MATHEMATICS FROM SCRATCH

LECTURE NOTES FOR MATH 307: INTRODUCTION TO PROOFS

Contents

Introduction

What is truth?

If someone asks you for an unequivocally true statement, you might answer by giving one of the following:

(1) The sun rises from the east.
(2) My name is X.
(3) $6 + 10 = 16$.
(4) Propositions that are not false must be true.

However, each of these propositions, I claim, is not unequivocally "true" depending on your assumptions, definitions, and logical framework!

(1) could be false if you're on a different planet with a different sun. Indeed, the words "the sun" might not even make sense since a planet could have multiple suns in three-body system.

(2) is also problematic for less obvious reasons. For some people, "name" means what one's parents agreed to call one, and for others it's what appears on your government ID, and for others still it's what one choses

to be called by their acquaintances; all of which could be different in the following scenario: you were born to some biological parents who gave you a name X, but accidentally got switched for another baby (who was given another name Y) at the hospital and later in life you changed your name in your ID to Z, but everyone knows you by yet another name W.

(3) could be false if you are talking about numbers on a clock, in which case $6 + 10 = 4$. Similarly, the equation $1 + 1 = 1$ could be true in the following sense: adding one drop of water onto another drop of water gives one drop of water and not two.

(4) is more difficult... indeed, for most people this is an agreed upon rule called *the law of excluded middle*, yet some mathematicians avoid using this in their logical framework because it leads to deductions that cannot be explicitly verified. This will make more sense later in the course.

The punch line is that there is no such thing as universal truth! First, we have to agree on some common ground: a collection of propositions we all shall henceforth not contest and we shall declare them as "true" without justification. These are called *axioms*. For example, if we want to formalize our proposition (1), we could pose as an axiom "we live on Earth"

Next, we can only speak of the truth and falsity of a statement if all the words in that statement have been explicitly defined. For example, "the sun is that star which Earth orbits". Wait but what's "Earth"? We can fix this by defining "the Earth is that planet in the solar system"... and "a star is a bright celestial object in which hydrogen atoms fuse to form helium" and "and "hydrogen ...

You see the problem? We can define things only in terms of previously defined objects. But this is bound to be either circular, e.g. "the sun is a star..." and "a star is a sun..."; or it will go on indefinitely such as what we attempted above to formalize (1). Therefore, our only hope is to agree on some basic undefinable objects whose meaning we can only intuit and go from there. We will do this in Section 3.

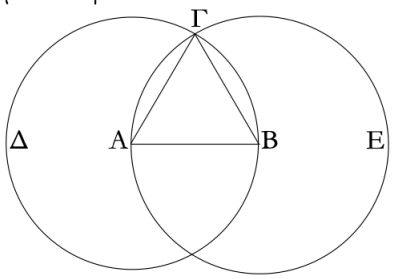
Now suppose we have defined all we need and clearly stated our axioms. How do we deduce new facts. That's the whole point after all. If mathematics is a game of chess, what we've done so far is set the board to the starting position and given each piece a name. Now we need to play, but for that we need rules to move from the starting position to more interesting ones. In mathematics, the rules of deduction from known true statements to new ones is also something we have to agree on. This is the role logic plays.

Example: Euclid's Elements. In ancient Alexandria, the Greek mathematician Euclid set the standards of mathematical rigor for the following two millennia when he wrote his book "Elements". It begins with 23 definitions (e.g. points, lines, circles, angles, etc.), 5 axioms/*postulates* (e.g. "for any two points, one can draw a straight line passing through them"), and 5 common notions (e.g. "things equal to the same thing are also equal to one another"). He then used these, along with the rules of logical deduction (which has long been studied in Greek philosophy and rhetoric to deduce mathematical theorems including the pythagorean theorem, the classification of Platonic solids, the infinitude of prime numbers, and much more. Below is a picture showing the proof of the first proposition (note the citations for each of the postulates, definitions, and common notions being used):

In the 18^{th} century, however, people realized one of Euclid's postulates was only true for geometry on a flat surface; and due to interest in non-flat geometries and other mathematical topics including algebra and analysis, a more unified foundations of modern mathematics were conceived beginning with the work of Cantor: Zermelo-Fraenkel Set Theory, which we will study in Section 3.

α΄.

Ἐπὶ τῆς δοθείσης εὐθείας πεπερασμένης τρίγωνον ἰσόπλευρον συστήσασθαι.



Ἔστω ἡ δοθεῖσα εὐθεῖα πεπερασμένη ἡ ΑΒ.

Δεῖ δὴ ἐπὶ τῆς ΑΒ εὐθείας τρίγωνον ἰσόπλευρον συστήσασθαι.

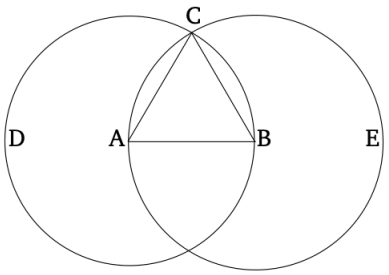
Κέντρῳ μὲν τῷ Α διαστήματι δὲ τῷ ΑΒ κύκλος γεγράφθω ὁ ΒΓΔ, καὶ πάλιν κέντρῳ μὲν τῷ Β διαστήματι δὲ τῷ ΒΑ κύκλος γεγράφθω ὁ ΑΓΕ, καὶ ἀπὸ τοῦ Γ σημείου, καθ᾽ ὃ τέμνουσιν ἀλλήλους οἱ κύκλοι, ἐπί τὰ Α, Β σημεῖα ἐπεζεύχθωσαν εὐθεῖαι αἱ ΓΑ, ΓΒ.

Καὶ ἐπεὶ τὸ Α σημεῖον κέντρον ἐστὶ τοῦ ΓΔΒ κύκλου, ἴση ἐστὶν ἡ ΑΓ τῇ ΑΒ· πάλιν, ἐπεὶ τὸ Β σημεῖον κέντρον ἐστὶ τοῦ ΓΑΕ κύκλου, ἴση ἐστὶν ἡ ΒΓ τῇ ΒΑ. ἐδείχθη δὲ καὶ ἡ ΓΑ τῇ ΑΒ ἴση· ἑκατέρα ἄρα τῶν ΓΑ, ΓΒ τῇ ΑΒ ἐστιν ἴση. τὰ δὲ τῷ αὐτῷ ἴσα καὶ ἀλλήλοις ἐστὶν ἴσα· καὶ ἡ ΓΑ ἄρα τῇ ΓΒ ἐστιν ἴση· αἱ τρεῖς ἄρα αἱ ΓΑ, ΑΒ, ΒΓ ἴσαι ἀλλήλαις εἰσίν.

Ἰσόπλευρον ἄρα ἐστὶ τὸ ΑΒΓ τρίγωνον. καὶ συνέσταται ἐπὶ τῆς δοθείσης εὐθείας πεπερασμένης τῆς ΑΒ. ὅπερ ἔδει ποιῆσαι.

Proposition 1

To construct an equilateral triangle on a given finite straight-line.



Let AB be the given finite straight-line.

So it is required to construct an equilateral triangle on the straight-line AB.

Let the circle BCD with center A and radius AB have been drawn [Post. 3], and again let the circle ACE with center B and radius BA have been drawn [Post. 3]. And let the straight-lines CA and CB have been joined from the point C, where the circles cut one another,† to the points A and B (respectively) [Post. 1].

And since the point A is the center of the circle CDB, AC is equal to AB [Def. 1.15]. Again, since the point B is the center of the circle CAE, BC is equal to BA [Def. 1.15]. But CA was also shown (to be) equal to AB. Thus, CA and CB are each equal to AB. But things equal to the same thing are also equal to one another [C.N. 1]. Thus, CA is also equal to CB. Thus, the three (straight-lines) CA, AB, and BC are equal to one another.

Thus, the triangle ABC is equilateral, and has been constructed on the given finite straight-line AB. (Which is) the very thing it was required to do.

† The assumption that the circles do indeed cut one another should be counted as an additional postulate. There is also an implicit assumption that two straight-lines cannot share a common segment.

FIGURE 1. Euclid's *Elements – Book I*, Prop.1 [E]

The logical framework used by Euclid, however, was flawless and we will turn our attention to its understanding (or rather a modern take on it) very soon.

Euclid's Elements is an example of what we shall call a *formal system*, i.e. a set of axioms along with a set of rules for deducing theorems. One may consider much more abstract formal systems such as the following one:

Example: the $pq-$system - Version I [H]. In this system, statements are strings of the symbols 'p', 'q', and '$-$'. We shall have infinitely many axioms[1], namely

$$x\,p-q\,x-\ \textit{is an axiom whenever } x \textit{ is any string consisting of hyphens only.}$$

[1]An infinite collection of axioms like this is sometimes called an *axiom schema*.

Moreover, we have the following rule of deduction:

Whenever $x\,p\,y\,q\,z$ is a theorem, then so is $x\,p\,y-q\,z-$ for any string x, y, z consisting of hyphens only.

Now, we can start making new theorems from old:

- $---p-q----$ holds (axiom).
- Thus, $---p--q------$.
- Thus, $---p---q--------$.

We have just written our first "proof" in the $pq-$system.

Example: the $pq-$system - Version II. In this system, statements are again strings of the symbols 'p', 'q', and '$-$'. But now we only have a single axiom:

$$-p-q--$$

and we have two rules of deduction

(1) Whenever $x\,p\,y\,q\,z$ is a theorem, then so is $x\,p\,y-q\,z-$ for any string x, y, z consisting of hyphens only.
(2) Whenever $x\,p\,y\,q\,z$ is a theorem, then so is $x-p\,y\,q\,z-$ for any string x, y, z consisting of hyphens only.

