv$ produces a homomorphism $\pi : \mathbb{Z} \to \mathbb{Z}/\equiv$ given by $n \mapsto [n]$ for any $n \in \mathbb{Z}$. Thus, π maps an even number to [0] and an odd number to [1]. This is a homomorphism because $\equiv$ is a congruence so we have that $\pi(m + n) = [m + n] = [m] + [n] = \pi(m) + \pi(n)$. This homomorphism is surjective since both elements of $\mathbb{Z}/\equiv$ are in the images, [0] of 0 (or any other even number) and [1] of 1 (or any other odd number).

It turns out that *any* congruence on *any* set with an operation defines a homomorphism as π in the previous example. The following subsection shows this.

8.1. **Every congruence determines a surjective homomorphism.** If A is a set with an operation $*$ and a congruence $\sim$, let $\pi_\sim : A \to A/\sim$ be given by

$$\pi_\sim : a \mapsto [a].$$

This map is called the **canonical projection** or **natural map** of $\sim$. It is a homomorphism since

$$\pi_\sim(a * b) = [a * b] = [a] * [b] = \pi_\sim(a) * \pi_\sim(b)$$

and it is surjective since the preimage of any element $[a] \in A/\sim$ is $a \in A$.

The complete duality between homomorphisms and congruences is achieved by the following.

8.2. **Every homomorphism determines a congruence.** If A and B are sets with operations $*$ and $\cdot$ respectively, and if $f : A \to B$ is a homomorphism, the relation $\sim_f$ on A given by

$$a \sim_f b \text{ if } f(a) = f(b)$$

for any $a, b \in A$, is a congruence.

Let us show that $\sim_f$ is an equivalence first. It is reflexive since $f(a) = f(a)$, it is symmetric since $f(a) = f(b)$ implies that $f(b) = f(a)$, and it is transitive since $f(a) = f(b)$ and $f(b) = f(c)$ implies that $f(a) = f(c)$, for any $a, b, c \in A$.

To show that $\sim_f$ is a congruence, assume that $a \sim_f c$ and $b \sim_f d$. Then $f(a) = f(c)$ and $f(b) = f(d)$ and so

$$f(a * b) = f(a) \cdot f(b) = f(c) \cdot f(d) = f(c * d)$$

which implies that $a * b \sim_f c * d$.

For the set A with an operation $*$, if we consider both correspondences $F : \sim \mapsto \pi_\sim$ for a given congruence $\sim$ on A and $G : f \mapsto \sim_f$ for a given homomorphism f defined on A, then $G \circ F$ is the identity in the sense that

$$\sim_{\pi_\sim} = \sim \text{ for any } \sim.$$

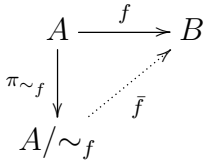
Indeed, given a congruence $\sim$, we have that

$$a \sim_{\pi_\sim} b \Leftrightarrow \pi_\sim(a) = \pi_\sim(b) \Leftrightarrow [a] = [b] \Leftrightarrow a \sim b$$

for any $a, b \in A$. This shows that the relation $\sim_{\pi_\sim}$ is the same relation as $\sim$.

The first practice problem below focuses on the composition $F \circ G$. Together with the above conclusion on $G \circ F$, this indicates a *duality between homomorphisms and congruences*. The course Abstract Algebra explores applications of this duality. One of them we encounter in this course during the formations of number sets in section 9.

Practice Problems 8. (1) Let A be a set with an operation $*$. For any set B with operation $\cdot$ and any homomorphism $f : A \to B$, there is a unique injective homomorphism $\bar{f}$ such that the diagram below **commutes** (meaning that $f = \bar{f} \circ \pi_{\sim_f}$). Here $\sim_f$ is the congruence from section 8.2 and $\pi_{\sim_f}$ is the natural map $A \to A/\sim_f$ from section 8.1.



If f is surjective, then $\bar{f}$ is also surjective, so it is an **isomorphism** of $A/\sim_f$ and B.

(2) Let $A, B, *, \cdot, f$, and $\sim_f$ be as in the previous problem. Show that f is injective if and only if $\sim_f = \{(a, a) : a \in A\}$.

(3) Consider the relation $\sim$ on $\mathbb{N} \times \mathbb{N}$ from part (4) Example 1. If $\mathbb{N} \times \mathbb{N}$ is considered with addition defined *by coordinates* as follows

$$(k, l) + (m, n) = (k + m, l + n),$$

show that $\sim$ is a congruence. Deduce that this enables us to define the addition on the quotient set $(\mathbb{N} \times \mathbb{N})/\sim$ by

$$[(k, l)] + [(m, n)] = [(k + m, l + n)].$$

Solutions. (1) The problem is asking us to show the following claims.

(a) Define a function $\bar{f}$ such that the following hold.

(b) $\bar{f}$ is a homomorphism.
(c) $\bar{f}$ is injective.
(d) The diagram commutes (i.e. $f = \bar{f} \circ \pi_{\sim_f}$).
(e) $\bar{f}$ is unique with the above properties.
(f) If f is onto, then $\bar{f}$ is onto.

Let us go over each of these steps.

(a) To define $\bar{f}$, first note what the other two maps in the diagram are. If $a \in A$, they map it to the elements as in the diagram below.

$$\begin{array}{ccc} a & \overset{f}{\longmapsto} & f(a) \\ {\scriptstyle \pi_{\sim_f}}\downarrow & & \\ [a] & & \end{array} \text{ . Thus define } \bar{f} \text{ as } \begin{array}{ccc} a & \overset{f}{\longmapsto} & f(a) \\ {\scriptstyle \pi_{\sim_f}}\downarrow & \nearrow_{\bar{f}} & \\ [a] & & \end{array} .$$

To make sure this indeed defines a function, one needs to check that if $[a] = [b]$ then $\bar{f}([a]) = \bar{f}([b])$ for any $a, b \in A$. Assume that $[a] = [b]$. Thus, $a \sim_f b$ so $f(a) = f(b)$. Hence, $\bar{f}([a]) = f(a) = f(b) = \bar{f}([b])$.

(b) To show that $\bar{f}$ is a homomorphism, let $a, b \in A$. As f is a homomorphism, we have that

$$\bar{f}([a] * [b]) = \bar{f}([a * b]) = f(a * b) = f(a) \cdot f(b) = \bar{f}([a]) \cdot \bar{f}(b).$$

(c) To show $\bar{f}$ is injective, assume that $\bar{f}([a]) = \bar{f}([b])$. Then $[a] = [b]$ since

$$\bar{f}([a]) = \bar{f}([b]) \Rightarrow f(a) = f(b) \Rightarrow a \sim_f b \Rightarrow [a] = [b].$$

(d) The diagram commutes since, for any $a \in A$, $(\bar{f} \circ \pi_{\sim_f})(a) = \bar{f}(\pi_{\sim_f}(a)) = \bar{f}([a]) = f(a)$.

(e) To show that $\bar{f}$ is unique, assume that g is another map $A/\sim_f \to B$ such that $f = g \circ \pi_{\sim_f}$ and let us show that $\bar{f} = g$. This holds since, for any $a \in A$,

$$\bar{f}([a]) = f(a) = (g \circ \pi_{\sim_f})(a) = g(\pi_{\sim_f}(a)) = g([a]).$$

(f) If f is surjective, let us show that $\bar{f}$ is surjective. This means that for any $b \in B$, we need to find $a \in A$ such that $\bar{f}([a]) = b$. As f is surjective, we can find $a \in A$ such that $f(a) = b$. Then we have that $\bar{f}([a]) = f(a) = b$.

(2) Recall that $\sim_f = \{(a, b) \in A \times A : f(a) = f(b)\}$. If f is injective, then $f(a) = f(b)$ implies that $a = b$ so we have that $\sim_f = \{(a, a) : a \in A\}$. Conversely, if $\sim_f = \{(a, a) : a \in A\}$, then no $b \neq a$ is such that $f(a) = f(b)$. Thus, $f(a) = f(b)$ implies that $a = b$ which shows that f is injective.

(3) In part (4) of Example 1, we showed that $\sim$ is an equivalence. To show it is a congruence, it remains to show that

$$(k, l) \sim (k', l') \text{ and } (m, n) \sim (m', n') \text{ implies that } (k + m, l + n) \sim (k' + m', l' + n').$$

This indeed holds since if the assumption of the above implication holds, then $k + l' = k' + l$ and $m + n' = m' + n$. Adding these two relations produces $k + l' + m + n' = k' + l + m' + n$ and so $(k + m) + (l' + n') = (k' + m') + (l + n)$ which implies that $(k + m, l + n) \sim (k' + m', l' + n')$.

As $\sim$ is a congruence, addition defined "by coordinates" is a well defined operation on the quotient set $(\mathbb{N} \times \mathbb{N})/\sim$ (see the paragraph following Example 7).

9. From natural to rational numbers

From natural numbers to integers. Recall that subtraction defined on the set of natural numbers $\mathbb{N}$ by

$$n - m = k \quad \text{if} \quad n = k + m$$

is only a partial operation (defined only for $n \geq m$). Thus, the equation $n = x + m$ is solvable for x only when $m \leq n$. One would aim to be able to solve *any* equation of the form $n = x + m$ for any two natural numbers n and m. Because of this, we *enlarge* the set of natural number to another number set, which is only as large as needed to guarantee that any equation of the above form has a solution in this set (i.e. that the operation $-$ defined as above is really an operation, not only a partial operation). While it is intuitively clear that such set should be obtained by adding the negative integers

$$-1, -2, -3 \ldots$$

to the set $\mathbb{N}$, we would like to be very specific about the nature of these added elements (what exactly one such new element "$-n$" is). Because of this, we introduce an equivalence relation on the set $\mathbb{N} \times \mathbb{N}$ and obtain the set of integers as the quotient set of this relation. So, let us consider a relation $\sim$ defined on $\mathbb{N} \times \mathbb{N}$ by

$$(k, l) \sim (m, n) \quad \text{if} \quad k + n = m + l.$$

Recall that we have shown that this is an equivalence relation in part (4) of Example 1. This means that we can consider *quotient set* $\mathbb{N} \times \mathbb{N}/\sim$. For a natural number n, we would like to define n, considered as an integer now, as the equivalence class of $(n, 0)$ and we would like to define

$$\text{the negative integer } -n \text{ as the equivalence class of } (0, n).$$

Using this approach, if $(k, l) \sim (0, n)$, then $k + n = l$, and so the difference of k and l is indeed the same as the difference of 0 and n and both of those differences correspond to the intuitive understanding of $-n$.

More generally, if $(k, l) \sim (m, n)$, then $k + n = m + l$ and so the difference $k - l$ matches the difference $m - n$ and both correspond to the same equivalence class $[(k, l)] = [(m, n)]$.

We denote the quotient set $(\mathbb{N} \times \mathbb{N})/\sim$ by $\mathbb{Z}$. There is a natural injection $\iota : \mathbb{N} \to \mathbb{Z}$ given by

$$n \mapsto [(n, 0)].$$

This map is indeed injective since if $[(n, 0)] = [(m, 0)]$, then $(n, 0) \sim (m, 0)$ and this implies that $n + 0 = m + 0$ so $n = m$.

The existence of the injection ι let us abbreviate $[(n, 0)]$ as n. Thus, if we denote

$$\text{the equivalence class of } (n, 0) \text{ by } n \text{ and}$$

$$\text{the equivalence class of } (0, n) \text{ by } -n$$

for any $n \in \mathbb{N}$. With this convention, we have that $0 = -0$ because both 0 and -0 correspond to the class of $(0, 0)$.

The identification of $\iota(n) = [(n, 0)]$ and n for $n \in \mathbb{N}$ enables us to consider $\mathbb{N}$ as a **subset** of $\mathbb{Z}$. So, we can think of $\mathbb{Z}$ as the set consisting of

$$\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots$$

and we have that

$$\begin{array}{rl}
 & \vdots \\
-2 = & [(0,2)] = [(1,3)] = [(2,4)] = \ldots = [(n, n+2)] = \ldots \\
-1 = & [(0,1)] = [(1,2)] = [(2,3)] = \ldots = [(n, n+1)] = \ldots \\
0 = & [(0,0)] = [(1,1)] = [(2,2)] = \ldots = [(n, \ \ n \ \ )] \ \ = \ldots \\
1 = & [(1,0)] = [(2,1)] = [(3,2)] = \ldots = [(n+1, n)] = \ldots \\
2 = & [(2,0)] = [(3,1)] = [(4,2)] = \ldots = [(n+2, n)] = \ldots \\
 & \vdots
\end{array}$$

The elements $1, 2, \ldots$ are **positive integers** and the elements $-1, -2, \ldots$ are **negative integers.** Note that if an integer n is $[(k, l)]$ for some natural numbers k and l, then $-n$ is $[(l, k)]$. So, we can write

$$-[(k, l)] = [(l, k)].$$

Addition, multiplication and the usual order. Next, we define the addition, multiplication and the usual order of integers. **The addition** is defined as in Practice Problem (3) of section 8: *"by coordinates"* as follows.

$$[(k, l)] + [(m, n)] = [(k, l) + (m, n)] = [(k + m, l + n)]$$

One can check that addition satisfies the familiar properties below.

Exercise 31. Show that the following properties hold.

(1) The element 0 is *neutral* for addition: for any integer n,
$$n + 0 = 0 + n = n.$$
(2) For any integer n, $-n$ is *the inverse* of n.
$$n + (-n) = (-n) + n = 0$$

Solution. (1) Let $n = [(k, l)]$ for some natural numbers k and l. We have that
$$[(k, l)] + [(0, 0)] = [(k + 0, l + 0)] = [(k, l)]$$
and the relation $0 + n = n$ is shown similarly.

(2) Recall that if an integer n is $[(k, l)]$ for some natural numbers k and l, then $-n$ is $[(l, k)]$. Thus, showing $n + (-n) = 0$ translates into checking that
$$[(k, l)] + [(l, k)] = [(k + l, l + k)] = [(k + l, k + l)] = [(0, 0)].$$
The relation $(-n) + n = 0$ can be shown similarly.

Other familiar properties hold as, for example,

Associativity. $(k + m) + n = k + (m + n)$ for any integers k, m, and n.
Commutativity. $n + m = m + n$ for any integers m and n.

When defining multiplication, the goal we would like to achieve is that the classes $[(k, l)]$ and $[(m, n)]$, which represent $k-l$ and $m-n$ should multiply to $(k-l)(m-n) = km-lm-kn+ln = (km + ln) - (lm + kn)$. Hence, we define the **multiplication** by

$$[(k, l)] \cdot [(m, n)] = [(km + ln, lm + kn)]$$

Exercise 32. Show that the following properties hold.

(1) The element 1 is *neutral* for multiplication: for any integer n,

$$n \cdot 1 = 1 \cdot n = n.$$

(2) $\mathbb{Z}$ has no *zero divisors*: for any integers n an m, if $m \cdot n = 0$ then $m = 0$ or $n = 0$.

Solution. (1) Let $n = [(k, l)]$ for some natural numbers k and l. So, showing $n \cdot 1 = n$ translates to showing that

$$n \cdot 1 = [(k, l)] \cdot [(1, 0)] = [(k \cdot 1 + l \cdot 0, l \cdot 1 + k \cdot 0)] = [(k, l)] = n.$$

The equation $1 \cdot n = n$ can be shown analogously.

(2) We can consider the cases when both n and m are natural numbers, when one is a natural number and the other a negative integer and when both are negative integers. All these cases are similar so we list details for the proof of only one of them. For example, let n, m be natural numbers and assume that $m \cdot n = 0$ which means that $[(m, 0)] \cdot [(n, 0)] = [(0, 0)]$ so that $[(m \cdot n + 0 \cdot 0, m \cdot 0 + 0 \cdot n)] = [(mn, 0)] = [(0, 0)]$. This implies that $(mn, 0) \sim (0, 0)$ so that $mn + 0 = 0 + 0$ and so $mn = 0$. As the product of natural numbers is such that mn is zero only if m is zero or n is zero, this implies that $m = 0$ or $n = 0$ which implies that $[(m, 0)] = [(0, 0)]$ or $[(n, 0)] = [(0, 0)]$.

Other familiar properties can be shown to hold as, for example,

Associativity. $(k \cdot m) \cdot n = k \cdot (m \cdot n)$ for any integers k, m, and n.
Commutativity. $n \cdot m = m \cdot n$ for any integers m and n.
Distributivity. $k \cdot (m + n) = (k \cdot m) + (k \cdot n)$ and $(m + n) \cdot k = (m \cdot k) + (n \cdot k)$ for any integers k, m, and n.