Exercise 0.1. *Which statements of the form $x\,p\,y\,q\,z$ are theorems in version 1 of the $pq-$system where x, y, z are strings consisting of hyphens only? Answer the same question for version 2.*

Of course, one can invent formal systems all day long, but the goal is to create a system that is useful/meaningful in some way. Euclid's system is capable of deducing facts of flat geometry and the theory of number that agree with our experience of the real world. Similarly, the $pq-$system is able to deduce some facts about numbers (though in a much more modest scope than Euclid's). The goal of this course, is to introduce you to a formal system that is capable of deducing *most* of the theorems that modern mathematics deals with along with gaining a lot of practice in the art of deducing new theorems from old within that system.

Course outline: In Section 1, we will look closely at language and logical equivalences in order to be able to articulate what we want to say precisely and avoid logical fallacies in our writing. Next, we will examine the logical rules of deduction and learn how to write formal proofs in Section 2. This will help us understand the structure of mathematical proofs in a controlled environment before we move on to deduce more interesting mathematical theorems. Section 3 marks the beginning of our mathematical story: set theory. There, we will introduce the axioms and basic definitions that we will use to build interesting mathematical structures from scratch. As an application, we will define the natural numbers and prove some of their basic properties in Section 4. In Section 5, we will examine a very useful proof technique that applies to statements about the natural numbers and look at many applications of the proof techniques we learned so far in various contexts. Section 6 studies functions and their properties, which will allow us to formalize the notion of counting to infinity and beyond. We will learn a general construction that will help us define the set of integer and rational numbers, examine their properties, and prove that some "numbers" are not rational in Section 7. In Section 8, we study more properties of the natural numbers; there we will see many examples of the proof techniques applied in clever ways, including Euclid's proof of the infinitude

FIGURE 2. Euclid of Alexandria

of prime numbers. Finally, in Section 9, we define the real numbers and study some of their properties, a prelude to real analysis.

1. Language and Logic

1.1. **Propositions and Connectives.** The language of mathematics, like any other language is expressed in sentences (a.k.a. propositions). Some propositions will be true and some will be false, and that will depend on which axioms we choose. But let us not concern ourselves for the moment of what these statements would look like and what our axioms are. For now, we will use everyday English sentences to illustrate how our logic would work.

Throughout this section, we will use the letters $P, Q, R, \ldots$ are variables/placeholders which can be substituted for by any proposition; we will call *terms*, and use them to build more complicated *propositional expressions*. For example, P can refer to the sentence "I love geometry" and Q can refer to "I love music"[2].

We can use old propositions to build new ones using *logical connectives*. Here are the most common logical connectives:

- NOT (denoted $\neg$): From the sentence P, we can build a new sentence $\neg P$ (vocalized as "not P" or "the negation of P"). In our example, the sentence $\neg P$ would refer to "I do not love geometry" (how bizarre!). As our first logic rule, if P is true then $\neg P$ is false and if P is false, then $\neg P$ is true. This is summarized in the following table, called the *truth table* of $\neg$

P	$\neg Q$
T	F
F	T

- AND (denoted $\wedge$): From P and Q, we may form their *conjunction* $P \wedge Q$ (vocalized as P and Q). In our example, $P \wedge Q$ would refer to the sentence "I love geometry, and I love music", or more simply we would say "I love geometry and music". Its truth table is as follows

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

Example. The sentence "I love music, but I don't love geometry" may be written as $Q \wedge \neg P$. Notice that the word "but" carries exactly the same meaning as "and" but we often use it in everyday language when there is some negation or even a connotation of negation, e.g. "math is fun but hard" carries the same meaning as "math is fun and hard".

Before we talk about OR, let us make an important distinction between two ways we use "or" in everyday language. If I say "I will go to a part or watch a movie tonight" what you probably guessed is that I will either go to a party or watch a movie **but not both**. This is called *exclusive OR*. But if I say "I want to buy book A or book B" I could mean that I want to buy at least one of the two books and possibly both. This is called *inclusive OR*. As a convention, whenever we say "or" in mathematics without qualification, we mean **inclusive** OR.

[2]The choice of these sentences was inspired by the following quote, often attributed to Pythagoras: "There is geometry in the humming of strings; there is music in the spacing of spheres".

- (Inclusive) OR (denoted $\vee$) From P and Q, we may form their *disjunction* $P \vee Q$ (vocalized as P or Q). In our example, $P \vee Q$ would refer to the sentence "I love music or geometry (or both)". Here is the truth table of OR (note the line in bold distinguishes inclusive OR from exclusive OR).

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

We can also make a truth table for any valid combination of the statements and connectives, e.g. here is a truth table for $\neg(P \wedge Q)$:

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

Exercise 1.1. *Make a truth table for $\neg P \vee \neg Q$. Do you notice anything?*

Definition 1.2. Two expressions A and B formed using logical connectives from the same terms $P, Q, R, \ldots$ are said to be equivalent if they have the same truth table values. We denote this by $A \equiv B$.

Example 1.3. **De Morgan's Laws**:

(1) $\neg(P \wedge Q) \equiv \neg P \vee \neg Q$.
(2) $\neg(P \vee Q) \equiv \neg P \wedge \neg Q$.

Another linguistic digression: often we use the word "if" in an incorrect or at best inaccurate way. Imagine the following scenario: your parent says "if you get good grades, we'll go on a nice vacation". You may point out that they did not say what happens if you get bad grades. In particular, getting bad grades and still going on vacation does not contradict the statement they said!

Let us examine this more closely. Let P be the sentence "You got good grades" and Q be "we'll go on a nice vacation". What your parent said is if P then Q (or symbolically, $P \to Q$). What your parent should have said is "we'll go on a nice vacation *only if* you get good grades". This is equivalent to saying if Q then P, i.e. the *converse* of the first statement! Indeed, saying "if we go on vacation, you got good grades" is the same as saying "we'll on vacation only if you got good grades".

Summary: $Q \to P$ **is equivalent to** P only if Q, but different from $P \to Q$.

- IF (denoted $\to$) From the sentences P and Q we can build the *implication* $P \to Q$ (vocalized "P implies Q" or "if P then Q") or its converse $Q \to P$, which are not equivalent to each other. In the proposition $P \to Q$, the term P is called the hypothesis of the conditional and the term Q is called the conclusion of the conditional. The following is their truth table:

P	Q	$P \to Q$	$Q \to P$
T	T	T	T
T	F	F	T
F	T	T	F
F	F	T	T

The following English expressions are all equivalent:
- If P then Q
- P implies Q
- Q if P
- P only if Q
- Q is necessary for P
- P is sufficient for Q
- Q whenever P

Exercise 1.4. *Design a proposition equivalent to $P \to Q$ using only (some of) $\wedge, \vee, \neg$.*

But now suppose your parent was a logic savvy and said "we'll go on a nice vacation only if you get a good grade". Then, you might be in trouble because it's possible that you get good grades and still not go on vacation! The solution is to demand that your parent also promise the other statement: "we'll go on a nice vacation only if you get a good grade". In other words you parent would be saying ""we'll go on a nice vacation *if and only if* you get a good grade"

- IFF (denoted $\leftrightarrow$) From the sentences P and Q we can build the *bi-conditional/bi-implication* $P \leftrightarrow Q$ (vocalized "P if and only if Q") its truth table is the following:

P	Q	$P \leftrightarrow Q$
T	T	T
T	F	F
F	T	F
F	F	T

Exercise 1.5. *Write the truth table for $(P \to Q) \wedge (Q \to P)$. Deduce that this is equivalent to $P \leftrightarrow Q$.*

Definition 1.6. A *tautology* is a statement that is always true and a *contradiction* is one that is always false.

Exercise 1.7. *Write the truth tables of $P \wedge \neg P$, of $\neg\neg P$, and of $P \vee \neg P$. Which one(s) is/are a tautology and which is/are a contradiction? Can you think of more examples of Tautologies and contradictions?*

Now, suppose we want to evaluate the truth table of a proposition formed using connectives joining three different terms, say P, Q, and R. For example, $(P \wedge Q) \to R$. Then, each of P, Q, R can be true or false independently of one another, resulting in 8 different possibilities. So, our truth table has 8 rows:

P	Q	R	$P \wedge Q$	$(P \wedge Q) \to R$
T	T	T	T	T
T	T	F	T	F
T	F	T	F	T
T	F	F	F	T
F	T	T	F	T
F	T	F	F	T
F	F	T	F	T
F	F	F	F	T

Question: how many rows does the truth table of a proposition involving n terms? **Answer:** 2^n.

Exercise 1.8. *Demonstrate each of the following logical equivalences using a truth table*

(1) $P \wedge (Q \vee R) \equiv (P \wedge Q) \vee (P \wedge R)$.
(2) $P \vee (Q \wedge R) \equiv (P \vee Q) \wedge (P \vee R)$.
(3) $P \wedge (Q \wedge R) \equiv (P \wedge Q) \wedge R$.
(4) $P \vee (Q \vee R) \equiv (P \vee Q) \vee R$.
(5) $(P \to Q) \wedge (Q \to R) \wedge (R \to P) \equiv (P \leftrightarrow Q) \wedge (Q \leftrightarrow R) \wedge (R \leftrightarrow P)$

If our goal is to deduce which propositions are true given the truth of some other propositions, truth tables seem like a very inefficient way to do so. That's where rules of deduction come in.