Just as for natural numbers, we suppress writing $\cdot$ often so we shorten

$$m \cdot n \text{ to } mn \quad \text{for } m, n \in \mathbb{Z}.$$

Next, we aim to define the familiar **order** $\ldots < -1 < 0 < 1 < 2 < \ldots$. We would like to have that the classes $[(k, l)]$ and $[(m, n)]$, which represent $k - l$ and $m - n$, are in relation $[(k, l)] \leq [(m, n)]$ if $[(m, n)] - [(k, l)] = [(m, n)] + [(l, k)] = [(m + l, n + k)]$ corresponds to a nonnegative integer. Recall that this means that the first coordinate $m + l$ is larger or equal to the second $n + k$. So, we define $\leq$ by

$$[(k, l)] \leq [(m, n)] \quad \text{if} \quad k + n \leq l + m.$$

The strict order can be defined from $\leq$ as usually

$$[(k, l)] < [(m, n)] \quad \text{if} \quad [(k, l)] \leq [(m, n)] \text{ and } [(k, l)] \neq [(m, n)].$$

One can directly show that $\leq$ is a partial order. In addition, we have that $n < n + 1$ because, if n is a nonnegative integer, then $[(n, 0)] < [(n + 1, 0)]$ since $n + 0 = n < n + 1 = n + 1 + 0$.

One can show that some familiar properties of $<$, as those listed below, hold.

Compatibility of $<$ with addition. If $k < m$ and $l < n$, then $k + l < m + n$ for any integers k, l, m, and n.
Compatibility of $<$ with multiplication. If $k < m$ and $0 < l < n$, then $k \cdot l < m \cdot n$ for any integers k, l, m, and n.

The cardinality of integers. Although $\mathbb{N}$ is a strict subset of $\mathbb{Z}$ and $\mathbb{Z}$ seems to have "twice as many" elements as $\mathbb{N}$, the cardinality of $\mathbb{N}$ and $\mathbb{Z}$ is the same because the map given by

$$n \mapsto 2n \text{ for } n \in \mathbb{N} \text{ and}$$

$$-n \mapsto 2n-1 \text{ for } n \in \mathbb{N} - \{0\}$$

is a bijection $\mathbb{Z} \to \mathbb{N}$. This shows that the cardinality of $\mathbb{Z}$ is the same as that of $\mathbb{N}$ which is $\aleph_0$. So, $\mathbb{Z}$ is *countable*. Alternatively, one can argue that the inclusion $\mathbb{N} \subseteq \mathbb{Z}$ implies that

$$|\mathbb{Z}| \geq |\omega|.$$

The converse holds by using Claim 2 to conclude that $\mathbb{N} \times \mathbb{N}$ is countable so that

$$|\mathbb{Z}| = |(\mathbb{N} \times \mathbb{N})/\!\sim| \leq |\mathbb{N} \times \mathbb{N}| = |\omega|.$$

From integers to rationals. By enlarging $\mathbb{N}$ to $\mathbb{Z}$, we ensured that subtraction is an operation, not only a partial operation. Thus, every equation of the form $n + x = m$ has a solution for x for any two integers m and n. We enlarge the set of integers to have that the division is a full, not a partial, operation and that every equation of the form

$$nx = m$$

has a solution for any two integers $n \neq 0$ and m (note that for $n = 0$ the equation has no solutions if $m \neq 0$ and infinitely many solutions if $m = 0$). So, we would like to obtain the set of rational numbers $\mathbb{Q}$ by enlarging the integers by the set containing fractions of the form

$$\frac{m}{n}$$

where $m, n \in \mathbb{Z}$ and $n \neq 0$. This can be obtained by considering a suitable equivalence relation, just as when forming $\mathbb{Z}$ from $\mathbb{N}$. The definition of the equivalence relation comes from the requirement that two fractions $\frac{k}{l}$ and $\frac{m}{n}$ are equal, $\frac{k}{l} = \frac{m}{n}$ if the cross multiplication produces $kn = ml$. Thus, we introduce an equivalence relation $\sim$ on the set $\mathbb{Z} \times (\mathbb{Z} - \{0\})$ by

$$(k, l) \sim (m, n) \quad \text{if} \quad kn = ml.$$

One can directly show that this is an equivalence relation. So, we can introduce the set $\mathbb{Q}$ as the *quotient set* $\mathbb{Z} \times (\mathbb{Z} - \{0\})/\!\sim$ and shorten the notation

$$[(m, n)] \quad \text{to} \quad \frac{m}{n}.$$

We have that

$$[(m, n)] = [(mk, nk)]$$

for any nonzero integer k (since $mnk = nmk$ so $(m, n) \sim (mk, nk)$).

If we identify the class $[(m, 1)] = \frac{m}{1}$ with the integer m, we can consider $\mathbb{Z}$ as a subset of $\mathbb{Q}$.

Operations and order of rationals. We define the addition, multiplication, and the usual order of rationals. The **addition** is defined by aiming to add two fractions by finding their common denominator and then proceeding in the usual way to have that

$$\frac{k}{l}+\frac{m}{n}=\frac{kn}{ln}+\frac{ml}{ln}=\frac{kn+ml}{ln}.$$

Thus, we define the addition as follows.

$$[(k,l)]+[(m,n)]=[(kn+ml,\ ln)]$$

The element $0=\frac{0}{1}=[(0,1)]=[(0,k)]$, for any nonzero integer k, has a special significance for addition since it is the *neutral element* for the addition:

$$[(k,l)]+[(0,m)]=[(km+l\cdot 0,\ ml)]=[(km,ml)]=[(k,l)].$$

The element $-[(m,n)]$ stands for the additive *inverse* of $[(m,n)]$ and it is $[(-m,n)]$ since $[(m,n)]+[(-m,n)]=[(0,n^2)]=0$.

The **multiplication** is defined by aiming to have $\frac{k}{l}\cdot\frac{m}{n}=\frac{km}{ln}$, so we define it by

$$[(k,l)]\cdot[(m,n)]=[(km,ln)].$$

The element $1=\frac{1}{1}=\frac{n}{n}$, for any nonzero integer n, has a special significance for multiplication since $[(k,l)]\cdot[(1,1)]=[(k,l)]$ so 1 is the *neutral element* for multiplication. One of the practice problems focuses on showing that if $a=[(m,n)]\neq 0$, then the multiplicative *inverse* $\frac{1}{a}$ of a is $[(n,m)]$.

Note that the property $[(m,n)]=[(mk,nk)]$ for any nonzero integer k enables us to represent a rational number $a=[(m,n)]$ using a pair with *positive* integer as the second coordinate. Indeed, if $n>0$ this is already the case. If $n<0$, take $k=-1$ and write a as $[(-m,-n)]$. As $n<0$, we have that $-n>0$.

The **order** $\leq$ is defined by requiring that $\frac{k}{l}\leq\frac{m}{n}$ for two rational numbers with l and n positive, if $\frac{m}{n}-\frac{k}{l}\geq 0$ that is if $\frac{ml-nk}{nl}\geq 0$. As we assumed that l and n are positive, the product nl is positive so this happens exactly when $ml-nk\geq 0$, equivalently $nk\leq ml$. Thus we define the order by

$$[(k,l)]\leq[(m,n)]\quad\text{if}\quad kn\leq lm$$

for any integers k and m and any positive integers l and n. The strict order can be defined from $\leq$ as usually: $a<b$ if $a\leq b$ and $a\neq b$ for any $a,b\in\mathbb{Q}$.

One can check that these operations and relation satisfy the familiar properties.

0 is the neutral element for addition. For any rational number a,

$$a+0=0+a=a.$$

$-a$ is the additive inverse of a. For any rational number a,

$$a+(-a)=(-a)+a=0.$$

Associativity of addition. $(a+b)+c=a+(b+c)$ for any $a,b,c\in\mathbb{Q}$.
Commutativity of addition. $a+b=b+a$ for any $a,b\in\mathbb{Q}$.
1 is the neutral element for multiplication. $a\cdot 1=1\cdot a=a$ for any $a\in\mathbb{Q}$.
$\frac{1}{a}$ is the multiplicative inverse of $a\neq 0$. $a\cdot\frac{1}{a}=\frac{1}{a}\cdot a=1$ for any $a\in\mathbb{Q}-\{0\}$
No zero divisors. For any $a,b\in\mathbb{Q}$, if $a\cdot b=0$ then $a=0$ or $b=0$.
Associativity of multiplication. $(ab)c=a(bc)$ for any $a,b,c\in\mathbb{Q}$.
Commutativity of multiplication. $ab=ba$ for any $a,b\in\mathbb{Q}$.
Distributivity. $a(b+c)=ab+ac$ and $(b+c)a=ba+ca$ for any $a,b,c\in\mathbb{Q}$.

Compatibility of $<$ with addition. If $a < c$ and $b < d$, then $a + b < c + d$ for any $a, b, c, d \in \mathbb{Q}$.

Compatibility of $<$ with multiplication. If $a < c$ and $0 < b < d$, then $ab < cd$ for any $a, b, c, d \in \mathbb{Q}$.

Cardinality of the rationals. As $\mathbb{Q}$ contains $\mathbb{Z}$, we have that the cardinality of $\mathbb{Q}$ is larger than or equal to the cardinality of $\mathbb{Z}$ which is $|\omega|$. On the other hand, since the natural map $\mathbb{Z} \times (\mathbb{Z} - \{0\}) \to \mathbb{Q}$ is onto, we have that the cardinality of $\mathbb{Q}$ is smaller than or equal to the cardinality of $\mathbb{Z} \times (\mathbb{Z} - \{0\})$. As $\mathbb{Z} - \{0\}$ has the same cardinality as $\mathbb{Z}$ (the map given by $n \mapsto n - 1$ if $n > 0$ and $n \mapsto n$ if $n < 0$ is a bijection $\mathbb{Z} - \{0\} \to \mathbb{Z}$), we have that

$$|\omega| = |\mathbb{Z}| \leq |\mathbb{Q}| \leq |\mathbb{Z} \times (\mathbb{Z} - \{0\})| = |\omega \times \omega| = |\omega|$$

where the second equality holds by Practice Problem (1b) and Claim 2 from section 6 and the last equality by Claim 2. The relations $|\omega| \leq |\mathbb{Q}| \leq |\omega|$ imply that

$$|\mathbb{Q}| = |\omega|$$

so $\mathbb{Q}$ is *countable.*

Practice Problems 9. (1) Show that

$$[(n, m)] = [(0, m - n)] \text{ if } m \geq n \quad \text{and} \quad [(n, m)] = [(n - m, 0)] \text{ if } m < n$$

for any natural numbers m and n.

(2) Find the sum and the product of the integers $[(5, 3)]$ and $[(2, 6)]$.

(3) The relation $\leq$ on $\mathbb{Z}$ matches the familiar order of integers when $[(m, n)]$ is shortened to $m - n$ (note that the favorable properties of the operations enable us to do this). Using this representation, rearrange the integer numbers below, if needed, so that the elements in the new list are non-decreasing.

$$[(6, 3)], \quad [(1000, 1005)], \quad [(6, 8)], \quad [(57, 56)], \quad [(56, 58)]$$

(4) Show that $[(n, m)]$ is the multiplicative inverse of any $[(m, n)] \in \mathbb{Q}$ such that $m \neq 0$.

(5) Find the sum and the product of the rational numbers $[(5, 3)]$ and $[(2, 6)]$.

(6) The relation $\leq$ on $\mathbb{Q}$ matches the familiar order of integers when $[(m, n)]$ is shortened to $\frac{m}{n}$ (note that the favorable properties of the operations enable us to do this). Using this representation, rearrange the rational numbers below, if needed, so that the elements in the new list are non-decreasing.

$$[(5, 15)], \quad [(50, -100)], \quad [(15, 10)], \quad [(20, -10)], \quad [(-10, 20)]$$

(7) Show that $\mathbb{Q}$ has no zero divisors, that is $ab = 0 \Rightarrow a = 0$ or $b = 0$ for any $a, b \in \mathbb{Q}$.

(8) If a, b, c are rational numbers such that $a < b$ and $c > 0$, show that $ac < bc$.

Solutions. (1) Let us consider the case $m \geq n$ first. In this case, $m - n$ is a natural number and the relation $[(n, m)] = [(0, m - n)]$ is equivalent with $(n, m) \sim (0, m - n)$ and this last relation is, by definition of $\sim$ equivalent with $n + m - n = m + 0$. This last relation is true since both $m + 0$ and $n + m - n$ are equal to m.

Let us consider the case $m < n$ now. In this case $n - m$ is a natural number and the relation $[(n, m)] = [(n - m, 0)]$ is equivalent with $(n, m) \sim (n - m, 0)$. This last relation is equivalent with $n + 0 = m + n - m$ by the definition of $\sim$. The relation $n + 0 = m + n - m$ is true since both sides are equal to n.

(2) By the definition of the addition of integers, $[(5,3)]+[(2,6)]=[(5+2,3+6)]=[(7,9)]$. Alternatively, if we note that $[(5,3)]$ stands for $5-3=2$ and $[(2,6)]$ for $2-6=-4$, we can use the familiar addition and say that $2+(-4)=-2$. Representing $[(7,9)]$ as $7-9=-2$, we obtain the same answer.

By the definition of the multiplication of integers, $[(5,3)]\cdot[(2,6)]=[(5\cdot 2+3\cdot 6, 5\cdot 6+3\cdot 2)]=[(28,36)]$. Alternatively, if we note that $[(5,3)]$ stands for $5-3=2$ and $[(2,6)]$ for $2-6=-4$, we can use the familiar multiplication and say that $2\cdot(-4)=-8$. Representing $[(28,36)]$ as $28-36=-8$, we obtain the same answer.

(3) $[(6,3)]$ can be shortened to $6-3=3$, $[(1000,1005)]$ to $1000-1005=-5$, $[(6,8)]$ to $6-8=-2$, $[(57,56)]$ to $57-56=1$, and $[(56,58)]$ to $56-58=-2$. As $-5<-2=-2<1<3$, we have that

$$[(1000,1005)]<[(6,8)]=[(56,58)]<[(57,56)]<[(6,3)].$$

(4) Recall that 1 stands for $[(1,1)]$ and that 1 is neutral for multiplication in $\mathbb{Q}$. For $[(m,n)]\in\mathbb{Q}$ such that $m\neq 0$, the ordered pair (n,m) is an element of $\mathbb{Z}\times\mathbb{Z}-\{0\}$, so $[(n,m)]$ is in $\mathbb{Q}$.

We show that it is the multiplicative inverse of $[(m,n)]$. Indeed, $[(m,n)]\cdot[(n,m)]=[(mn,nm)]=[(mn,mn)]=[(1,1)]$. Similarly, $[(n,m)]\cdot[(m,n)]=[(nm,mn)]=[(nm,nm)]=[(1,1)]$.

(5) By the definition of the addition of rationals, $[(5,3)]+[(2,6)]=[(5\cdot 6+2\cdot 3,3\cdot 6)]=[(36,18)]$. Alternatively, if we note that $[(5,3)]$ stands for $\frac{5}{3}$ and $[(2,6)]$ for $\frac{2}{6}=\frac{1}{3}$, we can use the familiar addition and say that $\frac{5}{3}+\frac{1}{3}=\frac{6}{3}=2$. Representing $[(36,18)]$ as $\frac{36}{18}=2$, we obtain the same answer.

By the definition of the multiplication of integers, $[(5,3)]\cdot[(2,6)]=[(5\cdot 2,3\cdot 6)]=[(10,18)]$. Alternatively, if we note that $[(5,3)]$ stands for $\frac{5}{3}$ and $[(2,6)]$ for $\frac{2}{6}=\frac{1}{3}$, we can use the familiar multiplication and say that $\frac{5}{3}\cdot\frac{1}{3}=\frac{5}{9}$. Representing $[(10,18)]$ as $\frac{10}{18}=\frac{5}{9}$, we obtain the same answer.

(6) $[(5,15)]$ can be shortened to $\frac{5}{15}=\frac{1}{3}$, $[(50,-100)]$ to $\frac{50}{-100}=\frac{-1}{2}$, $[(15,10)]$ to $\frac{15}{10}=\frac{3}{2}$, $[(20,-10)]$ to $\frac{20}{-10}=-2$, and $[(-10,20)]$ to $\frac{-10}{20}=\frac{-1}{2}$. As $-2<\frac{-1}{2}=\frac{-1}{2}<\frac{1}{3}<\frac{3}{2}$, we have that

$$[(20,-10)]<[(50,-100)]=[(-10,20)]<[(5,15)]<[(15,10)].$$

(7) Let $a=[(m,n)]$ and $b=[(k,l)]$ and assume that $ab=0$ so that $[(mk,nl)]=[(0,1)]$. This implies that $mk\cdot 1=nl\cdot 0$ so that $mk=0$. As $\mathbb{Z}$ has no zero divisors (see part (2) of Exercise 32), this implies that $m=0$ or $k=0$. If $m=0$, then $a=[(0,n)]=[(0,1)]=0$. If $k=0$, then $b=[(0,l)]=[(0,1)]=0$.

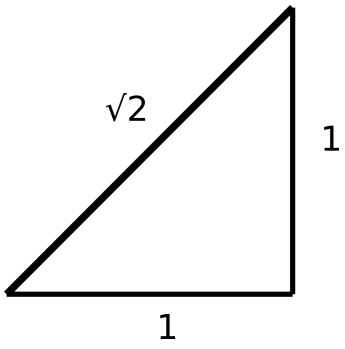
(8) Let $a=[(k,l)], b=[(m,n)]$, and $c=[(p,q)]$ where l,n and q are *positive* integers (see the paragraph before the introduction of the relation $\leq$ on $\mathbb{Q}$). The condition $c=[(p,q)]>0=[(0,1)]$ implies that $p\cdot 1>q\cdot 0$, so $p>0$. The assumption $a=[(k,l)]<b=[(m,n)]$ implies that $kn<lm$. As $<$ is compatible with multiplication by a positive integers and both p and q are positive, we have that $knpq<lmpq$. This ensures that $ac=[(kp,lq)]<bc=[(mp,nq)]$ since this is equivalent with $kpnq<lqmp$.

10. Fundamentals of Real Analysis – real numbers

From rationals to reals. Now that we ensured that both equations $a + x = b$ and $ax = b$ have solutions in the set of rationals for any two rational numbers a ($a \neq 0$ for the second equation) and b, we are exploring the type of polynomial equations with rational coefficients which do not have solutions in the set of rational numbers and we aim to further expand $\mathbb{Q}$ to a larger set of numbers.

The existence of such equations has been known already in Ancient Greece (circa 500 BC) and in India (circa 800 BC).

One of the first irrational numbers to be considered was $\sqrt{2}$. Today many algebraic and geometrical proofs of the fact that $\sqrt{2}$ is not rational are known. We consider one of them.



Claim 4. *The positive solution of the equation $x^2 = 2$ is not a rational number.*

Note that the figure above guarantees the existence of such positive solution: if x denotes the length of the hypotenuse, we have that $x^2 = 1^2 + 1^2$ by Pythagoras's Theorem. Thus, $x^2 = 2$ so there is a physical length corresponding to a positive number x which is a solution of $x^2 = 2$.

Proof. Assume that $\sqrt{2}$ is equal to a rational number $\frac{m}{n}$. We can assume that m and n do not have any common factors except 1 because if $m = m_1 k$ and $n = n_1 k$ for some integers m_1, n_1, and k, then $\frac{m}{n} = \frac{m_1}{n_1}$. Continuing this process of canceling common factors, we eventually arrive to a rational number which has the numerator and denominator without any common factors except 1.

If $\sqrt{2} = \frac{m}{n}$, then $2 = \frac{m^2}{n^2}$ and so

$$2n^2 = m^2.$$

This implies that m^2 is an even number and so m is also an even number (the square of an odd number is also odd). Thus, $m = 2k$ for some k and we have that $2n^2 = 4k^2$ which implies that

$$n^2 = 2k^2.$$

So, n^2 is also even and then n is even too. Thus, $n = 2l$ for some l. But this implies that $m = 2k$ and $n = 2l$ have a common factor 2. This contradicts our assumption that m and n do not have any common factors except 1. Hence, our assumption that $\sqrt{2}$ is rational cannot be correct. □

Now that we know that there are numbers outside of $\mathbb{Q}$, we are to specify how exactly to enlarge $\mathbb{Q}$, how to define addition, multiplication and order on this enlarged set, and how to determine its cardinality.

The outcome of such enlargement of $\mathbb{Q}$ is the set of real numbers. Real numbers can be introduced on several different ways. Three most standard ways are

(1) by listing a set of axioms,
(2) by considering Dedekind cuts, or
(3) by considering Cauchy sequences.

The first approach would require familiarity with the concept of a *field* which is not covered before the Modern Algebra course. The second approach does not require any prerequisites, but we opt for the third approach because some familiarity with Cauchy sequences may be beneficent in Real Analysis.

Cauchy sequences. Recall that a sequence is a list of numbers indexed by natural numbers. We consider sequences of rational numbers

$$a_0, a_1, \ldots, a_n, \ldots$$

Intuitively, a Cauchy sequence is a sequence such that any two sufficiently large terms are very close to each other. More formally, no matter what small (rational) distance ε we chose to consider, we can find two terms, indexed by sufficiently large natural numbers such that the distance between them is smaller than ε. As the distance between a_n and a_m is $|a_n - a_m|$, and as "sufficiently large" is ensured that m and n are larger than some natural number n_0, this requirement can be written using a formula of predicate logic as

$$(\forall \varepsilon > 0)(\exists n_0 \in \mathbb{N})(\forall n, m > n_0)\ |a_n - a_m| < \varepsilon$$

in which $\varepsilon \in \mathbb{Q}$ and $n, m \in \mathbb{N}$.

It turns out that every such Cauchy sequence has a limit and, conversely, every convergent sequence is Cauchy (Real Analysis covers this equivalence). Because of this equivalence one may wonder about the reason we would want to consider Cauchy sequences when we can consider sequences with a limit instead. The main reason is that, as a Cauchy sequence is convergent, we can refer to its limit *without knowing what it is*.

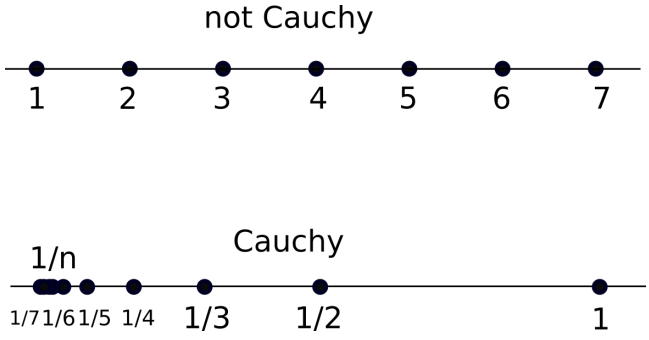
Let us consider the following examples.

Exercise 33. (1) Show that the sequence given by $a_n = n$ for $n \in \mathbb{N}$ is not Cauchy.
(2) Show that the sequence given by $a_n = \frac{1}{n}$ for $n \in \mathbb{N} - \{0\}$ is Cauchy.

Solution. (1) If $a_n = n$ for $n \in \mathbb{N}$, the terms of this sequence are 0,1,2,... The limit of this sequence is infinity, so this sequence is not convergent. To show it is not Cauchy, note that the distance between two consecutive terms is 1. So, if we take ε to be 1, for any n_0 and for any $n > n_0$ $|a_n - a_{n+1}| = |n - (n+1)| = 1$ which is not smaller than $\varepsilon = 1$. This shows that the negation of the above formula holds

$$(\exists \varepsilon > 0)(\forall n_0 \in \mathbb{N})(\exists n, m > n_0)\ |a_n - a_m| \geq \varepsilon$$

so this sequence is not Cauchy.



(2) Let us consider the sequence $a_n = \frac{1}{n}$ for $n \in \mathbb{N} - \{0\}$. Note that the terms of this sequence converge to 0. Let us show this sequence is Cauchy. Let $\varepsilon > 0$ be arbitrary. To find n_0, consider the formula $|\frac{1}{m} - \frac{1}{n}|$ which we need to relate to ε so that we can find n_0 somehow. As $|a + b| \leq |a| + |b|$ for any a and b, we have that

$$\left|\frac{1}{m}-\frac{1}{n}\right| \leq \left|\frac{1}{m}\right| + \left|-\frac{1}{n}\right| = \frac{1}{m}+\frac{1}{n}.$$

As $n \leq m$ or $m \leq n$, we can consider the last expression in either case. So, if $n \leq m$, then $\frac{1}{m} \leq \frac{1}{n}$ and $\frac{1}{m}+\frac{1}{n} \leq \frac{1}{n}+\frac{1}{n} = \frac{2}{n}$. So, if $\frac{2}{n} < \varepsilon$, we have that $\frac{n}{2} > \frac{1}{\varepsilon} \Rightarrow n > \frac{2}{\varepsilon}$. Similarly, the case $m \leq n$ produces $m > \frac{2}{\varepsilon}$. Hence, if n_0 is any natural number larger than $\frac{2}{\varepsilon}$ (Lemma 8 has more details on why such n_0 exits) then we have that for any $n, m < n_0$

$$\left|\frac{1}{m}-\frac{1}{n}\right| \leq \left|\frac{1}{m}\right| + \left|-\frac{1}{n}\right| = \frac{1}{m}+\frac{1}{n} < \frac{1}{n_0}+\frac{1}{n_0} = \frac{2}{n_0} < \varepsilon.$$

The next example shows that the limit of a Cauchy sequence of rational numbers can be a number which is not rational.

Example 8. Let a_n be a sequence given recursively by

$$a_{n+1} = \frac{a_n}{2} + \frac{1}{a_n}$$

and $a_0 = 1$. The first few terms of this sequence are

$$a_0 = 1, \quad a_1 = \frac{1}{2}+\frac{1}{1} = \frac{3}{2} = 1.5, \quad a_2 = \frac{3}{4}+\frac{2}{3} = \frac{17}{12} \approx 1.417, \quad a_3 = \frac{17}{24}+\frac{12}{17} = \frac{577}{408} \approx 1.414, \quad \ldots$$

and all the terms of this sequence are positive rational numbers. A quick induction proves it: $a_0 = 1$ is a positive rational number and assuming that a_n is positive and rational, its half is a rational number and its reciprocal is a rational number, so the sum $\frac{a_n}{2} + \frac{1}{a_n} = a_{n+1}$ is a positive rational number.

By taking the limit when $n \to \infty$ of both sides of the equation defining a_{n+1} and denoting the unknown limit of a_n by a, we have that

$$\lim_{n\to\infty} a_{n+1} = \frac{\lim_{n\to\infty} a_n}{2} + \frac{1}{\lim_{n\to\infty} a_n} \quad \Rightarrow \quad a = \frac{a}{2}+\frac{1}{a}$$

By multiplying both sides by $2a$ to get rid of denominators, we obtain

$$2a^2 = a^2 + 2 \quad \Rightarrow \quad a^2 = 2 \quad \Rightarrow \quad a = \pm\sqrt{2}.$$

As all the terms of the sequence are positive, its limit cannot be a negative number and so

$$a = \sqrt{2}.$$

Thus, a Cauchy sequence consisting of rational numbers can have a limit which is not rational.

The limit of a recursive sequence. The process of finding the limit in the above example generalizes to any recursive sequence given by a **recursive formula** of the form

$$a_{n+1} = f(a_n)$$

where f is a continuous function and a_0 the initial term of the sequence. The limit of the sequence, if it exists, is its *fixed point* – a number a such that $a = f(a)$. This is because we have that $\lim_{n\to\infty} a_n$ is a in this case, so that $\lim_{n\to\infty} a_{n+1}$ is also a.

Formation of the reals via Cauchy sequences. The underlying idea of the construction is that we **complete** the set of rational numbers by including all the limits of Cauchy sequences.

Two different Cauchy sequences can have the same limit. For example, the constant sequence $b_n = 0$ for any n has limit zero which is the same limit as of the sequence $a_n = \frac{1}{n}$ considered above. Because of this, we would like to *identify* two Cauchy sequences having the same limit. As before, this is done by an equivalence relation.

Let R be the set of all Cauchy sequences of rational numbers. We write (a_n) for a sequence whose n-th term is a_n. Let $\sim$ be a relation on R given by

$$(a_n) \sim (b_n) \text{ if } (a_n - b_n) \text{ has limit zero.}$$

This relation is reflexive since for every $(a_n) \in R$, the sequence with the n-th term $a_n - a_n = 0$ converges to 0. The relation is symmetric since if the limit of $a_n - b_n$ is zero, then the limit of $b_n - a_n$ is also zero. If $a_n - b_n$ and $b_n - c_n$ converge to zero, then their sum $a_n - n_n + b_n - c_n = a_n - c_n$ converges to zero also. So, $\sim$ is transitive.

We define addition on R by

$$(a_n) + (b_n) = (a_n + b_n)$$

that is: the sum of two Cauchy sequences is the sequence whose n-th term is the sum of the two n-th terms. The sequence defined in this way can be shown to be Cauchy directly (see Practice Problem (2) below). Alternative argument (but one requiring the Real Analysis statement that a sequence is Cauchy if and only if it is convergent) is that if the limit of (a_n) is a and the limit of (b_n) is b, then the limit of $(a_n + b_n)$ is $a + b$ so $(a_n + b_n)$ is convergent and, hence, Cauchy.

Defining the reals. Let $\mathbb{R}$ be the quotient set $R/\sim$. We think of the equivalence class $[(a_n)]$ as of the real number which is the limit of a_n as well as of any b_n such that $(a_n) \sim (b_n)$. For example, the real number 0 is the limit of $a_n = \frac{1}{n}$ but also of the constant sequence $b_n = 0$. The real number $\sqrt{2}$ is the limit of the sequence given by the recursive formula $a_{n+1} = \frac{a_n}{2} + \frac{1}{a_n}$ and the initial term $a_0 = 1$ (or any other element of R which converges to $\sqrt{2}$).

We define the **addition** on $\mathbb{R}$ by

$$[(a_n)] + [(b_n)] = [(a_n) + (b_n)] = [(a_n + b_n)].$$

The multiplication can be defined on R by $(a_n) \cdot (b_n) = (a_n \cdot b_n)$ and one can show that we can define the **multiplication** on $\mathbb{R}$ by

$$[(a_n)] \cdot [(b_n)] = [(a_n) \cdot (b_n)] = [(a_n \cdot b_n)].$$

The set $\mathbb{Q}$ embeds into $\mathbb{R}$. Indeed, for $a \in \mathbb{Q}$, we can consider the constant sequence $a_n = a$ which has the limit a, so by identifying the equivalence class of this sequence and its limit, we can consider a as an element of $\mathbb{R}$.

The element $0 \in \mathbb{R}$ is neutral for addition since $[(a_n)] + [(0)] = [(a_n + 0)] = [(a_n)]$. Similarly, $1 = [(1)]$ is neutral for multiplication.

The element $[(-a_n)]$ is the additive inverse of $[(a_n)]$. We say that the real number a is not zero if $a = [(a_n)]$ for a sequence which does not have its limit zero. In this case, there is n_0 such that all the terms of a_n for $n > n_0$ are nonzero. Hence, we can consider $b_n = \frac{1}{a_n}$ for those n. The limit of b_n is $\frac{1}{a}$, the reciprocal of the limit of a_n. Thus $[(a_n)] \cdot [(b_n)] = [(1)]$. This shows that every nonzero $a \in \mathbb{R}$ has a multiplicative inverse $\frac{1}{a}$.

The order $\leq$ is defined by requiring that $a \leq b$ for two real numbers $a = [(a_n)]$ and $b = [b_n]$ if for every $\varepsilon > 0$, there is some n_0 such that for all $n > n_0$ we have that $a_n \leq b_n + \varepsilon$. This, in

effect, ensures that that the limit of $b_n - a_n$ is not negative. The strict order can be defined from $\leq$ as usually: $a < b$ if $a \leq b$ and $a \neq b$ for any $a, b \in \mathbb{R}$.

The elements of the set $\mathbb{R} - \mathbb{Q}$ of reals which are not rationals are said to be **irrationals**. There are two types of irrational numbers: **algebraic** irrationals, obtained as solutions of polynomial equations with integer coefficients and **transcendental** irrationals, the irrationals which are not algebraic. The roots of rational numbers are examples of algebraic irrationals. For example, $\sqrt{2}$ is algebraic since it is the solution of the equation $x^2 - 2 = 0$. Numbers like e and π can be shown to be transcendental.

Irrational?

One can check that the addition, the multiplication, and the order satisfy the familiar properties below.

0 is neutral for addition. For any real number a, $a + 0 = 0 + a = a$.
$-a$ is the additive inverse of a. For any real number a, $a + (-a) = (-a) + a = 0$.
Associativity of addition. $(a + b) + c = a + (b + c)$ for any $a, b, c \in \mathbb{R}$.
Commutativity of addition. $a + b = b + a$ for any $a, b \in \mathbb{R}$.
1 is neutral for multiplication. $a \cdot 1 = 1 \cdot a = a$ for any $a \in \mathbb{R}$.
$\frac{1}{a}$ is the multiplicative inverse of $a \neq 0$. For any real number $a \neq 0$, $a \cdot \frac{1}{a} = \frac{1}{a} \cdot a = 1$.
Associativity of multiplication. $(ab)c = a(bc)$ for any $a, b, c \in \mathbb{R}$.
Commutativity of multiplication. $ab = ba$ for any $a, b \in \mathbb{R}$.
Distributivity. $a(b + c) = ab + ac$ and $(b + c)a = ba + ca$ for any $a, b, c \in \mathbb{R}$.
No zero divisors. For any $a, b \in \mathbb{R}$, if $a \cdot b = 0$ then $a = 0$ or $b = 0$.
Compatibility of $<$ with addition. If $a < c$ and $b < d$, then $a + b < c + d$ for any $a, b, c, d \in \mathbb{R}$.
Compatibility of $<$ with multiplication. If $a < c$ and $0 < b < d$, then $ab < cd$ for any $a, b, c, d \in \mathbb{R}$.