1.2. **Predicates and Quantifiers.** Sometimes we want our statements to contain variables to be substituted later on. For example, the phrase "x is a letter in the English alphabet" is true if $x = A$ and false if $x = \#$. We can denote this phrase by $P(x)$ to indicate its dependence on a variable x. Such a phrase is called a *predicate*. Notice that I avoided calling it a proposition because it is not yet one. Depending on what x is, it can be true or false, so we do not want to call such a phrase a proposition. Predicates allow us to examine many related propositions at once.

We may want to assert the truth or falsity of $P(x)$ for *all/some* x belonging to a certain set of values. If S is the set of values over which x can range, we denote the phrase "x belonging to S" symbolically as $x \in S$. We also denote the words "for all" by the symbol $\forall$ and "there exists" by the symbol $\exists$.

Example 1.9. Let A be the animal kingdom and $H(x)$ be the predicate "x is a human". Then,

- The statement $\forall x \in A, P(x)$ is false. In English, it says "for all x belonging to the animal kingdom, x is a human".
- But the statement $\exists x \in A, P(x)$ is true. It says "there exists a member of the animal kingdom who is a human".

The symbol $\forall$ is called the *universal quantifier*, whereas $\exists$ is called the *existential quantifies*.

Here is a more mathematical example[3]:

[3]The symbols $=$, 1, and -1 will only be defined in Section 3 but for now let's ignore that and use them intuitively. The same goes for the "set of natural numbers" $\mathbb{N}$

Example 1.10. $x^2 = 1$ is not a mathematical statement; it is grammatically incorrect in the language of mathematics because it can mean different things depending on what x is, and indeed its truth value cannot be determined. To make it precise, we can *quantify* x in any of the following ways:

- $\forall x \in \{1, -1\},\ x^2 = 1$, which is a true proposition;
- $\forall x \in \mathbb{N},\ x^2 = 1$, which is false;
- $\exists x \in \mathbb{N},\ x^2 = 1$, which is true.

In everyday language, we use many words to express universal/existential quantification. Universal quantification keywords include

- for [all], for every (e.g. "for x a human, x must die");
- if (e.g. ("if x is a human, then x must die");
- whenever, for, given (e.g. "given a human x, x must die");
- every, any (e.g. "any human x must die");
- a, an arbitrary (e.g. "a human x must die");
- let ... be (e.g. "let x be a human. x must die").

Existential quantification keywords include

- for some (e.g. "for some animal x, climate change will cause x to go extinct");
- there exists (e.g. "there exists an animal x such that climate change will cause x to go extinct");
- at least one (e.g. "climate change will cause at least one animal x to go extinct");
- some (e.g. "climate change will cause some animal x to go extinct");
- has a (e.g. "the set of animals has an x whom climate change will cause to go extinct").

Negation. What is the negation of "*everyone* loves geometry"? Answer: "*someone* does not love geometry". In general, we have

- $\neg\,[\forall x \in S,\ P(x)] \equiv \exists x \in S\,[\neg P(x)]$
- $\neg\,[\exists x \in S,\ P(x)] \equiv \forall x \in S\,[\neg P(x)]$

Exercise 1.11. *Negate the following sentences, noting the change in quantifiers:*

(1) No lazy students attend this school.
(2) Some numbers are cooler than others.
(3) Passing the test requires solving all of the problems.
(4) Whenever I sleep, I have weird dreams

Vacuous truth. Weird as it may sound, the statement "all flying horses are purple" is actually a true statement. This is called vacuous truth, because the set of "flying horses" is empty, and therefore, anything said about a flying horse is true. Another, perhaps slightly more intuitive, way to say this is "there isn't a single flying horse that isn't purple".

Here are some more examples of vacuously true statements:

- "All dragons that live in my closet can speak French".
- "All penguins that live in the Sahara Desert wear sunglasses".
- "All living people over 200 years old drink only lemonade".

Order of quantifiers matters! Consider the following two sentences:

- There is a traffic rule that all drivers break.
- All drivers break some traffic rule.

These have very different meanings, right? The former means that all drivers break the same traffic rule, whereas the latter means that all driver breaks some potentially different rules. Symbolically, let us denote by $P(x, y)$ the predicate "the driver x breaks the traffic rule y", and let D and R be the sets of all drivers and of all traffic rules, respectively; then the two sentences above are the following:

- $\exists y \in R\, \forall x \in D\ P(x, y)$.
- $\forall x \in D\, \exists y \in R\ P(x, y)$.

Exercise 1.12. *Write down each of the following sentences symbolically using quantifiers, choosing suitable predicates. Then, explain the difference in meaning between them:*

(1) A. Everyone has something they're good at. B. There's something that everyone is good at.
(2) A. Every student in the class asked at least one question. B. There is a question that every student in the class asked.
(3) A. Everyone loves someone. B. There is someone whom everyone loves.

Exercise 1.13. *Which of the following is a tautology for all predicates $P(x, y)$ (you may want to refer to the previous exercise to check your intuition):*

- $[\forall x \in X\, \exists y \in Y\ P(x, y)] \to [\exists y \in Y\, \forall x \in X\ P(x, y)]$
- $[\exists y \in Y\, \forall x \in X\ P(x, y)] \to [\forall x \in X\, \exists y \in Y\ P(x, y)]$

Homework 1.

- Read from [G]: pp. 1-17 and 28-32.
- Solve the following exercises from [G]: 1.1.3, 1.1.4, 1.3.18, 1.5.2, 1.5.3, 1.5.8
- Solve the following exercises from [DW]: 2.31, 2.32, 2.44, 2.45, 2.48

2. Formal Proofs

As we saw in the last section, we can discover tautologies by writing truth tables, but for sufficiently complicated propositions, it becomes quite tedious. Now, we will introduce a new tool to deduce new propositions from old. Let us begin with a definition.

Definition 2.1. A *rule of inference* is a tautology of the form $P \to Q$, where P and Q are some propositional expressions.

Example 2.2. The following rule of inference was called *Modus Ponens* in the Greek tradition: $[(P \to Q) \wedge P] \to Q$ (c.f. implication elimination below). For example, let $P(x)$ be the predicate "x is a man" and let $Q(x)$ be the predicate "x is mortal". Then, we have $\forall x, P(x) \to Q(x)$, and in particular $P(\text{“}Socrates\text{”}) \to Q(\text{“}Socrates\text{”})$. But since $P(\text{“}Socrates\text{”})$ hold (i.e. "Socrates is a man"), by Modus Ponens, we deduce that $Q(\text{“}Socrates\text{”})$ also holds (i.e. "Socrates is mortal").

Notice that the condition for the Modus Ponens implication itself contains an implication. To avoid confusion as to where the rule of inference is being applied, we use the following format to write our deductions (Note the citation of reasoning and line numbers and the placement of horizontal lines to separate premises from deductions):

1	$P \to Q$	Premise
2	P	Premise
3	Q	Modus Ponens: 1, 2

We will eventually have 10 rules of inference that will be used both formally and informally to prove statements throughout this course. We list them systematically below with some examples.

- $\wedge$-Elimination: This rule says that from the conjunction $P \wedge Q$, we may deduce either of the statements P or Q.

1	$P \wedge Q$	Premise
2	P	$\wedge$-Elim: 1
3	Q	$\wedge$-Elim: 1

- $\wedge$-Introduction: conversely, if we believe the two premises P and Q individually, we may deduce the statement $P \wedge Q$.

1	P	Premise
2	Q	Premise
3	$P \wedge Q$	$\wedge$-Intro: 1,2

- $\vee$-Introduction: If we believe either of the statements P or Q, then may deduce $P \vee Q$.

1	P	Premise
2	$P \vee Q$	$\vee$-Intro: 1

1	Q	Premise
2	$P \vee Q$	$\vee$-Intro: 1

With these simple rules of deduction, we can already start writing some formal proofs.

Definition 2.3. We say that a proposition Q follows from proposition P (denoted $P \models Q$) if the implication $P \to Q$ is a tautology, or equivalently, if Q can be deduced from P by applying a sequence of rules of inference.

Example 2.4. Below is a proof that $P \wedge Q \models P \vee Q$.

1	$P \wedge Q$	Premise
2	P	$\wedge$-Elim: 1
3	$P \vee Q$	$\vee$-Intro: 2

Sometimes, it will be useful to introduce subproofs relying on additional assumptions within a proof. In order to indicate this, we must have a way of determining the scope within which each additional assumption is made. We denote this by an increase in the indentation (further clarified by adding an extra vertical lines in the new scope's lines) as well as a horizontal line segment below the last line of assumptions within each scope. The next rule of inference will serve as an example which uses this notation.

- $\vee$-Elimination: suppose that we believe the statement $P \vee Q$, and suppose further that, if we assume either P or Q, we reach the same conclusion R. Then, the conclusion R must hold.

1	$P \vee Q$	Premise
2	P	Ass.
3	$\vdots$	
4	R	
5	P	Ass.
6	$\vdots$	
7	R	
8	R	$\vee$-Elim: 1, 2-4, 5-7

Example 2.5. Let us prove[4] that $(P \wedge Q) \vee (R \wedge S) \models (P \vee R)$.

[4]Note that this would require a 16 line truth table, but we can do it with a (more intuitive) formal proof with 8 lines instead.