A digression. Groups, rings, and fields. Comparing the properties of rationals and reals, we see that they are exactly the same and that many of those are also the properties of the integers. These "recurring themes" led to definitions of three general algebraic structures: *groups, rings, and fields.* The benefit of studying generalized structures should be evident already: by studying properties shared by all the number sets (and by some other structures) we can draw *simultaneous* conclusions about all of these sets without studying each one in particular.

A **group** is any set with an operation $*$ which is associative, has a neutral element and such that every element has its inverse. A group is **abelian** if $*$ is commutative. The properties of addition on the sets $\mathbb{Z}, \mathbb{Q}$ and $\mathbb{R}$ make them abelian groups. As another example, the addition on the set $\{0, 1\}$ defined by the table in part (4) of Example 6 is also an abelian group. Modern Algebra covers much more examples of groups, not all of which are abelian.

If a set A has two operations $*$ and $\circ$ such that A is an abelian group under $*$, such that $\circ$ is associative and that distributivity holds for $*$ and $\circ$, then A is a **ring**. If $\circ$ is commutative,

then such ring is said to be **abelian**. The properties of the addition and the multiplication on the sets $\mathbb{Z}, \mathbb{Q}$ and $\mathbb{R}$ make them abelian rings.

If a set A has two operations $*$ and $\circ$ such that A is a ring and such that $A - \{0\}$ is an abelian group under $\circ$, then A is a **field**. The properties of the addition and the multiplication on the sets $\mathbb{Q}$ and $\mathbb{R}$ make them fields. The set $\mathbb{Z}$ with $+$ and $\cdot$ is not a field since not every nonzero element has a multiplicative inverse (in fact most of the nonzero elements of $\mathbb{Z}$ do not have multiplicative inverses, only 1 and -1 do).

A group

A ring

A field

If a field has a partial order $\leq$ which is compatible with the two field operations, it is an **ordered field**. If the partial order is a total order and if every nonempty subset with an upper bound has the supremum, such a field is *isomorphic* to the field of real numbers as introduced via Cauchy sequences (or Dedekind cuts). Thus, the above requirements on an ordered field can be used to introduce $\mathbb{R}$ axiomatically.

The cardinality of the reals. It may appear that we are adding a handful of roots of rational numbers and sprinkling the mix with a few numbers like e and π. However, as it turns out, the cardinality $\mathfrak{c}$ of $\mathbb{R}$ is strictly larger than $\mathbb{Q}$. So, $\mathbb{R}$ is **uncountable.** This was shown by Georg Cantor by exhibiting a bijection between the set of reals and the power set of $\mathbb{N}$. This shows that

$$\mathfrak{c} = 2^{\aleph_0}$$

As every set has strictly less elements than its power set (recall Theorem 1), this shows that

$$\mathfrak{c} = 2^{\aleph_0} > \aleph_0$$

and that $\mathbb{R}$ is uncountable.

Before showing the relation $\mathfrak{c} = 2^{\aleph_0}$, we show some claims regarding the cardinality of $\mathbb{R}$. First, one may think that the cardinality of any interval, possibly very small, is smaller than the cardinality of $\mathbb{R}$, the interval $(-\infty, \infty)$. This, however, is not the case: any interval, no matter its size and no matter if it is open, closed, or half-closed, has the same cardinality as $\mathbb{R}$.

Claim 5. *Any of the following intervals has the same cardinality as* $\mathbb{R}$: $(-\frac{\pi}{2}, \frac{\pi}{2})$, $(0, 1)$, (a, b), $(a, b]$, $[a, b)$, *and* $[a, b]$, *for any* $a, b \in \mathbb{R}$ *such that* $a > b$, *and* $(a, \infty), [a, \infty), (-\infty, a)$, *and* $(-\infty, a]$ *for any* $a \in \mathbb{R}$.

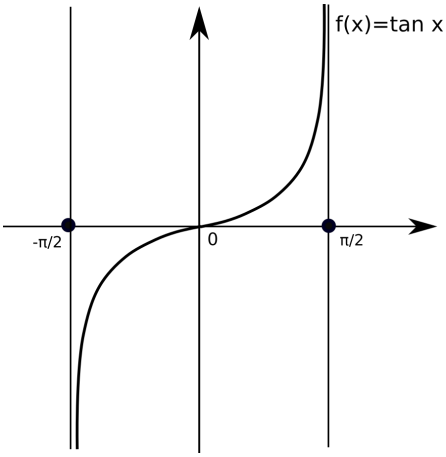
Proof. The function $\tan x$ is a bijection of the interval $(-\frac{\pi}{2}, \frac{\pi}{2})$ and $\mathbb{R}$. This can be checked by considering the graph (see the first figure below) and checking that any horizontal line at any y-value intercepts the graph exactly once or by noting that $\tan^{-1} x$ is the inverse of $\tan x$.

In section 6, we used linear function passing the points (a, c) and (b, d) to obtain a bijective correspondence of the intervals (a, b) and (c, d). This shows that each pair of the intervals $(-\frac{\pi}{2}, \frac{\pi}{2})$, $(0, 1)$, and (a, b), are in a bijective correspondence. Since the relation of equipotence is

transitive and since $(-\frac{\pi}{2}, \frac{\pi}{2})$ is equipotent to $\mathbb{R}$, we have that $(0,1)$ and (a,b) are also equipotent to $\mathbb{R}$.

Claim 3 (in section 6) implies that there are bijections between (a,b) and $[a,b)$, between (a,b) and $(a,b]$, and between $[a,b)$ and $[a,b]$. Alternatively, a specific bijection can be produced for any of those pairs. For example, a bijection $(0,1) \to [0,1)$ can be obtained by considering the elements of $(0,1)$ which are of the form $\frac{1}{n}$ for $n \in \mathbb{N} - \{0,1\}$ and the map given by

$$x \mapsto \begin{cases} x & x \neq \frac{1}{n}, n \geq 2 \\ \frac{1}{n-1} & x = \frac{1}{n}, n > 2 \\ 0 & x = \frac{1}{2} \end{cases}$$



(note that this definition follows the approach in the proof of Claim 3). We obtain a bijection $(a,b) \to [a,b)$ by considering the composition of bijections $(a,b) \to (0,1) \to [0,1) \to [a,b)$ where the middle map is the one given by the above formula and the first and the last are obtained by the linear functions passing the points $(a,0)$ and $(b,1)$ and its inverse.

One can define a bijections $(a,b) \to (a,b]$ and $[a,b) \to [a,b]$ similarly. To obtain a bijection $(a,b) \to [a,b]$, we can consider the composition of bijections $(a,b) \to [a,b) \to [a,b]$.

Let us consider intervals of infinite length. Note that the function e^x is a bijective correspondence $\mathbb{R} \to (0,\infty)$ so that $e^x + a$ is a bijective correspondence $\mathbb{R} \to (a,\infty)$. Composing this with the bijection $(a,\infty) \to [a,\infty)$ (where we use Claim 3 again), we have a bijection of $\mathbb{R}$ and $[a,\infty)$. The map $-e^x$ is a bijective correspondence $\mathbb{R} \to (-\infty, 0)$, so that $-e^x + a$ is a bijective correspondence of $\mathbb{R}$ and $(-\infty, a)$. Composing this with a bijection $(-\infty, a) \to (-\infty, a]$, we obtain all needed bijections.

□

Exercise 34. Show that the following sets are in bijective correspondences with $\mathbb{R}$.

(1) $(a,b) \cup (c,d)$ where $b \leq c$.
(2) $\bigcup_{i=1}^{n}(a_i, b_i)$ where $b_i \leq a_{i+1}$ for any positive integer n and $i = 1, 2, \ldots, n-1$.

Solution. (1) Since the intervals are disjoint, the cardinality of the union is equal to the sum of cardinalities of each interval (recall section 6). Since each interval has cardinality equal to $|\mathbb{R}|$, we have that

$$|(a,b) \cup (c,d)| = |(a,b)| + |(c,d)| = |\mathbb{R}| + |\mathbb{R}| = |\mathbb{R}|$$

where the last relation holds by the section 6 formula that $\alpha + \alpha = \alpha$ for infinite cardinals.

(2) Let us use the induction on n. If $n = 1$, the statement holds because there are bijections $(a_1, b_1) \to (0,1) \to \mathbb{R}$ by Claim 5. Assuming the statement holds for the union $\bigcup_{i=1}^{n}(a_i, b_i)$ of n intervals, let us consider the union $\bigcup_{i=1}^{n+1}(a_i, b_i) = \bigcup_{i=1}^{n}(a_i, b_i) \cup (a_{n+1}, b_{n+1})$ of $n+1$ intervals.

As the sets $\bigcup_{i=1}^{n}(a_i, b_i)$ and (a_{n+1}, b_{n+1}) are disjoint, we can use exactly the same argument as in part (a).

$$\left|\bigcup_{i=1}^{n}(a_i, b_i) \cup (a_{n+1}, b_{n+1})\right| = \left|\bigcup_{i=1}^{n}(a_i, b_i)\right| + |(a_{n+1}, b_{n+1})| = |\mathbb{R}| + |\mathbb{R}| = |\mathbb{R}|$$

where the relation $|\bigcup_{i=1}^{n}(a_i, b_i)| = |\mathbb{R}|$ holds by inductive hypothesis.

Claim 5 enables us to prove the relation $c = 2^{\aleph_0}$ by obtaining a bijection of the closed interval $[0, 1]$ and the power set $\mathcal{P}(\mathbb{N})$. We can do that by considering the **decimal representation** of a real number in $[0, 1]$.

Every rational number can be represented by a decimal number which either has finitely many nonzero decimals or it has periodic decimal representation. For example,

$$\frac{1}{5} = 0.2000000\ldots \text{ and } \frac{1}{3} = 0.33333\ldots$$

Geometric Series. Any decimal number with periodic representation can be converted to a fraction of two integers. To be able to do that, we consider the formula for the sum of a convergent geometric series.

A **geometric series** is any infinite sum of terms of a sequence such that the ratio of two consecutive terms is constant r. In general, this series has the form

$$ar^k + ar^{k+1} + ar^{k+2} + \ldots = ar^k \sum_{n=0}^{\infty} r^n.$$

We are interested exclusively in the case when $0 < r < 1$ in which case this infinite sum is *finite* (Calculus 3 covers full details).

Let us concentrate on the series $\sum_{n=0}^{\infty} r^n$. Assuming that the sum $1+r+r^2+\ldots$ is convergent and equal to s, we have that $s = 1 + r + r^2 + r^3 + \ldots = 1 + r(1 + r + r^2 + \ldots) = 1 + rs$. Hence, $s = 1 + rs$. Solving this equation for s, we have that $s = \frac{1}{1-r}$.

Thus, the geometric series $\sum_{n=k}^{\infty} ar^n = ar^k + ar^{k+1} + ar^{k+2} + \ldots = ar^k \sum_{n=0}^{\infty} r^n$ has the sum

$$\sum_{n=k}^{\infty} ar^n = \frac{ar^k}{1-r}$$

For example, the series $\sum_{n=1}^{\infty} \frac{9}{10^n}$ is equal to $\sum_{n=1}^{\infty} 9\left(\frac{1}{10}\right)^n$ and, hence, it is a geometric series with $a = 0, k = 1$ and $r = \frac{1}{10}$. Its sum can be found as below.

$$\sum_{n=1}^{\infty} \frac{9}{10^n} = \sum_{n=1}^{\infty} 9\left(\frac{1}{10}\right)^n = \frac{9 \cdot \frac{1}{10}}{1 - \frac{1}{10}} = \frac{\frac{9}{10}}{\frac{9}{10}} = 1.$$

Cardinality of reals. An irrational number has a decimal representation without any periodicity of the digits appearing after the decimal point. In any case, any real number a in $[0, 1]$ can be written as zero followed by a decimal point with infinitely many digits (periodic or not) afterwards. So, if $a_1a_2a_3\ldots$ denote the digits after the decimal point, we can write

$$a = 0.a_1a_2a_3\ldots$$

Let us consider the sequence given by

$$b_0 = 0, \quad b_1 = 0.a_1, \quad b_2 = 0.a_1a_2, \quad \ldots, \quad b_n = 0.a_1a_2\ldots a_n, \quad \ldots$$

Each term of the sequence b_n is rational since it has only finitely many nonzero decimals. The fractional representation of b_n can be found by representing b_n as a sum

$$0 + \frac{a_1}{10} + \frac{a_2}{10^2} + \ldots + \frac{a_n}{10^n} = \frac{a_1 10^{n-1} + \ldots + a_{n-1}10 + a_n}{10^n}$$

Since b_n is converging to a, the sequence b_n is a Cauchy sequence.

However, the above decimal representation of a is not unique in general: $0.9999\ldots$ and 1 represent the same real number. Indeed

$$0.99999\ldots = 0.9 + 0.09 + 0.009 + \ldots = \frac{9}{10} + \frac{9}{10^2} + \frac{9}{10^3} + \ldots \frac{9}{10^n} + \ldots$$

Note that the last expression can be written using the $\sum$ notation as $\sum_{n=1}^{\infty} \frac{9}{10^n}$. We have found the sum of this geometric series to be 1.

$$\sum_{n=1}^{\infty} \frac{9}{10^n} = \sum_{n=1}^{\infty} 9\left(\frac{1}{10}\right)^n = \frac{9 \cdot \frac{1}{10}}{1 - \frac{1}{10}} = \frac{\frac{9}{10}}{\frac{9}{10}} = 1.$$

So, the decimal representations are not unique but the Cauchy sequences obtained from them using the process above have the same limit and, hence, represent the same real number.

Now let us consider the **binary** representation instead of the usual base 10 representation. In this case, only zeros and ones appear as the digits and any real number in $[0, 1]$ can be written as

$$0.a_1a_2\ldots = \sum_{n=1}^{\infty} \frac{a_n}{2^n}$$

Just as with base 10 representations, the same number can have two different binary representations. For example

$$0.1 = \frac{1}{2} \quad \text{and} \quad 0.01111\ldots = \sum_{n=2}^{\infty} \frac{1}{2^n} = \frac{\frac{1}{4}}{1 - \frac{1}{2}} = \frac{1}{2}.$$

However, any infinite sequence a_n, for $n = 1, 2, \ldots$, of zeros and ones determines a *unique* decimal number

$$a = \sum_{n=1}^{\infty} \frac{a_n}{10^n}.$$

With these prerequisites, we can show the theorem below.

Theorem 6. $\mathfrak{c} = 2^{\aleph_0}$

Proof. We will show that $2^{\aleph_0} \leq \mathfrak{c}$ by displaying an injection $\mathcal{P}(\mathbb{N}) \to [0, 1]$. Then, we show that $\mathfrak{c} \leq 2^{\aleph_0}$ by displaying an injection $[0, 1] \to \mathcal{P}(\mathbb{N})$.

First, let us define an injective map $f : \mathcal{P}(\mathbb{N}) \to [0, 1]$. For any nonempty $A \subseteq \mathbb{N}$, we map it to a real number $f(A)$ given by

$$0.a_1a_2\ldots = \sum_{n=1}^{\infty} \frac{a_n}{10^n}$$

where $a_n = 1$ if $n \in A$ and $a_n = 0$ if $n \notin A$. In addition, we map $\emptyset$ to 0. As two different subsets of $\mathbb{N}$ determine two different arrays of zeros and ones, the comments before the statement of the theorem indicate that this map one-to-one.

Second, let us define an injection $g : [0,1] \to \mathcal{P}(\mathbb{N})$. For $a \in [0,1]$ let us consider again the decimal representation

$$a = 0.a_1a_2\ldots = \sum_{n=1}^{\infty} \frac{a_n}{10^n}$$

which does not end with an infinite array of 9's. For example, if $a = 0.12399999\ldots$, we represent a as $0.1240000\ldots$. This requirement ensures that such representation is unique which will make the map g well-defined. For such a representation, let us define a subset $g(a)$ of $\mathbb{N}$ by

$$g(a) = \{2^n 3^{a_n} \ : \ n \in \mathbb{N} - \{0\}\}$$

If $a \neq b$, then there is n such that $a_n \neq b_n$. Hence, $2^n 3^{a_n} \neq 2^n 3^{b_n}$ so $2^n 3^{a_n} \in g(a)$ and $2^n 3^{a_n} \notin g(b)$ which shows that $g(a) \neq g(b)$ so g is injective. □

The fact that $\mathbb{Q}$ is countable and $\mathbb{R}$ is not implies that there are uncountably many irrational numbers. So, there are "much more" irrationals than rationals. However, the rationals can be still found "everywhere" in the sense that in every interval, no matter how small it is, there is a rational number. This statement is usually shortened by saying that the rational numbers are **dense** in the set of reals. We prove this statement after a short digression.