1	$(P \wedge Q) \vee (R \wedge S)$	Premise
2	$P \wedge Q$	Ass.
3	P	$\wedge$-Elim: 2
4	$P \vee R$	$\vee$-Intro: 3
5	$R \wedge S$	Ass.
6	R	$\wedge$-Elim: 5
7	$P \vee R$	$\vee$-Intro: 6
8	$P \vee R$	$\vee$-Elim: 1, 2-4, 5-7

Exercise 2.6. *Prove the associativity laws for $\wedge$ and $\vee$ using formal proofs:*

(1) $P \wedge (Q \wedge R) \equiv (P \wedge Q) \wedge R$
(2) $P \vee (Q \vee R) \equiv (P \vee Q) \vee R$

Notation 2.7. We will use the symbol $\bot$ to denote a contradiction. It can be thought of as a shorthand for $P \wedge \neg P$. Similarly, we use the symbol $\top$ to mean a tautology, or a shorthand for $P \vee \neg P$.

- $\bot$-Introduction: we can deduce a contradiction whenever we deduce a statement P and its negation $\neg P$.

1	P	Premise
2	$\neg P$	Premise
3	$\bot$	$\bot$-Intro: 1, 2

- $\top$-Introduction: we can deduce the tautology $P \vee \neg P$ whenever we want without any constraints.

1	$P \vee \neg P$	$\top$-Intro

The importance of $\bot$-Introduction lies in the following sneaky strategy to prove mathematical claims, known as a **proof by contradiction**: Suppose we want to prove a statement P. Assume the opposite, i.e. assume $\neg P$; if we reach a contradiction, then, our assumption must have been false, so P must hold. This is formally achieved using the following two rules of inference.

- $\neg$-Introduction: If an assumption P leads to deducing a contradiction, we may conclude $\neg P$.

1	P	Ass.
2	$\vdots$	
3	$\bot$	
4	$\neg P$	$\neg$-Intro: 1-3

Example 2.8. Let us prove one of the two De Morgan's Law: $\neg(P \wedge Q) \equiv \neg P \vee \neg Q$. Notice that in order to prove an equivalence we need to separate proofs: one for $\neg(P \wedge Q) \models \neg P \vee \neg Q$ and one for $\neg P \vee \neg Q \models \neg(P \wedge Q)$.

1	$\neg(P \wedge Q)$	Premise
2	P	Ass.
3	Q	Ass.
4	$P \wedge Q$	$\wedge$-Intro: 2,3
5	$\perp$	$\perp$-Intro: 1,4
6	$\neg Q$	$\neg$-Intro: 3-5
7	$\neg P \vee \neg Q$	$\vee$-Intro: 6
8	$\neg P$	Ass.
9	$\neg P \vee \neg Q$	$\vee$-Intro: 8
10	$P \vee \neg P$	$\top$-Intro
11	$\neg P \vee \neg Q$	$\vee$-Elim: 10, 2-7, 8-9

1	$\neg P \vee \neg Q$	Premise
2	$P \wedge Q$	Ass.
3	P	$\wedge$-Elim: 2
4	Q	$\wedge$-Elim: 2
5	$\neg P$	Ass.
6	$\perp$	$\perp$-Intro: 3,5
7	$\neg Q$	Ass.
8	$\perp$	$\perp$-Intro: 4,7
9	$\perp$	$\vee$-Elim: 1, 5-6, 7-8
10	$\neg(P \wedge Q)$	$\neg$-Intro: 2-9

Exercise 2.9. *Prove the distributivity law for $\wedge$ over $\vee$ using formal proofs: $P \wedge (Q \vee R) \equiv (P \wedge Q) \vee (P \wedge R)$.*

So far, we were lucky with our use of $\neg$-Introduction because the statements we tried to prove with it were of the form $\neg P$ so we could just assume P and apply $\neg$-Intro directly. But, sometimes, we would need to prove a non-negated statement P, so if we assume $\neg P$ and arrive at a contradiction, our rule $\neg$-Intro says we can deduce the negation of our assumption, namely $\neg(\neg P)$. But we have no rule to identify $\neg\neg P$ as P yet! This is the infamous law of excluded middle, otherwise known as $\neg$-Elimination:

- $\neg$-Elimination: From $\neg\neg P$, you can deduce P.

1	$\neg\neg P$	Premise
2	P	$\neg$-Elim: 1

Example 2.10. Let us prove a disguised form of Modus Ponens: $(\neg P \vee Q) \wedge P \models Q$

1	$(\neg P \vee Q) \wedge P$	Premise
2	P	$\wedge$-Elim: 1
3	$\neg P \vee Q$	$\wedge$-Elim: 1
4	$\neg Q$	Ass.
5	$\neg P$	Ass.
6	$\perp$	$\perp$-Intro: 2, 5
7	Q	Ass.
8	$\perp$	$\perp$-Intro: 4, 7
9	$\perp$	$\vee$-Elim: 3, 5-6, 7-8
10	$\neg\neg Q$	$\neg$-Intro: 4-9
11	Q	$\neg$-Elim: 10

Remark 2.11. The Law of Excluded Middle (i.e. $\neg$-Elim) and proofs by contradiction in general, however intuitive, are strongly contested by *constructivist mathematicians*. Their issue is that it allows one to deduce the existence of objects without giving a construction (hence the name). For example, we will prove the following claim later in the course: "For any given language with finitely many letters, there exists a real number that cannot be described by that language". The proof goes as follows: assuming such a number does not exist, you get a contradiction; hence it must exist (even if I can't tell you what it is by definition!) The majority of mathematicians accept such proofs, however, but whenever you are able to avoid a proof by contradiction, you should opt for the direct proof.

Food for thought: As a mathematician, would you be a constructivist?

The following example shows another reason why proofs by contradiction are so dangerous if we make a mistake:

Example 2.12. Assuming a contradiction, we prove that all other statements are true! Symbolically, $\perp \models P$ for an arbitrary statement P. This is known as the *Principle of Deductive Explosion*!

1	$\perp$	Premise
2	$\neg P$	Ass.
3	$\perp$	Reiterate 1
4	$\neg\neg P$	$\neg$-Intro: 2-3
5	P	$\neg$-Elim: 4

Notice that P could mean that the sky is magenta and horses fly and the world was created by the any queen, for example! So, if we are to use proofs by contradictions (and we will!), we ought to be very careful not to accidentally assume any contradictions.

Theorem 2.13 (Gödel's Completeness Theorem)**.** *The connectives $\neg$ and $\vee$ are sufficient to express all propositional expressions. Moreover, if $P \models Q$ then there exists a proof of Q from P (the last phrase is symbolically denoted by $P \vdash Q$, vocalized "P proves Q") using the rules of inference above.*[5]

We will not attempt to prove or even formally state Gödel's Completeness Theorem, but it is comforting to know that it exists and that we are all set in our search for a strong foundation in our pursuit of proofs.

Remark 2.14. Naturally, we do not necessarily *need* rules of inference for $\rightarrow$ since we saw in Exercise 1.4 that we can express $\rightarrow$ using other connectives. In fact, all tautologies can be proved with fewer rules than the ones mentioned so far (can you think of a minimal set of rules of inference that are needed to prove all others?), but the more rules we have, the shorter the proofs become. Thus, we shall not shy away from mentioning two more rules.

- $\rightarrow$-Introduction: Suppose we can deduce Q assuming P. Then, we can deduce $P \rightarrow Q$.

1	P	Ass.
2	$\vdots$	
3	Q	
4	$P \rightarrow Q$	$\rightarrow$-Intro: 1-3

- $\rightarrow$-Elimination (a.k.a. Modus Ponens): If we know $P \rightarrow Q$ and we know P, we may deduce Q.

1	$P \rightarrow Q$	Premise
2	P	Premise
3	Q	

Example 2.15. Let us prove that $P \vee Q \equiv \neg P \rightarrow Q$.

[5] This is different from Gödel's much more famous (and much more difficult) Incompleteness Theorems, but it is the same Gödel.

1	$P \vee Q$	Premise
2	$\quad \neg P$	Ass.
3	$\quad\quad P$	Ass.
4	$\quad\quad \bot$	$\bot$-Intro: 2,3
5	$\quad\quad\quad \neg Q$	Ass.
6	$\quad\quad\quad \bot$	Reit. 4
7	$\quad\quad \neg\neg Q$	$\neg$-Intro: 5-6
8	$\quad\quad Q$	$\neg$-Elim: 7
9	$\quad\quad Q$	Ass.
10	$\quad\quad Q$	Reit. 9
11	$\quad Q$	$\vee$-Elim: 1, 3-8, 9-10
12	$\neg P \to Q$	*to*-Intro: 2-11

1	$\neg P \to Q$	Premise
2	$P \vee \neg P$	$\top$-Intro
3	$\quad P$	Ass.
4	$\quad P \vee Q$	$\vee$-Intro: 3
5	$\quad \neg P$	Ass.
6	$\quad Q$	$\to$-Elim: 1, 5
7	$\quad P \vee Q$	$\vee$-Intro: 6
8	$P \vee Q$	$\vee$-Elim: 2, 3-4, 5-7

Exercise 2.16. *Prove that* $(A \to B) \wedge (C \to D) \models (A \vee C) \to (B \vee D)$.

Finally, we need rules of inference to handle quantifiers and predicates

- $\forall$-Instantiation: From $\forall x \in S,\ P(x)$, we may deduce $P(a)$ for any $a \in S$.
- $\exists$-Instantiation: From $\exists x \in S,\ P(x)$, we may deduce $P(a)$ for some $a \in S$.

1	$\forall x \in S,\ P(x)$	Premise
2	$\quad \boxed{a}$	any $a \in S$
3	$\quad P(a)$	$\forall$-Instan: 1, 2

1	$\exists x \in S,\ P(x)$	Premise
2	$\quad \boxed{a}$	some $a \in S$
3	$\quad P(a)$	$\exists$-Instan: 1, 2

Remark 2.17. With the existential instantiation, special case must be taken: if we invoke $\exists$-Instantiation twice with two different quantified predicates, we cannot use the same letter for both instances. For example, if we are instantiating the statements $\exists x \in S,\ P(x)$ and $\exists x \in S,\ Q(x)$, we cannot say $P(a)$ and $Q(a)$, but rather we say $P(a)$ and $P(c)$ for example; this is because $P(x)$ and $Q(x)$ need not hold for the same x. This problem does not arise with universal instantiation, as we are indeed free to pick any element of S we like, including the same element multiple times.

Similarly, we have rules of inference to introduce quantifiers:

- $\forall$-Generalization: If a statement $P(a)$ holds for an **arbitrary** $a \in S$ (i.e. for **any** $a \in S$), we can deduce $\forall x \in S,\ P(x)$.
- $\exists$-Generalization: If a statement $P(a)$ holds for *some* $a \in S$, we can deduce $\exists x \in S,\ P(x)$.

1	$\boxed{a}$	any $a \in S$
2	$P(a)$	Premise
3	$\forall x \in S,\ P(x)$	$\forall$-Gen: 1, 2

1	$\boxed{a}$	some $a \in S$
2	$P(a)$	Premise
3	$\exists x \in S,\ P(x)$	$\exists$-Gen: 1, 2

Example 2.18. Let us prove that $\forall x \in S,\ P(x) \models \exists x \in S,\ P(x)$, but that the converse does not hold.

1	$\forall x \in S,\ P(x)$	Premise
2	$\boxed{a}$	any $a \in S$
3	$P(a)$	$\forall$-Instan: 1, 2
4	$\exists x \in S,\ P(x)$	$\exists$-Gen. 2, 3

To show that the converse does not hold it is **enough to find one counterexample**. For example, let $S = \{0, 1\}$, and let $P(x)$ be the predicate "$x = 0$". Then, $\exists x \in S,\ P(x)$ holds (take $x = 0$), but $\forall x \in S,\ P(x)$ is false (because $x = 1$ does not satisfy $x = 0$).

Remark 2.19. The above philosophy is completely general: **to prove a statement of the form $P \models Q$, we have to write a complete proof. But to show that $P \not\models Q$ (i.e. P does not imply Q), it is enough to find a single instance where P is true but Q is false.**

Example 2.20. Let us prove that one order of quantification is stronger than the other, namely

$$\exists x \in A,\ \forall y \in B\ \ P(x, y) \models \forall y \in B,\ \exists x \in A\ \ P(x, y)$$

1	$\exists x \in A,\ \forall y \in B,\ P(x, y)$	Premise
2	$\boxed{a}$	some $a \in A$
3	$\forall y \in B,\ P(a, y)$	$\exists$-Instan: 1, 2
4	$\boxed{b}$	any $b \in B$
5	$P(a, b)$	$\forall$-Instan: 3, 4
6	$\exists x \in A,\ P(x, b)$	$\exists$-Gen: 2, 5
7	$\forall y \in B,\ \exists x \in A,\ P(x, y)$	$\forall$-Gen: 4, 6
8	$\forall y \in B,\ \exists x \in A,\ P(x, y)$	Reit. 7 (no dependance on a).

Observe that an attempt to prove the converse in a similar fashion fails because of the potential dependence of a on the previously chosen b. Let's try and see where we get stuck:

1	$\forall y \in B,\ \exists x \in A,\ P(x,y)$	Premise
2	$\boxed{b}$	any $b \in B$
3	$\exists x \in A,\ P(x,b)$	$\forall$-Instan: 1, 2
4	$\boxed{a_b}$	some $a_b \in A$ (note that a potentially depends on b as it occurs within b's scope)
5	$P(a_b,b)$	$\exists$-Instan: 3, 4
6	$\forall y \in B,\ P(a_y,y)$	Ooops ... now we have many a's each depending on a different y, i.e. a predicate!
7		We cannot invoke an existential generalization on this type of statement,

Let us instead prove that this converse implication does not hold, i.e. that $\forall y \in B,\ \exists x \in A,\ P(x,y)$ does not imply $\exists x \in A,\ \forall y \in B\ \ P(x,y)$.

Exercise 2.21. *Show that* $\forall y \in B,\ \exists x \in A,\ P(x,y) \nvDash \exists x \in A,\ \forall y \in B\ \ P(x,y)$.

Remark 2.22. Notice in the example above, in the case of nested quantifiers, we have to instantiate the outer quantifier first before instantiating the inner one. Conversely, generalization happens from the innermost quantifier working outwards.

Exercise 2.23. *Show that* $\forall x \in S,\ (P(x) \wedge P(x) \to Q(x)) \models \forall x \in S,\ Q(x)$.

Homework:

Using formal proofs, demonstrate each of the following:

(1) $(P \to Q) \wedge (Q \to R) \models P \to R$.
(2) $\neg(P \vee Q) \models \neg P \wedge \neg Q$.
(3) $P \to Q \equiv \neg Q \to \neg P$ (this is called the **contrapositive**).
(4) $P \vee (Q \wedge R) \equiv (P \vee Q) \wedge (P \vee R)$.

Quantifiers of the same type commute, i.e.

(5) $\forall x \in A, \forall\, y \in B,\ P(x,y) \equiv \forall y \in B, \forall\, x \in A,\ P(x,y)$.
(6) $\exists x \in A, \exists\, y \in B,\ P(x,y) \equiv \exists y \in B, \exists\, x \in A,\ P(x,y)$.
(7) $\models P \to (Q \to P)$ (i.e. this is a tautology)
(8) Exercise 1.4 together with Example 2.10 show that $\to$-Elimination is not a necessary rule of inference to deduce all statements (provided we replace all instances of $P \to Q$ with the equivalent form $\neg P \vee Q$). Now, show that $\to$-Introduction is also redundant by giving a proof of $\neg P \vee Q$ from a subproof of Q assuming P (c.f. the $\to$-Intro rule above).

Problems 3 and 4 are worth 10 points each and all others are worth 5 points each.

3. Zermelo–Fraenkel Set Theory

We are now ready to begin defining our foundations of mathematics. We need to define everything precisely and, guided by our logic training, reason about these mathematical objects to find out their nature. But as everything is defined in terms of something else, we must start with some undefinable notion: a set.

Intuitively, a *set* is thought of as a collection of objects which we call its *members*, and we write $x \in A$ if x is a member of the set A. But then, what could x be? It will also be a set! In fact, everything will be a set and what distinguishes them is the collection of members they contain.

When we say everything is a set, we must be very careful, though. As we will soon see, if we allow any collection to be treated as a set, we get some unresolvable paradoxes. For example, the collection of all sets cannot be formally treated as a set if we want to avoid such paradoxes. One of the most famous paradoxes that may arise if we naïvely assume any collection is a set is Russells Paradox:

Russell's Paradox : "There is a barber in a village who shaves every person who does not shave themself and no one else. Does the barber shave himself?"

If the barber shaves himself, then by his own rule he must not shave himself; but if he does not, then he must! There are many formulations of equivalent paradoxes, but they are all abstractly a contradiction of the form

$$S = \{x \text{ such that } x \notin x\}. \text{ Then, } S \in S \leftrightarrow S \notin S.$$

If such an object as S above was to be admitted as a set, our theory of sets will contain a contradiction, which, according to the Principle of Deductive Explosion, would let us prove any statement we like! So, the solution is to not admit such objects in our theory. But how do we prevent them? We need to do better than just using the intuitive meaning of a collection to decide what is a set and what is not. Let us start from one set, namely, the *empty set*, denoted $\emptyset$, and build more sets from it while being careful not to create any paradoxes along the way.

Axiom I (Empty Set): There exists a set with no elements, i.e. $\exists x \, \forall y \, (y \notin x)$.

The phrase $y \notin x$ is just an abbreviation to $\neg(y \in x)$. Note that the axiom says that an empty set exists, but it doesn't rule out the existence of multiple distinct empty set. But in the world of sets, we would like the contents (i.e. members) of a set to completely determine what it is. This is our second axiom.

Axiom II (Equality): Two sets are the same if they have the same members, i.e.

$$\forall x \, \forall y \, [\forall z \, (z \in x \leftrightarrow z \in y) \rightarrow x = y].$$

Proposition 3.1. *There exists a unique empty set.*

Proof. The existence of such a set is the content of Axiom 1. To show that it is unique, suppose that x and x' are two empty sets. Then, for every z, $z \in x$ if and only if $z \in x'$ since both conditions are never satisfied. Thus, by the Axiom of Equality, $x = x'$. □

Therefore, we are henceforth justified in calling it *the* empty set and giving it the symbol $\emptyset$. Okay, but to get anywhere exciting we need more than just the empty set, and so far we have no way of making any new sets that are not empty. Let us fix this.