A digression. Labeling mathematical statements. We have encounter statements labeled as "theorems": Cantor's Theorem (Theorem 1) and recently shown Theorem 6. We also made references to Gödel Incompleteness Theorems, and you are probably familiar with Fundamental Theorem of Calculus from the first Calculus course. A label **theorem** is usually used for statements which are nontrivial to prove and which are proven often by revoking several other already proved statements. A label **proposition** is used for statements of less major impact and depth or statements used for proving other theorems or other propositions. Many of the exercises in this text are, in fact, theorems or propositions. For example, all the properties of naturals, integers, rational or reals as well as Exercises 20, 23, 25 could been called propositions and Exercises 18, 24, 28, 29 could be called theorems. A label **lemma** is used for statements of even smaller impact or scope than a proposition (although there are some very useful and well-known results with "lemma" in their names) and they are usually used only to shorten the proof of a larger result. A **corollary** is a statement that follows from a theorem, a proposition or a lemma. For example, Lemmas 7 and 8 and Corollary 10 below are examples of lemmas and corollaries.

While theorems, propositions, lemmas and corollaries are statements to be shown, a **definition** is a statement in which a new concept is introduced using the existing concepts. Hence, it does not require a proof. For example, given a partial order $\leq$, we are defining a new relation $<$ by specifying that $a < b$ means that $a \leq b$ and $a \neq b$ both hold.

The terms "exercise, practice problem," or "claim" were used so far in the text because these terms may be less intimidating that "theorem, proposition, lemma" or "corollary" for a novice. Also, "solution" has been used instead of "proof" often. But at this point, we start using the proper labeling.

The rationals are dense in the reals. Let us state the claim on the density of the rationals in the reals in a form of a proposition and let us prove it using two lemmas.

Lemma 7. *For any real number $a \in \mathbb{R}$, there is an integer n such that $n - 1 \leq a < n$.*

Proof. The union of the intervals $[n-1, n)$ for $n \in \mathbb{Z}$ is equal to the entire number line $\mathbb{R}$, so $\mathbb{R} = \bigcup_{n\in\mathbb{Z}}[n-1, n)$. Thus, $a \in \mathbb{R}$ is in the union $\bigcup_{n\in\mathbb{Z}}[n-1, n)$ and so there is $n \in \mathbb{Z}$ such that $a \in [n-1, n)$ which implies that $n - 1 \leq a < n$. □

The next lemma is often referred to as the **Archimedean Property**.

Lemma 8. *For any positive real number ε, there is a positive integer n such that $n\varepsilon > 1$ (equivalently $\frac{1}{n} < \varepsilon$ and, also equivalently $n > \frac{1}{\varepsilon}$).*

By the first equivalent statement in parenthesis, for every $\varepsilon > 0$, no matter how small it is, there is a natural number n such that $\frac{1}{n}$ is even smaller. By the second equivalent statement, for every $\varepsilon > 0$, no matter how large $\frac{1}{\varepsilon}$ is, there is an even larger natural number n.

Proof. By Lemma 7 applied to $a = \frac{1}{\varepsilon}$, there is an integer n such that $\frac{1}{\varepsilon} \in [n-1, n)$.

As $\varepsilon > 0$, we have that $\frac{1}{\varepsilon} > 0$ and so $n - 1 \geq 0$ so $n \geq 1$ and, hence, such n is a positive integer. Since $\frac{1}{\varepsilon} \in [n-1, n)$, we have that $\frac{1}{\varepsilon} < n$, so $n\varepsilon > 1$. □

Proposition 9. *For every $a, b \in \mathbb{R}$ such that $a < b$, there is $q \in \mathbb{Q}$ such that $a < q < b$.*

Proof. As $a < b$, we have that $b - a > 0$. By Lemma 8, there is a positive integer n such that $n(b-a) > 1$. Thus, $nb > na + 1$. By Lemma 7, for na there is an integer m such that $m - 1 \leq na < m$. By adding 1 to the relation $m - 1 \leq na$, we have that $m \leq na + 1$. Hence,

$$na < m \leq na + 1 < nb$$

and so $na < m < nb$. Dividing by n we obtain

$$a < \frac{m}{n} < b$$

which finishes the proof since $\frac{m}{n}$ is a rational number. □

We show that the existence of one rational in any interval implies the existence of infinitely many of them.

Corollary 10. *For every $a, b \in \mathbb{R}$ such that $a < b$, there are infinitely many rational numbers q such that $a < q < b$.*

Proof. By Proposition 9, there is $q_0 \in \mathbb{Q}$ such that

$$a < q_0 < b.$$

Applying Proposition 9 to the interval (a, q_0), we obtain a rational $q_1 \in \mathbb{Q}$ such that

$$a < q_1 < q_0.$$

Continuing the process, we obtain a sequence q_n for $n = 0, 1, 2, \ldots$ By construction $q_{n+1} < q_n$ for any n so the terms of the sequence are different rational numbers. We have that

$$a < \ldots < q_{n+1} < q_n < \ldots < q_1 < q_0 < b$$

so any terms of the sequence is in the interval (a, b). □

Practice Problems 10.

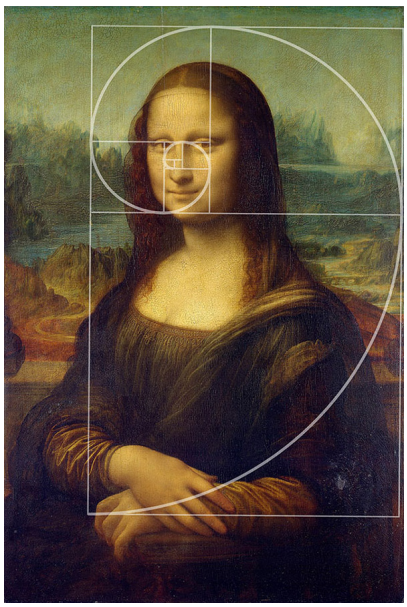
(1) Show that any constant sequence $a_n = a$ is Cauchy.
(2) Show that the sum of two Cauchy sequences is a Cauchy sequence. Using the relation $|a + b| \leq |a| + |b|$ for any $a, b \in \mathbb{R}$ may be useful at some point.
(3) Show the following properties of real numbers.
    (a) For any real number a, $-a$ is the additive inverse of a.

(b) 1 is neutral for multiplication.
(c) $\mathbb{R}$ has no zero divisors.

(4) Using the method for finding the limit of a recursive sequence, find the limit of the following recursive sequences.
(a)
$$a_{n+1} = \sqrt{2 + a_n}, \quad a_0 = 0.$$
(b)
$$a_{n+1} = \frac{1}{1 + a_n}, \quad a_0 = 1.$$

(5) **Fibonacci numbers** are terms of the following recursive sequence.
$$f_{n+2} = f_{n+1} + f_n \quad \text{with} \quad f_0 = 0, \text{ and } f_1 = 1$$
for $n = 0, 1, 2, \ldots$. Thus one starts with 0 and 1, and then produces the next Fibonacci number by adding the two previous Fibonacci numbers. The first few terms are
$$0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233, 377, 610, 987, 1597, 2584, \ldots$$
and it is clear that this sequence is clearly divergent because these terms increase without a bound.

On the other hand, two quantities are said to be in the **golden ratio** if the ratio of the larger to smaller quantity is the same as the ratio of their sum to the larger quantity. So, if a and b are two quantities and $a > b$, then a and b are in the golden ratio if
$$\frac{a}{b} = \frac{a+b}{a}.$$
To find the ratio $x = \frac{a}{b}$, note that the right side is $\frac{a+b}{a} = \frac{a}{a} + \frac{b}{a} = 1 + \frac{1}{x}$. Thus,
$$x = 1 + \frac{1}{x} \;\Rightarrow\; x^2 = x + 1 \;\Rightarrow\; x^2 - x - 1 = 0.$$
The positive solution $\frac{1+\sqrt{5}}{2} \approx 1.618$ of this quadratic equation is prominently used in science as well as in art, architecture, and music. While the Fibonacci sequence is divergent the **quotient** $\frac{f_{n+1}}{f_n}$ of two consecutive terms of the Fibonacci sequence is *convergent*. Show that the limit of the sequence $a_n = \frac{f_{n+1}}{f_n}$ is the golden ratio $\frac{1+\sqrt{5}}{2} \approx 1.618$.



(6) Show that the following pairs of sets are in a bijective correspondence. You can assume the existence of any of the bijective correspondences from Claim 5.
(a) $(3, 5) \cup [8, 9)$ and $(7, \infty)$
(b) $(3, 5] \cup [0, 9) \cup [7, \infty)$ and $(-\infty, 1]$
(c) $\bigcup_{n \in \mathbb{N} - \{0\}} (-n, n)$ and $(0, 1)$
(d) $\bigcap_{n \in \mathbb{N}} [0, n + 1)$ and $\mathbb{R}$
(e) $\bigcup_{n \in \mathbb{N}} (-\infty, -n)$ and $(1, \infty)$

(7) Represent the following decimal numbers as quotients of two integer numbers.
(a) $0.222222\ldots$
(b) $0.27272727\ldots$
(c) $1.2345454545\ldots$

(8) Let us consider the characteristic function $\chi_{\mathbb{Q}}$ where $\mathbb{Q}$ is considered as a subset of $\mathbb{R}$ (see practice problem (6) in section 5). Show that χ maps uncountably many numbers to 0.

Solutions. (1) We need to show that for every $\varepsilon > 0$ there is a natural number n_0 such that for all $m, n > n_0$ $|a_n - a_m| < \varepsilon$. As $|a_n - a_m| = |a - a| = 0 < \varepsilon$, we can take $n_0 = 0$ so that for any positive natural numbers m and n we have that $|a_n - a_m| = |a - a| = 0 < \varepsilon$.

(2) Let (a_n) and (b_n) be two Cauchy sequences. We need to show that for every $\varepsilon > 0$ we can find a natural number N_0 such that for every $m, n > N_0$, $|a_n + b_n - (a_m + b_m)| < \varepsilon$. By the given absolute value relation, we have that

$$|a_n + b_n - (a_m + b_m)| = |(a_n - a_m) + (b_n - b_m)| \leq |a_n - a_m| + |b_n - b_m|.$$

Thus, if we can find n_0 such that $|a_n - a_m| < \frac{\varepsilon}{2}$ and m_0 such that $|b_n - b_m| < \frac{\varepsilon}{2}$ for all m, n largest than the larger of n_0, m_0, then we would have that

$$|a_n + b_n - (a_m + b_m)| = |(a_n - a_m) + (b_n - b_m)| \leq |a_n - a_m| + |b_n - b_m| = \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon.$$

We *can* find such n_0 and m_0 since both (a_n) and (b_n) are Cauchy. Thus, we can take N_0 to be the larger of m_0 and n_0 (or n_0 if $m_0 = n_0$).

(3) (a) We need to show that $a + (-a) = (-a) + a = 0$. Let $a = [(a_n)]$ for some Cauchy sequence (a_n) and $0 = [(0)]$ where (0) is the constant sequence $0, 0, 0, \ldots$. In this case, $-a$ can be represented as $[(-a_n)]$. We have that $a + (-a) = 0$ since $[(a_n)] + [(-a_n)] = [(a_n - a_n)] = [(0)] = 0$. Similarly, $(-a) + a = 0$.

(b) We need to show that $a \cdot 1 = 1 \cdot a = a$ for any real number a. Let $a = [(a_n)]$ for some Cauchy sequence (a_n) and $1 = [(1)]$ where (1) is the constant sequence $1, 1, 1, \ldots$. We have that $a \cdot 1 = [(a_n)] \cdot [(1)] = [(a_n \cdot 1)] = [(a_n)] = a$. Similarly, $1 \cdot a = a$.

(c) We need to show that $a \cdot b = 0$ implies that $a = 0$ or $b = 0$. Let $a = [(a_n)]$ for some Cauchy sequence (a_n) and $b = [(b_n)]$ for some Cauchy sequence (b_n). The assumption that $ab = 0$ implies that $[(a_n b_n)] = 0$. Let us assume the contrary of $a = 0$ or $b = 0$: assume that both a and b are nonzero. This means that there is n_0 such that $a_n \neq 0$ for all $n > n_0$ and that there is m_0 such that $b_n \neq 0$ for all $n > m_0$. By taking N_0 larger than n_0 and m_0, we have that both a_n and b_n are nonzero and so $a_n \cdot b_n \neq 0$ because $\mathbb{Q}$ does not have zero divisors. This shows that the element $[(a_n b_n)]$ is nonzero which contradicts our assumption.
One can also show this claim by using contrapositive instead of contradiction: assume that $a \neq 0$ and $b \neq 0$ and show that $ab \neq 0$.

(4) (a) Let a stand for the limit of this sequence in case it exists. Note that then $a = \lim_{n\to\infty} a_n$ and $a = \lim_{n\to\infty} a_{n+1}$ as well. To find the value of a let $n \to \infty$ in the equation $a_{n+1} = \sqrt{2 + a_n}$. The left side converges to a and the right side to $\sqrt{2 + a}$. So, a can be found from the equation $a = \sqrt{2 + a} \Rightarrow a^2 = 2 + a \Rightarrow a^2 - a - 2 = 0 \Rightarrow (a - 2)(a + 1) = 0 \Rightarrow a = 2$ or $a = -1$. Since -1 is an extraneous root (it does not satisfy the equation $a = \sqrt{2 + a}$), the limit of the sequence is $a = 2$. Alternatively, you can also argue that starting with the nonnegative term $a_0 = 0$, all the terms of the sequence are nonnegative and so the solution $a = -1$ can be discarded.

(b) Let a stand for the limit of this sequence in case it exists. Note that then $a = \lim_{n\to\infty} a_n$ and $a = \lim_{n\to\infty} a_{n+1}$ as well. To find the value of a let $n \to \infty$ in the equation $a_{n+1} = \frac{1}{1+a_n}$. The left side converges to a and the right side to $\frac{1}{1+a}$. So, a can be found from the equation $a = \frac{1}{1+a} \Rightarrow a(1 + a) = 1 \Rightarrow a^2 + a - 1 = 0 \Rightarrow a =$

$\frac{-1+\sqrt{5}}{2} \approx 0.618$ or $a = \frac{-1-\sqrt{5}}{2} \approx -1.618$. Starting with the positive term $a_0 = 1$, all the terms of the sequence are positive, so the sequence converges towards the positive value $a = \frac{-1+\sqrt{5}}{2} \approx 0.618$.

(5) Let us denote $a_n = \frac{f_{n+1}}{f_n}$. Dividing the equation $f_{n+2} = f_{n+1} + f_n$ by f_{n+1}, we obtain $\frac{f_{n+2}}{f_{n+1}} = 1 + \frac{f_n}{f_{n+1}}$. Note that the term on the left is $a_{n+1} = \frac{f_{n+2}}{f_{n+1}}$ and that the right side is $1 + \frac{1}{a_n}$. Thus, the recursive formula of the quotient sequence a_n is $a_{n+1} = 1 + \frac{1}{a_n}$.

Denote the limit by x. Thus $x = \lim_{n\to\infty} a_n = \lim_{n\to\infty} a_{n+1}$ and so value x satisfies the equation $x = 1 + \frac{1}{x}$. Multiply this equation by x to get $x^2 = x + 1 \Rightarrow x^2 - x - 1 = 0 \Rightarrow x = \frac{1\pm\sqrt{1+4}}{2} = \frac{1\pm\sqrt{5}}{2} \Rightarrow x = \frac{1+\sqrt{5}}{2} \approx 1.618$ or $x = \frac{1-\sqrt{5}}{2} \approx -0.618$. Negative solution is not relevant since all terms of the sequence are positive. Thus, the limit is the golden ratio $\frac{1\pm\sqrt{5}}{2} \approx 1.618$.

(6) (a) $|(3,5) \cup [8,9)| = |(3,5)| + |[8,9)| = |\mathbb{R}| + |\mathbb{R}| = |\mathbb{R}|$ and $|(7,\infty)| = |\mathbb{R}|$.

(b) Note that $[0,9) \cup [7,\infty) = [0,\infty)$ and $(3,5] \cup [0,\infty) = [0,\infty)$. So, $|(3,5] \cup [0,9) \cup [7,\infty)| = |[0,\infty)| = |\mathbb{R}|$ and $|(-\infty,1]| = |\mathbb{R}|$.

(c) Note that $\bigcup_{n\in\mathbb{N}}(-n,n) = (-1,1) \cup (-2,2) \cup (-3,3) \cup \ldots = (-\infty,\infty) = \mathbb{R}$. As $|(0,1)| = |\mathbb{R}|$, the two sets have the same cardinality.