Axiom III (Pairing): Given sets x and y, there exists a set A whose members are exactly x and y, i.e.

$$\forall x\, \forall y\, \exists A\, \forall z\ [z \in A \leftrightarrow (z = x \vee z = y)].$$

Notation 3.2. When we want to list the members of a given set, we shall list them within braces (i.e. $\{\}$) and separate them by commas. For example, the Axiom of Pairing says that for any sets x and y we have a set $A = \{x, y\}$.

Example 3.3. Let's try to use this to create new sets! The only set we have so far to substitute for x and y is the empty set, so let's use that: applying the axiom of pa $x = y = \emptyset$, we get a set $A = \{\emptyset, \emptyset\} = \{\emptyset\}$, where the last equality is due to the Axiom of Equality (exercise!). In general, if we take $x = y$, we can create a set $\{x\}$ containing a single element. Such a set is called a **singleton**.

Example 3.4. We now have two different sets, namely $\emptyset = \{\}$ and $\{\emptyset\} = \{\{\}\}$. We can apply the axiom of pairing again, but now with $x = \emptyset$ and $y = \{\emptyset\}$ to get a set with two elements: $\{\emptyset, \{\emptyset\}\}$.

Notation 3.5. We will define $0 := \emptyset$, $1 := \{\emptyset\}$, and $2 := \{\emptyset, \{\emptyset\}\}$. This is just notation (for now at least) to make it easier to write and read these sets

Exercise 3.6. *Construct the sets* $\mathscr{S} = \{2, \{2\}\}$.

Exercise 3.7. *Construct a sequence of sets* $x_1 \in x_2 \in x_3 \in \dots$.

There is a limitation to the sets we can create so far though: they cannot have more than two members. The next axiom will fix this limitation.

Axiom IV (Union): Given a set $\mathscr{S}$ whose elements are sets, there is a set U consisting of all those elements that are members of some member of $\mathscr{S}$, i.e.

$$\forall \mathscr{S}\, \exists U\, \forall x\ [x \in U \leftrightarrow \exists A\, (x \in A \wedge A \in \mathscr{S})]$$

Example 3.8. Let us create a set with 3 elements: applying the Axiom of Union to the set $\mathscr{S}$ from Exercise 3.6, we get a set $\{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\} = \{0, 1, 2\} =: 3$.

The (unique) set U described in the Axiom of Union is called the *union over* $\mathscr{S}$ or the *union of elements of* $\mathscr{S}$, and is denoted $\bigcup \mathscr{S}$. For example, Example 3.8 says that the set 3 is the union of 2 and $\{2\}$, or equivalently 3 is the union over $\{2, \{2\}\}$.

Notation 3.9. Given sets A and B, it is often more convenient to write $A \cup B$ instead of $\bigcup\{A, B\}$, so we can use either notation interchangeably.

Definition 3.10. A set A is said to be a subset of B (denoted $A \subseteq B$) if all members of A are also in B, i.e. $\forall x\, (x \in A \to x \in B)$. When $A \subseteq B$ but $A \neq B$, we write $A \subsetneq B$[6].

Exercise 3.11. *Construct a sequence of distinct sets* $x_1 \subsetneq x_2 \subsetneq x_3 \subsetneq \dots$. *Hint: consider Example 3.8.*

The following proposition offers a very useful characterization of equality of sets.

Proposition 3.12. *Two sets A and B are equal if and only if $A \subseteq B$ and $B \subseteq A$.*

[6]some authors use the symbol $\subset$ which, depending on the author might mean $\subseteq$ or $\subsetneq$. We avoid this ambiguity by not using the symbol $\subset$ at all.

Proof. First, suppose $A = B$. Then, all elements of A are in B, so $A \subseteq B$; and all elements of B are in A, so $B \subseteq A$. Conversely, suppose $A \subseteq B$ and $B \subseteq A$. Then, elements of A belong to B and vice versa, so the two sets contain exactly the same elements, i.e. they are equal. □

Doing Exercise 3.11, you may have accidentally discovered Von Neumann's definition of the natural numbers:

Definition 3.13. Define $0 = \emptyset$, and let the successor of n which we denote by $s(n)$ be the set $n \cup \{n\}$. Thus,

$$\begin{aligned} 1 &:= s(0) = \emptyset \cup \{\emptyset\} = \{\emptyset\} = \{0\} \\ 2 &:= s(1) = \{\emptyset\} \cup \{\{\emptyset\}\} = \{\emptyset, \{\emptyset\}\} = \{0, 1\} \\ 3 &:= s(2) = \{\emptyset, \{\emptyset\}\} \cup \{\{\emptyset, \{\emptyset\}\}\} = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\} = \{0, 1, 2\} \\ &\vdots \end{aligned}$$

Now we would like to be able to talk about the set of all natural numbers $\mathbb{N} = \{0, 1, 2, 3, ...\}$. But so far, all the axioms we have allow us to construct finite sets only; we can construct infinitely many sets, but each of them must contain finitely many elements. Thus, we need the following axiom:

Axiom V (Infinity): There exists a set I with the following properties: $\emptyset \in I$ and, whenever $x \in I$, then $s(x) := x \cup \{x\} \in I$, i.e.

$$\exists I \left[(\emptyset \in I) \wedge (\forall x \, (x \in I \to x \cup \{x\} \in I))\right].$$

Definition 3.14. A set I satisfying $\emptyset \in I$ and $x \in I \to s(x) \in I$ for all x is called *an inductive set.*

Note, however, that the set I guaranteed by the Axiom of Infinity need not be our desired set $\mathbb{N} = \{0, 1, 2, 3, \dots\}$. For example, for any given set x, the set $I = \{0, 1, 2, 3, \dots\} \cup \{x, s(x), s(s(x)), s(s(s(x))), \dots\}$ is also an inductive set but $\mathbb{N} \subsetneq I$. In general, any inductive set I must contain a copy of $\mathbb{N}$ as a subset since $0 = \emptyset \in I$ by definition and hence, so do all its successors, i.e. $1, 2, 3, \dots$. So in a sense, we are after the smallest possible inductive set!

Definition 3.15. Let $\mathbb{N}$ by the set consisting of all x which lie in every inductive set. We call it the set of *natural numbers.*

Definition 3.16. (Set operations)

- The *intersection* $A \cap B$ of the sets A and B is the set consisting of all elements contained in both A and B. More generally, if $\mathscr{S}$ is a set of sets, we define $\bigcap \mathscr{S}$ as the set consisting of all elements which are contained in every member set of $\mathscr{S}$. So, as with unions, $\bigcap\{A, B\} = A \cap B$.
- Two sets A and B are said to be *disjoint* if $A \cap B = \emptyset$.
- The *set difference* $A \setminus B$ of a set A minus a set B is the set consisting of those elements which belong to A but not to B.

Notation 3.17. When a set A is a subset of a big set U and U is easily understood from context, we use the notation $A^c := U \setminus A$, and call it *the complement of* A. This should be avoided if the set U is not clear.

Exercise 3.18. *Prove the following identities for any sets A, B, C which are subsets of some set U*

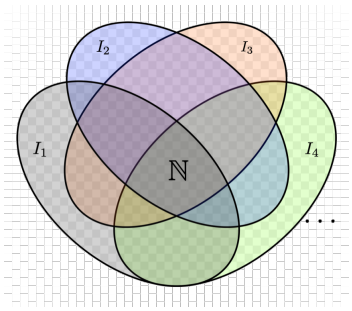


FIGURE 3. The natural numbers lying within every inductive set

- $A \cup B = B \cup A$.
- $A \cap B = B \cap A$.
- $A \cup (B \cup C) = (A \cup B) \cup C$.
- $A \cap (B \cap C) = (A \cap B) \cap C$.
- $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.
- $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.
- $(A \cup B)^c = A^c \cap B^c$.
- $(A \cap B)^c = A^c \cup B^c$.

Remark 3.19. This exercise should remind you of some logical equivalences. Indeed, $\cup$, $\cap$, and $\bullet^c$ play a very similar role in the theory of sets as the connectives $\vee$, $\wedge$, and $\neg$, respectively, do in propositional logic. To see why, the reader is invited to translate the propositions "$x \in A \cup B$", "$x \in A \cap B$", and "$x \in A^c$" to symbolic propositional expressions in terms of the propositions "$x \in A$" and "$x \in B$".

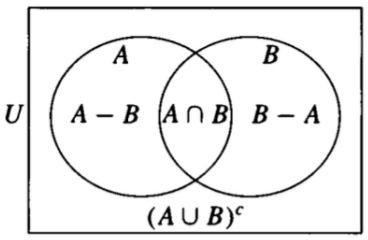


FIGURE 4. *Venn diagram* illustrating some set operations.

Even though we have been talking about intersections and differences, we did not prove that such sets exist in general. Our next axiom will help us do this. Both $A \cap B$ and $A \setminus B$ are naturally specified by predicates:

$$A \cap B = \{x : (x \in A) \wedge (x \in B)\} \quad \text{and} \quad A \setminus B = \{x : (x \in A) \wedge x \notin B\}.$$

So it is enough to have an axiom which says allows us to form sets whose elements are those making a certain predicate true.

Axiom VI (Comprehension – Attempt 1): Given a predicate $\varphi(x)$ there exists a set A consisting of those x satisfying $\varphi(x)$. i.e. given a predicate $\varphi(x)$, $\exists A \forall x\ (x \in A \leftrightarrow \varphi(x))$.

There are two issues with this axiom. First, is that it's not a single axiom but rather one axiom for each predicate, which is why we should call it *Axiom Schema of Comprehension*. This is not a problem since no one is stopping us from having infinitely many axioms in our theory.

The second issue is much more dangerous. Consider the predicate $\varphi(x)$: "$x \notin x$". Using the Axiom Schema of Comprehension, we have now allowed ourselves to create the paradoxical set of Russell, so our theory is doomed!

The solution is to only allow predicates to specify **a subset of an already constructed set**. Let's try again:

Axiom VI (Schema of Restricted Comprehension): Given a predicate $\varphi(x)$ and a set U, there exists a set A whose elements are those $x \in A$ satisfying $\varphi(x)$, i.e. given $\varphi(x)$,

$$\forall U\, \exists A\, \forall x\ [x \in A \leftrightarrow (x \in U) \wedge \varphi(x)]$$

Russell's problematic set cannot be thought of as a subset of any of the sets thus far constructed, so it seems that we are safe from contradictions for now. The Axiom Schema of Restricted Comprehension is sometimes also called the *Axiom Schema of Specification* because it allows us to specify subsets of a given set based on some predicate.

Proposition 3.20. *The intersection $A \cap B$ and the set difference $A \setminus B$ always exist for any sets A and B.*

Proof. $A \cap B = \{x \in A : x \in B\}$, so taking $U = A$ and $\varphi(x)$: "$x \in B$" in the Axiom Schema of Restricted Comprehension yields the desired set. Similarly, $A \setminus B = \{x \in A : x \notin B\}$. □

In general, we are allowed to define sets of the form $\{x \in U : \varphi(x)\}$ as long as U is already a set.

Exercise 3.21. *Prove that the intersection over any set $\mathscr{S}$ of sets exists.*

Exercise 3.22. *Prove that the set of natural numbers as defined in Definition 3.15 exists.*

The Axiom Schema of Restricted Comprehension allows us to define a subset of any given set consisting of elements obeying some predicate. But we would also like to talk about the set of *all* subsets of a given set.

Axiom VII (Power Set): Given a set A, there is a set (called the *power set* of A) whose elements are all the subsets of A, i.e.

$$\forall A\, \exists P\, \forall x\ (x \in P \leftrightarrow x \subseteq A).$$

We denote the power set of A by $\wp(A)$.

Example 3.23. Let $A = \{0, 1, 2\}$. Then, $\wp(A) = \{\emptyset, \{0\}, \{1\}, \{2\}, \{0, 1\}, \{0, 2\}, \{1, 2\}, \{0, 1, 2\}\}$.

Remark 3.24. For any set A, we have $\emptyset \subseteq A$ (vacuously true, why?) and $A \subseteq A$.

We wish to define *Cartesian products* of sets A and B, i.e. a set $A \times B := \{(x, y) : x \in A,\ y \in B\}$, or, in other words, the set of all *ordered pairs* (x, y) where x and y are arbitrary elements of A and B, respectively. Before we do that, let us define what we mead by **ordered** pairs.

Definition 3.25. The *ordered pair* (x, y) is by definition the set $\{\{x\}, \{x, y\}\}$.

Exercise 3.26. *Prove that if x and y is a set, then so is (x, y).*

This is just a technical definition to make x and y not on equal footing somehow, and thereby distinguishing them as first component and second component; indeed, unlike $\{x, y\} = \{y, x\}$, we have $(x, y) := \{\{x\}, \{x, y\}\} \neq \{\{y\}, \{y, x\}\} =: (y, x)$.

Proposition 3.27. *The* Cartesian product $A \times B := \{(x, y) : x \in A,\, y \in B\}$ *is a set for any sets A and B.*

Proof. The Axiom of Union guarantees the existence of $A \cup B$. Moreover, for any ordered pair $(x, y) = \{\{x\}, \{x, y\}\}$, we have $(x, y) \subseteq \wp(A \cup B)$. Therefore, the set of all such pairs forms a subset $A \times B \subseteq \wp(\wp(A \cup B))$, which we can define by applying the Power Set Axiom twice to first define $\wp(\wp(A \cup B))$ and then apply the Axiom of Restricted Comprehension to define the desired subset. □

Definition 3.28. A *function* from a set A to a set B is a subset F of $A \times B$ satisfying the following conditions:

- for each $x \in A$, there exists $y \in B$ such that $(x, y) \in F$;
- if $(x, y) \in F$ and $(x, y') \in F$, then $y = y'$.

In other words, each $x \in A$ is the first component of a *unique* pair $(x, y) \in F$. We say A is the domain if F and B is the codomain of F and write $F : A \to B$ to concisely list this data. We also write $F(x) = y$ whenever $(x, y) \in F$. The *range/image* of F is the set $\mathrm{Im}\,(F) := \{y \in B : \exists x\,(x \in A \wedge (x, y) \in F)\}$.

Since the image of a function is a subset of the codomain defined by a predicate, it follows that it is also a set by the Axiom Schema of Restricted Comprehension.

Example 3.29. The following are two equivalent ways of describing the same function $F : \{0, 1, 2, 3\} \to \{0, 4, 5\}$: $F = \{(0, 0), (1, 5), (2, 5), (3, 0)\}$, or equivalently $F(0) = 0$, $F(1) = 5$, $F(2) = 5$, and $F(3) = 0$.

Example 3.30. The successor operation of Definition 3.13 defines a function $s : \mathbb{N} \to \mathbb{N}$ given by $s(n) = n \cup \{n\}$.

Example 3.31. For any set A, there is a function $\mathrm{Id} : A \to A$ defined by $\mathrm{Id}(x) = x$ for all $x \in A$.

Example 3.32. Given a set A and a subset $B \in A$, there is a function $\chi_B : A \to \{0, 1\}$, called the characteristic function of B, defined as follows $\chi_B(x) = 0$ if $x \notin B$ and $\chi_B(x) = 1$ if $x \in B$.

Exercise 3.33. *Given a set A, how many functions (if any) exist from $\emptyset$ to A? How many functions (if any) exist from A to $\emptyset$?*

Sometimes, mathematicians want images of a sort of "generalized functions" to exist even when they are not defined in terms of pre-existing sets for domain and codomain. Here is how this is done:

Axiom VIII (Schema of Replacement): Given a predicate $\varphi(x, y)$ such that $(\varphi(a, b) \wedge \varphi(a, b')) \to (b = b')$, then there exists a set R consisting of all y such that, for some y, $\varphi(x, y)$ is true.

We will never use this axiom in this class since we will never need these "generalized functions", but I mention it just for the sake of completeness.[7]

The following axiom is sometimes needed to avoid potential self-referential paradoxes.

Axiom IX (Regularity): For any nonempty set A there exists $x \in A$ such that $x \cap A = \emptyset$.

Proposition 3.34. *No set can be a member of itself.*

Proof. Suppose for the sake of contradiction that there is a set A with $A \in A$. Now, applying the Axiom of Regularity to the set $\{A\}$ (which is indeed nonempty), we conclude that there is some $x \in \{A\}$ with $x \cap \{A\} = \emptyset$. But x must equal A since that's the only element of $\{A\}$. Thus, $A \cap \{A\} = \emptyset$. But by assumption $A \in A$ and also $A \in \{A\}$ so that $A \in A \cap \{A\}$, contradicting its emptiness. □

Corollary 3.35. *The collection of all sets is not a set.*

Proof. If it were, it would be a member of itself, contradicting Proposition 3.34. □

The following exercise also shows another potentially paradoxical construction which the Axiom of Regularity precludes.

Exercise 3.36. *Prove that there can be no set $\{x_1, x_2, x_3, \dots\}$ containing an infinite sequence of sets satisfying $x_1 \ni x_2 \ni x_3 \ni \dots$ (c.f. Exercise 3.7). Hint: Apply the Axiom of Regularity to the set $\{x_1, x_2, x_3, \dots\}$.*

The following axiom is very controversial, but has become a lot more accepted over the years, and I personally use it everyday (by assuming theorems I don't know how to prove without it). But it is notoriously famous to leading to some perplexing consequences. The problem is that its negation lead to even more perplexing consequences too. So whether or not you accept it is a matter of taste, and I personally think mathematics is more beautiful and richer with it than without it. With my biases out of the way, let's see what it says

Axiom X (Choice): Given a set $\mathscr{S}$ of nonempty sets and each two elements of $\mathscr{S}$ are disjoint, there exists a set C consisting of exactly one element from each member of $\mathscr{S}$.

Example 3.37. If you have a collection of drawers, each of which contains a bunch of socks, you can *choose* a sock from each drawer and put them in a new drawer.

Looks innocent, right? Wrong! The power lies in combining it with the axiom of infinity: if you have infinitely many drawers, this is really allowing you to make infinitely many choices at once, which is a process a computer (including a human) is incapable of for example. But so what? Well, if you believe the axiom of choice, you must also believe all the following:

[7] I also trust the reader is by now sufficiently used to translating between English and formal logic, so we will omit the symbolic expressions for the last three axioms.

- **Banach-Tarski Paradox**[8]**:** One can cut a ball into 5 pieces and reassemble them to create two balls identical to the original one![9]
- **Non-measureable Sets:** There exists a set of points on a line/plane/space whose length/area/volume cannot be determined
- **Well-Ordering Theorem:**[10] Every set can be ordered in such a way that each subset of it has a least element.