(d) $\bigcap_{n\in\mathbb{N}}[0,n+1) = [0,1) \cap [0,2) \cap [0,3) \cap \ldots = [0,1)$. As $|[0,1)| = |\mathbb{R}|$, the two sets have the same cardinality.

(e) $\bigcup_{n\in\mathbb{N}}(-\infty,-n) = (-\infty,0) \cup (-\infty,-1) \cup (-\infty,-2) \cup (-\infty,-3) \cup \ldots = (-\infty,0)$. Since $|(-\infty,0)| = |\mathbb{R}|$ and $|(1,\infty)| = |\mathbb{R}|$, the two sets have the same cardinality.

(7) (a) $0.222222\ldots = 0.2 + 0.02 + 0.002 + \ldots = \frac{2}{10} + \frac{2}{10^2} + \frac{2}{10^3} + \ldots = \sum_{n=1}^{\infty} 2\left(\frac{1}{10}\right)^n$. Using the formula $\frac{ar^k}{1-r}$ with $a = 2$, $r = \frac{1}{10}$ and $k = 1$, we have that the sum is $\frac{\frac{2}{10}}{\frac{9}{10}} = \frac{2}{9}$.

(b) $0.27272727\ldots = 0.27 + 0.0027 + 0.000027 + \ldots = \frac{27}{100} + \frac{27}{100^2} + \frac{27}{100^3} + \ldots = \sum_{n=1}^{\infty} 27\left(\frac{1}{100}\right)^n$. Using the formula $\frac{ar^k}{1-r}$ with $a = 27$, $r = \frac{1}{100}$ and $k = 1$, we have that the sum is $\frac{\frac{27}{100}}{\frac{99}{100}} = \frac{27}{99} = \frac{3}{11}$.

(c) $1.2345454545\ldots = 1.23 + 0.0045 + 0.000045 + 0.00000045 + \ldots = 1.23 + \frac{45}{100^2} + \frac{45}{100^3} + \frac{45}{100^4} + \ldots = 1.23 + \sum_{n=2}^{\infty} 45\left(\frac{1}{100}\right)^n$. Using the formula $\frac{ar^k}{1-r}$ with $a = 45$, $r = \frac{1}{100}$ and $k = 2$, we have that the sum is $1.23 + \frac{\frac{45}{100^2}}{\frac{99}{100}} = \frac{123}{100} + \frac{45}{99(100)} = \frac{123(99)+45}{99(100)} = \frac{12222}{9900} = \frac{679}{550}$.

(8) Recall that the characteristic function $\chi_{\mathbb{Q}}$ is defined by $x \mapsto 1$ if $x \in \mathbb{Q}$ and $x \mapsto 0$ if $x \notin \mathbb{Q}$. Thus, every irrational number is mapped to 0. As there are uncountably many irrational numbers, there are uncountably many numbers which are mapped to 0.

11. Complex numbers

Let us summarize our journey with number sets. We started by counting things and obtained $\mathbb{N}$ as a result. This was followed by the introduction of integers in order to be able to solve all equations of the form $m + x = n$ with $m, n \in \mathbb{N}$. After that we introduced rationals so that we can solve all equations of the form $mx = n$ with $m, n \in \mathbb{Z}, m \neq 0$. Then, we introduced reals so that we can solve some polynomial equations with coefficients in rationals (e.g. $x^2 = a$ for $a \in \mathbb{Q}, a > 0$).

The set $\mathbb{R}$ was obtained by "completion": by adding the limits of all rational Cauchy sequences with limits outside of $\mathbb{Q}$. So, $\mathbb{R}$ seems "complete enough". However, there are still polynomial equations (with integer coefficients no less) without solution in $\mathbb{R}$. For example, $x^2 = -1$ does not have real solutions. So, there are still elements to be added to $\mathbb{R}$ to obtain a larger number set. It turns out that by extending $\mathbb{R}$ with a solution of this single equation, we end up with a number set which is "complete" also in the algebraic sense (not only in the sense that it contains the limits of all convergent sequences): it contains all n solutions of any degree n polynomial equation with real coefficients. This statement, known as the **Fundamental Theorem of Algebra**, implies that with complex numbers we really reached the roof – there are no solutions of any polynomial equation outside of the set of complex numbers.

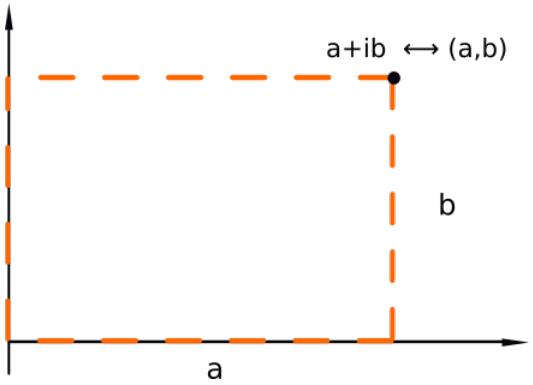
The introduction of complex numbers seems relatively easy in comparison to the introductions of $\mathbb{Z}, \mathbb{Q}$ or $\mathbb{R}$ because there is no equivalence relation, no quotient set, and no axioms – just denote any one of the solutions of the equation

$$x^2 = -1$$

by i (which would make $-i$ be the other solution) and consider all the sums of the form

$$a + ib$$

where a and b are real numbers called the **real** and the **imaginary** part respectively. We use $\mathbb{C}$ to denote the set of all sums $a + ib$ for $a, b \in \mathbb{R}$. The representation $a + ib$ is called the **algebraic form**.



The elements of $\mathbb{C}$ are in a bijective correspondence with the elements of $\mathbb{R} \times \mathbb{R}$

$$a + ib \mapsto (a, b)$$

which enables us to represent the complex numbers as points in the xy-plane.

The **addition** of two complex numbers is defined by adding the similar terms as below.

$$(a + ib) + (c + id) = (a + c) + i(b + d)$$

This operation is associative and commutative, the element $0 = 0+0i$ is neutral for the addition, and $-a - ib$ is the additive inverse of $a + ib$.

The **multiplication** of two complex numbers is defined by foiling and using that $i^2 = -1$ as below.

$$(a + ib) \cdot (c + id) = ac + iad + ibc + bd(i)^2 = (ac - bd) + (ad + bc)i$$

This operation is associative, commutative, and distributive for the addition. The element $1 = 1 + 0i$ is neutral for the multiplication. If $a + ib \neq 0 = 0 + 0i$ (which implies that $a \neq 0$ or $b \neq 0$), let us show that $\frac{a-ib}{a^2+b^2}$ is the inverse of $a + ib$. Indeed

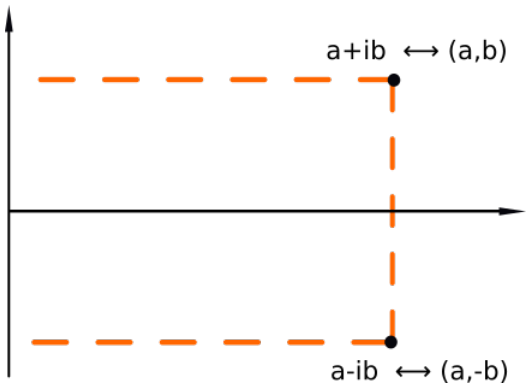
$$(a + ib) \cdot \frac{a - ib}{a^2 + b^2} = \frac{(a + ib)(a - ib)}{a^2 + b^2} = \frac{a^2 - abi + abi - b^2}{a^2 + b^2} = \frac{a^2 + b^2}{a^2 + b^2} = 1.$$

The form of the inverse brings the expressions $a^2 + b^2$ and $a - ib$ into focus. Let us expand on their relevance.

The complex number $a - ib$ is said to be the **complex conjugate** of the number $a+ib$. The product of the complex number and its conjugate is a real number since

$$(a + ib)(a - ib) = a^2 + b^2.$$

This can be used when dividing complex numbers: to find the quotient of two complex numbers, one multiplies both the numerator and the denominator by the complex conjugate of the denominator. In this way, the answer is again a sum of the algebraic form.



Exercise 35. Find the sum, product and quotient of $2 + i$ and $3 - 4i$.

Solution. The sum is $2 + i + 3 - 4i = 2 + 3 + i - 4i = 5 - 3i$.

The product is $(2 + i)(3 - 4i) = 6 - 8i + 3i - 4i^2 = 6 - 8i + 3i + 4 = 10 - 5i$.

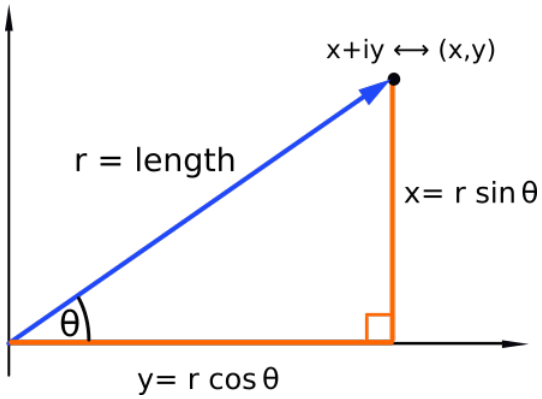
The complex number $3 + 4i$ is the conjugate of $3 - 4i$, so the quotient is

$$\frac{2 + i}{3 - 4i} = \frac{2 + i}{3 - 4i}\,\frac{3 + 4i}{3 + 4i} = \frac{(2 + i)(3 + 4i)}{(3 - 4i)(3 + 4i)} = \frac{6 + 8i + 3i - 4}{9 + 12i - 12i + 16} = \frac{2 + 11i}{25} = \frac{2}{25} + i\frac{11}{25}$$

If (x, y) is a point in the xy-plane, the the root of $x^2 + y^2$ is the **distance** of (x, y) from the origin. It is often denoted by r and it is called the **modulus** or **magnitude** of $x + iy$. It can be represented using the absolute value symbol

$$r = |x + iy| = \sqrt{x^2 + y^2}.$$

Let also use θ to denote the angle between positive part of x-axis and the position vector of the point (x, y) (in blue on the figure on the right). This angle is called the **argument** or the **phase** of $x + iy$. The right triangle on the figure indicates that



$$x = r\cos\theta \quad \text{and} \quad y = r\sin\theta.$$

This shows that, if we identify the complex number $x + iy$ with its representation (x, y) in the xy-plane, we have that

$$x + iy = r\cos\theta + ir\sin\theta.$$

If the number $x+iy$ is represented as $r\cos\theta + ir\sin\theta$, it is said to be in **polar coordinates** or to have a **trigonometric form**.

The formulas $r = \sqrt{x^2+y^2}$ and $\tan\theta = \frac{y}{x}$ enable you to find r and θ for given x and y. Recall that

$$\tan\theta = \tfrac{y}{x} \quad \text{implies that} \quad \theta = \tan^{-1}\tfrac{y}{x} \quad \text{or} \quad \theta = \pi + \tan^{-1}\tfrac{y}{x}$$

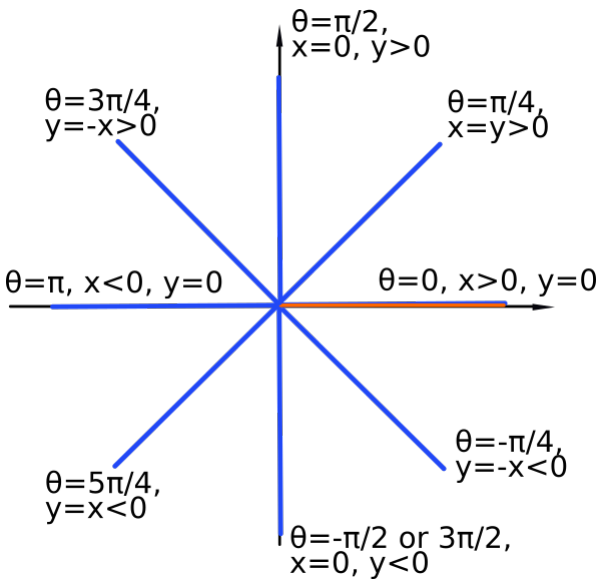
The value of θ which we need can be determined based on the position of the point in one of the quadrants: the first and the fourth quadrant correspond to the first solution for θ and the second and the third quadrant correspond to the second solution for θ.

For example, to determine the trigonometric representation of $2+7i$, compute r as $\sqrt{2^2+7^2} = \sqrt{53} \approx 7.28$. We have that $\tan\theta = \frac{7}{2}$. As $(2,7)$ is in the first quadrant, $\theta = \tan^{-1}\frac{7}{2} \approx 1.3$.

To determine the trigonometric representation of $-2+7i$, compute r as $\sqrt{2^2+7^2} = \sqrt{53} \approx 7.28$. We have that $\tan\theta = \frac{7}{-2}$. As $(-2,7)$ is in the third quadrant, $\theta = \pi + \tan^{-1}\frac{7}{-2} \approx 1.85$.

If the point is on one of the axis, the "wind rose" below can be used for finding the appropriate theta. The wind rose can also be used in the case when $x=0$ so that $\frac{y}{x}$ is not defined and the function $\tan^{-1}\frac{y}{x}$ is not defined at $x=0$.

- If a complex number is real and positive, then it is on the positive part of the x-axis and so $\theta = 0$.
- If a complex number is real and negative, then it is on the negative part of the x-axis and so $\theta = \pi$.
- If the real part is zero and the imaginary part is positive, then such number is on the positive part of the y-axis and so $\theta = \frac{\pi}{2}$.
- If the real part is zero and the imaginary part is negative, then such number is on the negative part of the y-axis and so $\theta = \frac{-\pi}{2}$.

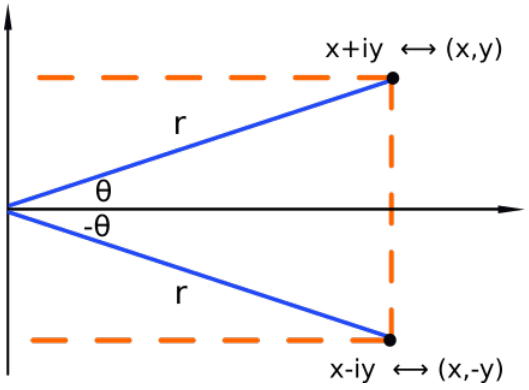


The figure above containing a"wind rose" exhibits some other scenarios for $x=y$ or $y=-x$. Exercise 36 present some specific examples.

For the converse (determining the algebraic form given the trigonometric form), the formulas $x = r\cos\theta$ and $y = r\sin\theta$ are more straightforward: they enable you to find x and y for any given r and θ.

For example, if $\theta = \frac{5\pi}{12}$ and $r=3$, we have that $x = 3\cos\frac{5\pi}{12} \approx 0.776$ and $y = 3\sin\frac{5\pi}{12} \approx 2.90$. Hence, $x+iy \approx 0.776 + 2.90i$.

If r and θ are polar coordinates of $x+iy$, then r and $-\theta$ are polar coordinates of the complex conjugate $x-iy$. This can be seen from geometric representation. Algebraically, this can be shown using the fact that $\cos(-\theta) = \cos\theta$ (cosine is an even function) and $\sin(-\theta) = -\sin\theta$



(sine is an odd function). Thus,

$$x - iy = r\cos\theta - ir\sin\theta = r\cos(-\theta) + ir\sin(-\theta).$$

Exercise 36. (1) Determine the moduli and the arguments given the following complex numbers in algebraic forms:

$$2,\ \ -2,\ \ 2i,\ \ 1+i,\ \ 1-i,\ \ -1-i.$$

(2) Determine the real and imaginary parts of the complex numbers given by their moduli and arguments:

$$\theta = \frac{\pi}{2}, r = 4; \qquad \theta = 0, r = 4; \qquad \theta = \pi, r = 4;$$

$$\theta = \frac{\pi}{4}, r = 2\sqrt{2}; \quad \theta = \frac{-\pi}{4}, r = 2\sqrt{2}; \quad \theta = \frac{3\pi}{4}, r = 2\sqrt{2}.$$

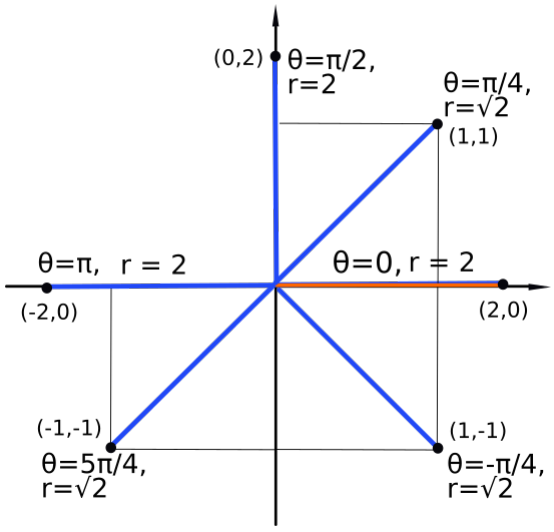
Solution. (1) You can use the graphical representation of the given numbers to determine their polar coordinate representation. The point $(2,0)$ is on the x-axis. Thus $\theta = 0$. The point $(2,0)$ is at a distance 2 from the origin, so $r = 2$. Alternatively, $r = \sqrt{2^2+0^2} = 2$ and $\theta = \tan^{-1}\frac{0}{2} = 0$.

The point $(-2,0)$ is on the negative part of x-axis and so $\theta = \pi$. The distance to the origin is 2, so $r = 2$.

The point $(0,2)$ is on the y-axis and so $\theta = \frac{\pi}{2}$. The distance to the origin is 2, so $r = 2$.

The point $(1,1)$ has $r^2 = 1^2 + 1^2 \Rightarrow r = \sqrt{2}$. From the graph, $\theta = \frac{\pi}{4}$. Alternatively, find θ as $\tan^{-1}\frac{1}{1} = \frac{\pi}{4}$.

The number $1-i$ is conjugated to $1+i$ so they have the same modulus and the opposite argument. Hence, $r = \sqrt{2}$ and $\theta = \frac{-\pi}{4}$.



The number $-1-i$ has $r^2 = (-1)^2 + (-1)^2 \Rightarrow r = \sqrt{2}$ and $\theta = \frac{5\pi}{4}$.

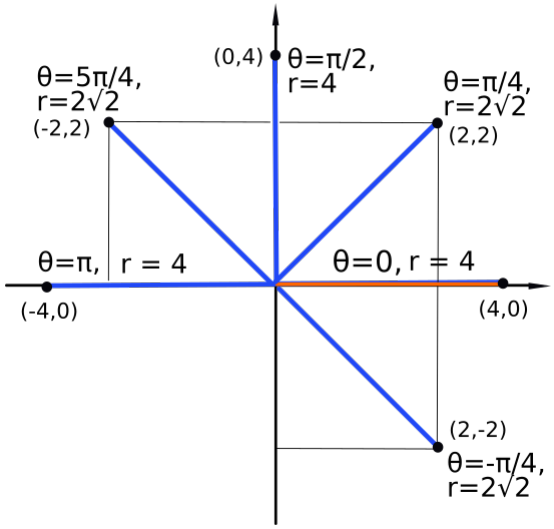
(2) In this problem also you can use the graph. Alternatively, use the formulas $x = r\cos\theta$ and $y = r\sin\theta$.

If $\theta = \frac{\pi}{2}$, the point is on the positive part of the y-axis. With $r = 4$, this gives us that $(x,y) = (0,4)$. Alternatively, $x = r\cos\theta = 4\cos\frac{\pi}{2} = 0$ and $y = r\sin\theta = 4\sin\frac{\pi}{2} = 4$.

If $\theta = 0$, the point is on the positive part of the x-axis. With $r = 5$, this gives us that $(x,y) = (5,0)$.

If $\theta = \pi$, the point is on the negative part of the x axis. With $r = 4$, we have that $(x,y) = (-4,0)$.

If $\theta = \frac{\pi}{4}$ and $r = 2\sqrt{2}$, $x = r\cos\theta = 2\sqrt{2}\cos\frac{\pi}{4} = 2\sqrt{2}\frac{1}{\sqrt{2}} = 2$ and



$y = r\sin\theta = 2\sqrt{2}\sin\frac{\pi}{4} = 2\sqrt{2}\frac{1}{\sqrt{2}} = 2$. Thus, $(x, y) = (2, 2)$.

If $\theta = \frac{-\pi}{4}$ and $r = 2\sqrt{2}$, $x = r\cos\theta = 2\sqrt{2}\cos\frac{-\pi}{4} = 2\sqrt{2}\frac{1}{\sqrt{2}} = 2$ and $y = r\sin\theta = 2\sqrt{2}\sin\frac{-\pi}{4} = 2\sqrt{2}\frac{-1}{\sqrt{2}} = -2$. Thus, $(x, y) = (2, -2)$.

Euler's formula and powers of complex numbers. Any power of i can be determined using the relation $i^2 = -1$. For example, $i^3 = i^2 i = -i$ and $i^{10} = (i^2)^5 = (-1)^5 = -1$. Note that $\frac{1}{i} = \frac{1\cdot(-i)}{i\cdot(-i)} = \frac{-i}{-i^2} = -i$, so i^{-3}, for example, is $\left(\frac{1}{i}\right)^3 = (-i)^3 = (-1)^3 i^3 = -(-i) = i$.

While it is easy to find powers of purely real or purely imaginary complex numbers, the algebraic form is not very handy for finding the powers of complex numbers in general because $(a+ib)^n \neq a^n + i^n b^n$. Using Euler's Formula, a complex number can be represented as a product, which helps with determining powers because $(ab)^n = a^n b^n$.

Euler's formula is stating that

$$e^{i\theta} = \cos\theta + i\sin\theta.$$

Euler's formula was proved (in a different form) for the first time by Roger Cotes in 1714, then rediscovered and popularized by Euler in 1748.

Euler proved that $e^{i\theta}$ and $\cos\theta + i\sin\theta$ are equal using the power series expansions of exponential, sine and cosine functions (if you took Calculus 3, you can write down the proof).

Euler's formula allows the following simplification

$$z = x + iy = r\cos\theta + ir\sin\theta = re^{\theta i}.$$

Using the trigonometric representation, the formulas for multiplication and division of two complex numbers become easier than if the algebraic form of complex numbers is used.

If $z_1 = r_1 e^{\theta_1 i}$ and $z_2 = r_2 e^{\theta_2 i}$, then

$$z_1 z_2 = r_1 e^{\theta_1 i} r_2 e^{\theta_2 i} = r_1 r_2 e^{i(\theta_1+\theta_2)}.$$

Euler's formula also produces an easy formula for the n-th power of a complex number $z = re^{\theta i}$,

$$z^n = \left(re^{\theta i}\right)^n = r^n e^{n\theta i}$$

as well as an easy switch from the exponential to the algebraic form (via the trigonometric form). For example, the algebraic form of $4e^{\frac{\pi}{3}i}$ is

$$4e^{\frac{\pi}{3}i} = 4(\cos\frac{\pi}{3} + i\sin\frac{\pi}{3}) = 4(\frac{1}{2} + i\frac{\sqrt{3}}{2}) = 2 + 2\sqrt{3}i.$$

Exercise 37. Determine the n-th power of the given complex numbers and given n. Express your answers in algebraic form.

(1) $z = 1 + i$, $n = 8$.
(2) $z = -1 - i$, $n = 6$.
(3) $z = 2 + 3i$, $n = 5$.

Solution. (1) For $z = 1 + i$, $\theta = \frac{\pi}{4}$ and $r = \sqrt{2}$ (see the first part of Exercise 36). Hence, $z = \sqrt{2}e^{\frac{\pi}{4}i}$. So,

$$z^8 = (\sqrt{2})^8 e^{8\frac{\pi}{4}i} = 16e^{2\pi i}.$$

To obtain algebraic form, note that

$$16e^{2\pi i} = 16(\cos 2\pi + i \sin 2\pi) = 16.$$

(2) For $z = -1-i$,$\theta = \frac{5\pi}{4}$ and $r = \sqrt{2}$ (see the first part of Exercise 36). Hence, $z = \sqrt{2}e^{\frac{5\pi}{4}i}$. So,

$$z^4 = (\sqrt{2})^4 e^{4\frac{5\pi}{4}i} = 4e^{5\pi i} = 4(\cos 5\pi + i \sin 5\pi) = -4.$$

(3) The number $2 + 3i$ has $r = \sqrt{2^2 + 3^2} = \sqrt{13} \approx 3.61$ and $\theta = \tan^{-1} \frac{3}{2} \approx 0.983$. Thus,

$$(2 + 3i)^5 = \sqrt{13}^5 e^{5 \cdot 0.983 i} = \sqrt{13}^5 e^{4.915i} \approx 609.34(\cos(4.915) + i \sin(4.915)) = 122.62 - 596.88i.$$

Using Euler's formula with $\theta = \pi$, we have that $e^{i\pi} = \cos \pi + i \sin \pi = -1 + 0 = -1$ so that the equation

$$e^{i\pi} = -1$$

holds. Many found this equation fascinating since the left side contains transcendental real numbers e and π and the imaginary number i and the right side, surprisingly, only an integer.

The field of complex numbers. The properties of addition and multiplication make $\mathbb{C}$ into a *field*. However, as opposed to the other number sets we encountered, there is no natural partial order on $\mathbb{C}$ which is compatible with addition and multiplication, so $\mathbb{C}$ is *not an ordered field*. As a consequence, there is no natural total order on $\mathbb{C}$: there are many incomparable complex numbers, like, for example $3 + 4i$ and $4 + 3i$. The modulus function still brings the notion of the distance between the two complex numbers and, in particular, the distance from the origin. So, although $3 + 4i$ and $4 + 3i$ are incomparable with each other, they are on the same distance $\sqrt{3^2 + 4^2} = 5$ from the origin.

Fundamental Theorem of Algebra. The field $\mathbb{C}$ has a valuable property – it is said to be *algebraically closed* meaning that every polynomial of degree n with complex coefficients has n solutions in $\mathbb{C}$. This statement (or one of its equivalent forms) is known as the Fundamental Theorem of Algebra.

This contrasts the situation with solutions in the set of real numbers. For example, a quadratic equation $ax^2+bx+c = 0$ can have two (possibly equal) real solutions or *no* real solutions. As opposed to this situation, in the complex plane, every quadratic equation has *exactly* two solutions (possibly equal).

Fundamental Theorem of Algebra implies that our work with the number sets is over – there is no polynomial equation without a solution outside of $\mathbb{C}$. So, $\mathbb{C}$ **does not need to be further enlarged** – we reached our goal of being able to solve any polynomial for all of its zeros (only fitting since we almost reached the end of the semester).

The part "of Algebra" in the name is a misnomer because this theorem is on solvability of equations, not really modern algebra. In addition, traditional proofs of this theorem rely on either real or complex analysis, geometry, or topology and, only fairly recently, algebra. The Complex Analysis course covers the proof of this theorem.

While we will not be finding n-solutions of just any polynomial of degree n, we can find solutions of one specific polynomial of degree n, namely the polynomial $z^n - a$. When solving

an equation of the form $z^n = a$ where a is a given complex number $a = re^{i\theta}$, we can obtain n solutions of the equation by the formula

$$\sqrt[n]{r}\, e^{\frac{(\theta+2k\pi)i}{n}} \quad \text{for } k = 0, 1, \ldots n-1.$$

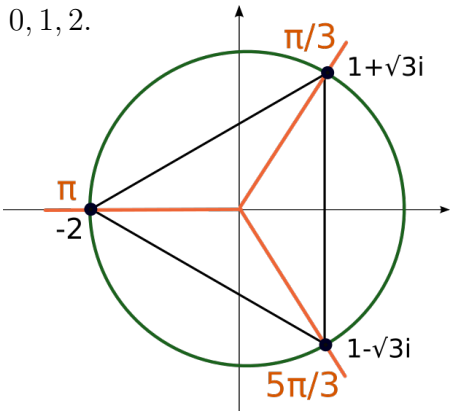
These solutions have a nice representation in the complex plane: they form the vertices of a regular polygon with n-sides inscribed in the circle of radius $\sqrt[n]{r}$ centered at the origin. We illustrate this in the following examples.

Example 9. Find all solutions of the following equations.

(1) $z^3 + 8 = 0$ (2) $z^5 = 32$ (3) $z^4 = 3 + 3i$

Solution. (1) We need to find all three solutions of the equation $z^3 = -8$. Note that -8 corresponds to the complex number $(-8, 0)$ which is on the negative side of the x-axis so $\theta = \pi$. The distance from $(-8, 0)$ to the origin is 8 so $r = 8$. Hence, the three solutions of the characteristic equation can be found by the formula

$$\sqrt[3]{8}\, e^{\frac{\pi+2k\pi}{3}i} = 2\, e^{\frac{\pi+2k\pi}{3}i} \quad \text{for } k = 0, 1, 2.$$



These three solutions form an equilateral triangle on the circle of radius 2 centered at the origin.

$k = 0 \Rightarrow z_0 = 2e^{\frac{\pi}{3}i} = 2(\cos\frac{\pi}{3} + i\sin\frac{\pi}{3}) = 1 + \sqrt{3}i$

$k = 1 \Rightarrow z_1 = 2e^{\frac{3\pi}{3}i} = 2e^{\pi i} = 2(\cos\pi + i\sin\pi) = -2$

$k = 2 \Rightarrow z_2 = 2e^{\frac{5\pi}{3}i} = 2(\cos\frac{5\pi}{3} + i\sin\frac{5\pi}{3}) = 1 - \sqrt{3}i.$

(2) We need to find all five solutions of $z^5 = 32$. Note that 32 corresponds to the complex number $(32, 0)$ which is on the positive side of the x-axis so $\theta = 0$. The distance from $(32, 0)$ to the origin is 32 so $r = 32$. Hence, the five solutions of the characteristic equation can be found by the formula

$$\sqrt[5]{32}e^{\frac{0+2k\pi}{5}i} = 2e^{\frac{2k\pi}{5}i} \quad \text{for } k = 0, 1, \ldots, 4.$$

These five solutions form a regular polygon with five sides on the circle of radius 2 centered at the origin.

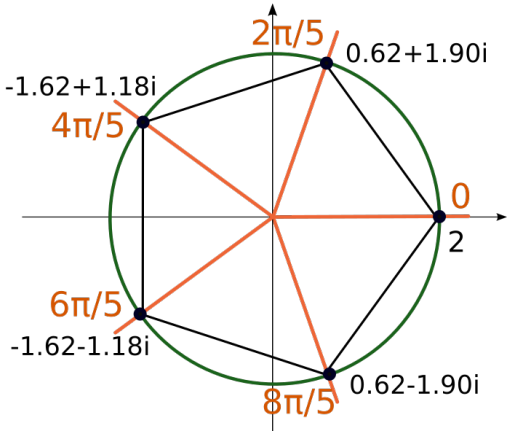
$k = 0 \Rightarrow z_0 = 2e^{0i} = 2,$

$k = 1 \Rightarrow z_1 = 2e^{\frac{2\pi}{5}i} = 2(\cos\frac{2\pi}{5} + i\sin\frac{2\pi}{5}) \approx 0.62 + 1.90i,$

$k = 2 \Rightarrow z_2 = 2e^{\frac{4\pi}{5}i} = 2(\cos\frac{4\pi}{5} + i\sin\frac{4\pi}{5}) \approx -1.62 + 1.18i,$

$k = 3 \Rightarrow z_3 = 2e^{\frac{6\pi}{5}i} = 2(\cos\frac{6\pi}{5} + i\sin\frac{6\pi}{5}) \approx -1.62 - 1.18i,$

$k = 4 \Rightarrow z_4 = 2e^{\frac{8\pi}{5}i} = 2(\cos\frac{8\pi}{5} + i\sin\frac{8\pi}{5}) \approx 0.62 - 1.90i.$



(3) Compute the modulus to be $r = \sqrt{3^2 + 3^2} = \sqrt{18}$ or $3\sqrt{2}$, and the argument to be $\theta = \tan^{-1}(\frac{3}{3}) = \tan^{-1}(1) = \frac{\pi}{4}$. Hence, $z = \sqrt{18}e^{\pi/4i}$.

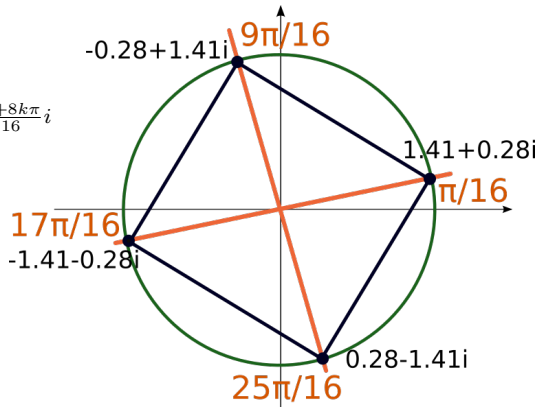
The four roots are obtained as

$$z_k = \sqrt[4]{\sqrt{18}e^{\frac{\pi/4+2k\pi}{4}i}} = 18^{1/8}e^{\frac{\pi+8k\pi}{16}i} \approx 1.435e^{\frac{\pi+8k\pi}{16}i}$$

for $k = 0, 1, 2, 3$. Thus,

$z_0 \approx 1.435e^{\pi/16i} = 1.435(\cos\frac{\pi}{16} + i\sin\frac{\pi}{16}) \approx 1.435(0.98 + i0.195) = 1.41 + 0.28i$

$z_1 \approx 1.435e^{9\pi/16i} = 1.435(\cos\frac{9\pi}{16} + i\sin\frac{9\pi}{16}) \approx 1.435(-0.195+0.98i) = -0.28+1.41i$



$z_2 \approx 1.435e^{17\pi/16i} = 1.435(\cos\frac{17\pi}{16} + i\sin\frac{17\pi}{16}) = 1.435(-0.98 - 0.195i) = -1.41 - 0.28i$

$z_3 \approx 1.435e^{25\pi/16i} = 1.435(\cos\frac{25\pi}{16} + i\sin\frac{25\pi}{16}) = 1.435(0.195 - 0.98i) = 0.28 - 1.41i$

Galois and solvability of polynomials. Let us mention a related and fascinating result. By the Fundamental Theorem of Algebra, a general polynomial of degree n has exactly n solutions. The word "general" here implies that the polynomial's coefficients are completely general numbers: $a_n \neq 0, a_{n-1}, \ldots, a_1, a_0$. The requirement that a_n is nonzero implies that the polynomial with those coefficients is indeed of degree n. For example, a general polynomial of degree 2 is $a_2x^2 + a_1x + a_0$. If we prefer a, b and c instead of a_2, a_1, a_0, such polynomial can be written as $ax^2 + bx + c$.

The Fundamental Theorem of Algebra states that a polynomial of degree n has n zeros, but it does not produce any method of actually *finding* those n zeros (such theorems are said to be **existential** and not **constructive**). If $n = 1$, we do know how to find the zero:

$$ax + b = 0 \Rightarrow x = \frac{-b}{a}$$

(note that $a \neq 0$ otherwise $ax + b$ would be a zero, not one, degree polynomial). For $n = 2$, there is also a well known formula

$$ax^2 + bx + c = 0 \quad \Rightarrow \quad x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

As it turns out, one can find similar formulas for cubic and quartic polynomials (the formulas are not nearly as short as for quadratic polynomial).

After those formulas have been discovered, mathematicians were looking for analogous formula for polynomials of degrees $n > 4$. However, no such formulas were found. That is when a young mathematician, **Évariste Galois**, stepped onto the stage circa 1820-1830 and managed to introduce the fundamentals of what is today known as Group Theory before he died (of an injury obtained in a duel) when he was only 20 years old.

While still in his teens, he showed that no formula for the solutions of a general polynomial of degree $n > 4$ exits. This shows that we can put a stop to our search of such formula - after Galois, we know that no such formula exists.

The idea of his proof is to relate the extension of the field which contains the coefficients of the polynomial with an object he introduced – **a group**. Today the groups of such field extensions are known as **Galois groups** and the correspondence between the field extensions and their Galois groups is known as the **Galois Theory** (although the term Galois Theory is used for other connections, not only those between fields and their Galois groups, presently). In the second part of the Modern Algebra course, you will see the proof of the statement that polynomials of degree larger than 4 cannot be "solved by radicals", i.e. that there is no formula involving the field operations, their inverses, the powers, and the radicals which describes zeros of such polynomials.

Complex-valued functions of a complex variable. A complex-valued function of a complex variable is a function $f(z) = f(x+iy) = u(x,y) + iv(x,y)$ where u, v are real-valued functions of two real variables x and y. For example, the **quadratic function** $f(z) = z^2 = (x+iy)^2 = x^2 + 2xyi - y^2$ is one such function. Its real part is $u = x^2 - y^2$ and its imaginary part is $v = 2xy$.

The **exponential function** e^z is another example. We have that

$$e^z = e^{x+iy} = e^x e^{iy} = e^x(\cos y + i \sin y)$$

so its real part is $e^x \cos y$ and the imaginary part $e^x \sin y$. We also have that the modulus is $r = e^x$ and that the argument is $\theta = y$.

The complex-valued **trigonometric functions** are defined via exponential function by

$$\sin z = \frac{1}{2i}(e^{iz} - e^{-iz}) \qquad \cos z = \frac{1}{2}(e^{iz} + e^{-iz})$$

The other trigonometric function can be defined via sine and cosine functions. For example, $\tan z$ can be defined as $\frac{\sin z}{\cos z} = \frac{e^{iz} - e^{-iz}}{i(e^{iz} + e^{-iz})}$.

With these definitions, the familiar identities on real numbers continue to hold for complex numbers. The following example illustrates this.

Example 10. Show that the following identities hold for any complex number z.

(1) $\cos z + i \sin z = e^{iz}$ (2) $\sin^2 z + \cos^2 z = 1$

Solution. (1)

$$\cos z + i \sin z = \frac{1}{2}(e^{iz} + e^{-iz}) + i\frac{1}{2i}(e^{iz} - e^{-iz}) = \frac{1}{2}\left(e^{iz} + e^{-iz} + e^{iz} - e^{-iz}\right) = \frac{1}{2}\left(2e^{iz}\right) = e^{iz}.$$

(2)

$$\sin^2 z + \cos^2 z = \left(\frac{1}{2i}(e^{iz} - e^{-iz})\right)^2 + \left(\frac{1}{2}(e^{iz} + e^{-iz})\right)^2 =$$

$$\frac{-1}{4}(e^{2iz} - 2 + e^{-2iz}) + \frac{1}{4}(e^{2iz} + 2 + e^{-2iz}) = \frac{1}{4}\left(-e^{2iz} + 2 - e^{-2iz} + e^{2iz} + 2 + e^{-2iz}\right) = \frac{1}{4}(4) = 1.$$

Practice Problems 11. (1) Determine the moduli and the arguments given the following complex numbers in algebraic forms:

$$-3i, \quad \sqrt{2} - \sqrt{2}i, \quad -\sqrt{3} + i, \quad -2 - i.$$

(2) Determine the real and imaginary parts of the complex numbers given by their moduli and arguments:

$$\theta = \frac{-\pi}{2}, r = 5; \qquad \theta = \frac{5\pi}{6}, r = 2; \qquad \theta = \frac{-2\pi}{3}, r = 3.$$

(3) Determine the n-th power of the given complex numbers and given n. Express your answers in algebraic form.
   (a) $z = -\sqrt{3} + i$, $n = 4$.
   (b) $z = -2 - i$, $n = 6$.

(4) Find all solutions of the following equations.

   (a) $z^3 = 8$ (b) $z^5 = -32$. (c) $z^4 = 3 - 3i$

(5) Show that the following identities hold for any complex number z.
   (a) $\sin^2 z = \frac{1}{2}(1 - \cos(2z))$ (b) $\cos^2 z = \frac{1}{2}(1 + \cos(2z))$

Solutions. (1) The complex number $-3i$ is on the negative part of y axis. Hence, $\theta = \frac{-\pi}{2}$. We have that $r = \sqrt{(-3)^2} = 3$.

The complex number $\sqrt{2} - \sqrt{2}i$ is on the $y = -x$ line and in the fourth quadrant. Hence, $\theta = \frac{-\pi}{4}$. We have that $r = \sqrt{\sqrt{2}^2 + (-\sqrt{2})^2} = \sqrt{2+2} = \sqrt{4} = 2$.

The complex number $-\sqrt{3}+i$ is in the second quadrant. Hence, $\theta = \pi + \tan^{-1}\frac{1}{-\sqrt{3}} = \pi + \frac{-\pi}{6} = \frac{5\pi}{6}$. The modulus is $r = \sqrt{(-\sqrt{3})^2 + 1^2} = \sqrt{4} = 2$.

The complex number $-2 - i$ is in the third quadrant. Hence, $\theta = \pi + \tan^{-1}\frac{-1}{-2} = \pi + \tan^{-1}\frac{1}{2} \approx \pi + 0.4636 \approx 3.605$. The modulus is $r = \sqrt{(-2)^2 + (-1)^2} = \sqrt{5} \approx 2.24$.

(2) If $\theta = \frac{-\pi}{2}$, the number is on the negative part of y-axis. As $r = 5, (x, y) = (0, -5)$. Alternatively, $x = 5\cos\frac{-\pi}{2} = 0$ and $y = 5\sin\frac{-\pi}{2} = -5$.

If $\theta = \frac{5\pi}{6}$ and $r = 2$, $x = r\cos\theta = 2\cos\frac{5\pi}{6} = 2 \cdot \frac{-\sqrt{3}}{2} = -\sqrt{3}$ and $y = r\sin\theta = 2\sin\frac{5\pi}{6} = 2 \cdot \frac{1}{2} = 1$. Thus, $(x, y) = (-\sqrt{3}, 1)$.

If $\theta = \frac{-2\pi}{3}$ and $r = 3$, $x = r\cos\theta = 3\cos\frac{-2\pi}{3} = 3 \cdot \frac{-1}{2} = \frac{-3}{2}$ and $y = r\sin\theta = 3\sin\frac{-2\pi}{3} = 3 \cdot \frac{-1}{\sqrt{2}} = \frac{-3}{\sqrt{2}}$. Thus, $(x, y) = (\frac{-3}{2}, \frac{-3}{\sqrt{2}})$.

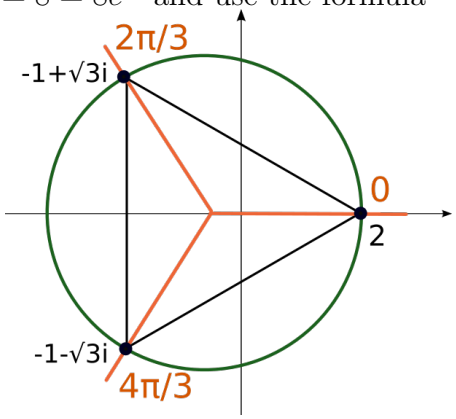
(3) (a) From problem (1), we have that $z = -\sqrt{3} + i = 2e^{5\pi/6i}$. Hence, $z^4 = 2^4 e^{4\cdot 5\pi/6i} = 16e^{10\pi/3i} = 16(\cos\frac{10\pi}{3} + i\sin\frac{10\pi}{3}) = 16(\frac{-1}{2} - \frac{\sqrt{3}}{2}) = -8 - 8\sqrt{3}i$.

(b) From problem (1), we have that $z = -2 - i \approx \sqrt{5}e^{3.605i}$. Hence, $z^6 \approx (\sqrt{5})^6 e^{6\cdot 3.605i} = 125e^{21.63i} = 125(\cos 21.63 + i\sin 21.63) = 125(-0.936 + 0.352) = -117 + 44i$.

(4) (a) One way to solve the equation is to note that $z^3 = 8 = 8e^{0i}$ and use the formula

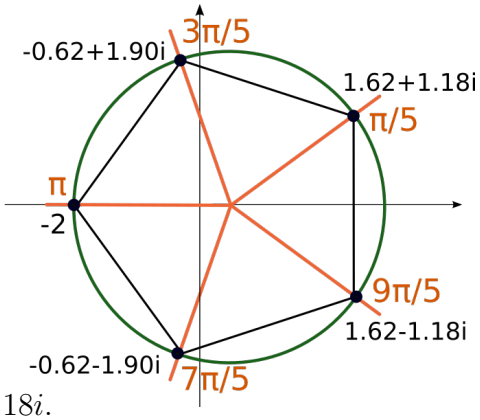
$$\sqrt[3]{8}\, e^{\frac{2k\pi}{3}i} = 2e^{\frac{2k\pi}{3}i}$$

for $k = 0, 1, 2$.
$k = 0 \Rightarrow z_0 = 2e^{0i} = 2$
$k = 1 \Rightarrow z_1 = 2e^{\frac{2\pi}{3}i} = 2(\cos\frac{2\pi}{3} + i\sin\frac{2\pi}{3}) = -1 + \sqrt{3}i$
$k = 2 \Rightarrow z_2 = 2e^{\frac{4\pi}{3}i} = 2(\cos\frac{4\pi}{3} + i\sin\frac{4\pi}{3}) = -1 - \sqrt{3}i$.



Alternatively, you can factor z^3-8 as $(z-2)(z^2+2z+4)$ and use the quadratic formula to find zeros of the second term. Obtain $z=2, z=-1\pm i\sqrt{3}$ which produce the same three solutions as using the first method.

(b) Determine the modulus to be $r=\sqrt{(-32)^2}=32$ and the argument to be $\theta=\pi$ (since $(-32,0)$ is on the negative side of the x-axis). So, $-32=32e^{\pi i}$ and $z_k=\sqrt[5]{32}e^{\frac{\pi+2k\pi}{5}i}=2e^{\frac{(2k+1)\pi}{5}i}$ for $k=0,1,\ldots,4$.



$k=0\Rightarrow \quad z_0=2e^{\frac{\pi}{5}i}=2(\cos\frac{\pi}{5}+i\sin\frac{\pi}{5})\approx 1.62+1.18i,$

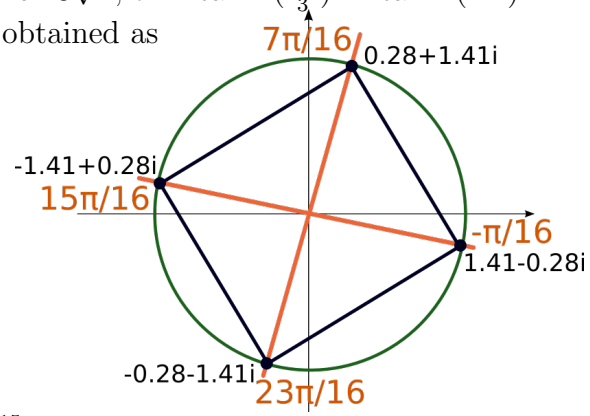
$k=1\Rightarrow \quad z_1=2e^{\frac{3\pi}{5}i}=2(\cos\frac{3\pi}{5}+i\sin\frac{3\pi}{5})\approx -0.62+1.90i,$

$k=2\Rightarrow \quad z_2=2e^{\frac{5\pi}{5}i}=2e^{\pi i}=2(\cos\pi+i\sin\pi)=-2,$

$k=3\Rightarrow \quad z_3=2e^{\frac{7\pi}{5}i}=2(\cos\frac{7\pi}{5}+i\sin\frac{7\pi}{5})\approx -0.62-1.90i,$

$k=4\Rightarrow z_4=2e^{\frac{7\pi}{5}i}=2(\cos\frac{9\pi}{5}+i\sin\frac{9\pi}{5})\approx 1.62-1.18i.$

(c) The modulus is $r=\sqrt{3^2+(-3)^2}=\sqrt{18}$ or $3\sqrt{2}$, $\theta=\tan^{-1}(\frac{-3}{3})=\tan^{-1}(-1)=\frac{-\pi}{4}$, so $z=\sqrt{18}e^{-\pi/4i}$. The four roots are obtained as



$z_k=\sqrt[4]{\sqrt{18}}e^{\frac{-\pi/4+2k\pi}{4}i}=18^{1/8}e^{\frac{-\pi+8k\pi}{16}i}\approx 1.435e^{\frac{-\pi+8k\pi}{16}i}$ for $k=0,1,2,3$. Thus,

$z_0\approx 1.435e^{-\pi/16i}=1.435(\cos\frac{\pi}{16}+i\sin\frac{\pi}{16})\approx 1.435(\ 0.98-i0.195)=1.41-0.28i$

$z_1\approx 1.435e^{7\pi/16i}=1.435(\cos\frac{7\pi}{16}+i\sin\frac{7\pi}{16})\approx 1.435(0.195+.98i)=0.28+1.41i$

$z_2\approx 1.435e^{15\pi/16i}=1.435(\cos\frac{15\pi}{16}+i\sin\frac{15\pi}{16})=1.435(-0.98+0.195i)=-1.41+0.28i$

$z_3\approx 1.435e^{23\pi/16i}=1.435(\cos\frac{23\pi}{16}+i\sin\frac{23\pi}{16})=1.435(-0.195-0.98i)=-0.28-1.41i$

(5) (a)

$$\sin^2 z=\left(\frac{1}{2i}(e^{iz}-e^{-iz})\right)^2=\frac{1}{-4}(e^{2iz}-2+e^{-2iz})=\frac{1}{4}\left(2-(e^{2iz}+e^{-2iz})\right)=$$
$$\frac{1}{2}\left(1-\frac{1}{2}(e^{2iz}+e^{-2iz})\right)=\frac{1}{2}(1-\cos(2z))$$

(b)

$$\cos^2 z=\left(\frac{1}{2}(e^{iz}+e^{-iz})\right)^2=\frac{1}{4}(e^{2iz}+2+e^{-2iz})=\frac{1}{4}(2+e^{2iz}+e^{-2iz})=$$
$$\frac{1}{2}\left(1+\frac{1}{2}(e^{2iz}+e^{-2iz})\right)=\frac{1}{2}(1+\cos(2z))$$

Department of Mathematics, Saint Joseph's University
Email address: lvas@sju.edu
URL: liavas.net