Those fascinating results are hard to state precisely at this stage (and even harder to prove), but they should give you a sense of why this is a somewhat scary axiom. It is customary therefore that whenever we invoke it, mathematicians explicitly state that they are relying on the Axiom of Choice (though this practice has waned in recent years due to its essential uses in modern algebra, geometry, and topology, for example). Nonetheless, it is controversial enough that we call Axioms I-IX Zermelo–Fraenkel Axioms (or ZF for short), whereas Axioms I-X are typically referred to as Zermelo–Fraenkel's Axioms plus Choice (or ZFC for short).

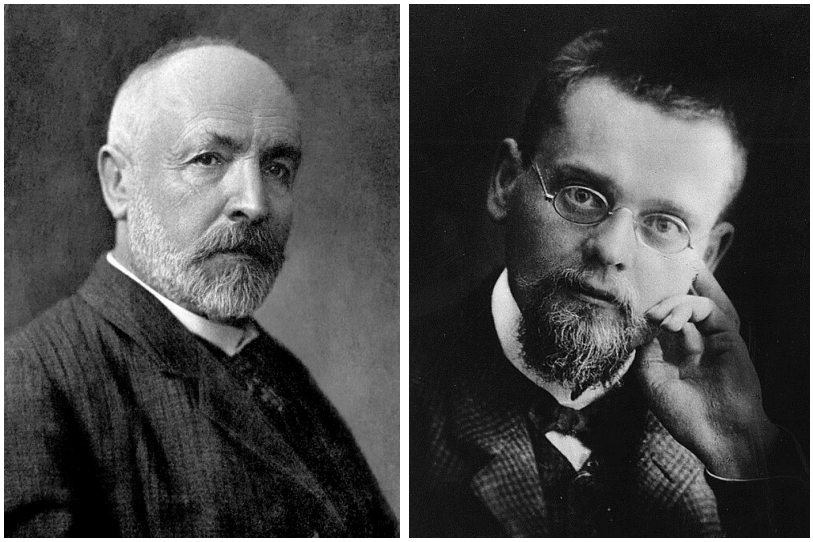


FIGURE 5. Georg Cantor (left), the father of set theory and Ernst Zermelo (right) the founder of ZFC Axioms (later improved by Fraenkel).

[8]Although we use the word paradox, this one (unlike Russell's) does not create a logical contradiction, but is merely perplexing to our human intuition; so mathematicians have no qualms about believing in such statements whenever convenient.

[9]One could also argue that the reason this is so counter-intuitive is because mathematical balls are made of infinitely many points, unlike real-life ones which are made of finitely many atoms; but still even with mathematical balls, all intuition says that this is ridiculous.

[10]Proving this theorem was the main task that led Zermelo to examine and write down the axioms we are now using as a foundation of mathematics. This theorem was conjectured by Cantor and Zermelo showed that it is equivalent to the Axiom of Choice.

Homework:

(1) Solve Exercise 3.7.
(2) Prove that $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ for any sets A, B and C.
(3) Prove that $(A \cup B)^c = A^c \cap B^c$ for any sets A and B (which are subsets of a big set U with respect to which we are taking complements)
(4) For which sets A and B does the equality $A \setminus B = B \setminus A$ hold? Prove your answer.
(5) Solve Exercise 3.21.
(6) Solve Exercise 3.22.
(7) Solve Exercise 3.32.
(8) Solve Exercise 3.34.
(9) Solve Exercise 1.50 from [DW]
(10) Solve Exercise 1.51 from [DW]

Bonus Problem: Prove that (some of) Axioms I-IX are enough to deduce Axiom X (Choice) in the case when $\mathscr{S}$ is a finite set, i.e. $\mathscr{S} = \{x_1, x_2, x_3, \ldots, x_n\}$ for some $n \in \mathbb{N}$.

4. The Natural Numbers

Last section, we defined the set $\mathbb{N}$ of natural numbers. Our goal in this section is to understand it better, as well as define its arithmetic operations (i.e. addition and multiplication), and examine its properties. Along the way we will discover a very powerful proof technique: mathematical induction.

Recall that we defined $\mathbb{N}$ as the set of those elements which belong to every inductive set. We also defined the successor function $s : \mathbb{N} \to \mathbb{N}$ given by $s(x) = x \cup \{x\}$.

Theorem 4.1 (1889, Peano)**.** *The set $\mathbb{N}$ of natural numbers satisfies the following properties:*

(1) 0 is a natural number;
(2) If n is a natural number, then so is $s(x)$;
(3) For all natural numbers n and m, if $s(m) = s(n)$, then $m = n$.
(4) For every natural number n, we have $s(n) \neq 0$.

Proof.

(1) By definition, $\mathbb{N}$ is the set of elements contained in every inductive set, and 0 belongs to every inductive set by definition of an inductive set.
(2) Suppose $n \in \mathbb{N}$, then n belongs to every inductive set by definition of $\mathbb{N}$. Thus, if I is any inductive set, we have $n \in I$ and hence $s(n) \in I$, again by definition of being inductive. Therefore, $s(n)$ also lies in every inductive set, and thus $s(n) \in \mathbb{N}$.
(3) Suppose $m \cup \{m\} = n \cup \{n\}$ for are any sets m and n. Then, either $m \in n$ or $m \in \{n\}$ (in the latter case, $m = n$). Similarly, either $n \in m$ or $n \in \{m\}$ (in the latter case, $n = m$). Assuming, towards a contradiction, that $m \neq n$, then we have $m \in n$ and $n \in m$. But then, the existence of the chain
$$m \ni n \ni m \ni n \ni \dots$$
contradicts the Axiom of Regularity by Exercise 3.36. Thus, $m = n$.
(4) Suppose towards a contradiction that there is some set n with $n \cup \{n\} = 0 := \emptyset$. Then, $\{n\} \subset \emptyset$, and $n \in \emptyset$, a contradiction. Hence, no set (and *a fortiori* no natural number) has 0 as its successor.

□

Definition 4.2. For any natural numbers n and m, define $n < m$ if $n \in m$ (vocalized n is *strictly less than* m); and we define $n \leq m$ if $n < m$ or $n = m$ (vocalized n is *less than or equal to* m). [11]

Example 4.3. $0 := \emptyset \in \{\emptyset\} =: 1$, and $1 \in \{0, 1\} =: 2$, and so on.

Exercise 4.4. *Show (by the Axiom of Regularity) that if $n < m$ then $n \neq m$ for any natural numbers n and m.*

Exercise 4.5. *Why are there are no natural numbers $n_1, n_2, n_3, \dots$ satisfying $n_{i+1} < n_i$ for each i.*

Lemma 4.6. *For any natural numbers n and m, we have $n < s(m)$ if and only if $n \leq m$.*

Proof. Suppose $n < s(m)$, which by definitions of s and $<$ means $n \in m \cup \{m\}$. So either $n \in m$ whence $n < m$, or $n \in \{m\}$ whence $n = m$. Conversely, suppose $n < m$ then $n \in m$ so $n \in m \cup \{m\} = s(m)$. And if $n = m$, then $n \in \{m\}$ so $n \in m \cup \{m\} = s(m)$. □

[11] Some people use the words "less than" to mean either $<$ or $\leq$ but we will try to avoid that due to potential ambiguity.

Theorem 4.7 (Principle of Mathematical Induction I)**.** *Suppose $A \subseteq \mathbb{N}$ is a subset satisfying the following two conditions:*

- $0 \in A$,
- *whenever $n \in A$, then $s(n) \in A$.*

Then, $A = \mathbb{N}$.

Proof. The two conditions are equivalent to saying that A is an inductive set. Since every $n \in \mathbb{N}$ is by definition a member of every inductive set, it follows that $A \subseteq \mathbb{N}$. But, by hypothesis, $A \subseteq \mathbb{N}$, so $A = \mathbb{N}$. □

The following version of induction is also very useful and will be immensely useful in the sequel:

Theorem 4.8 (Principle Mathematical Induction II)**.** *Suppose $\varphi(n)$ is a predicate with one variable n such that*

- *$\varphi(0)$ holds,*
- *For any $n \in \mathbb{N}$, if $\varphi(n)$ holds, so does $\varphi(s(n))$.*

Then, $\varphi(n)$ holds for all $n \in \mathbb{N}$. Stated symbolically,

$$[\varphi(0) \wedge \forall n \in \mathbb{N}\,(\varphi(n) \to \varphi(s(n))] \to \forall n \in \mathbb{N},\, \varphi(n)$$

Proof. Let $A := \{n \in \mathbb{N} : \varphi(n) \text{ holds}\}$ (defined by Restricted Comprehension). Then, by hypothesis, $0 \in A$ and, whenever $n \in A$, then $s(n) \in A$. Hence, by Mathematical Induction I, it follows that $A = \mathbb{N}$, i.e. $\varphi(n)$ holds for every $n \in \mathbb{N}$, as desired. □

This theorem gives us a new method to prove statements about the natural numbers: **a proof by induction**, which will always consist of three moves. To prove a claim $\varphi(n)$ for all $n \in \mathbb{N}$,

(1) **base case:** Prove the claim $\varphi(0)$;
(2) **Induction hypothesis/assumption:** Assume the claim $\varphi(n)$ holds for a generic n;
(3) **Induction Step:** Using the induction hypothesis (and anything else we know to be true already), prove that $\varphi(n+1)$ holds.

Let's use it in an example.

Proposition 4.9. *$m \subseteq n$ if and only if $m \leq n$ for any two natural numbers m and n.*

But how to prove this? There are infinitely many statements to prove, one for each choice of natural numbers m and n. The Principle of Mathematical Induction comes to the rescue! It says if we can prove a statement $\varphi(n)$ hold for $n = 0$ and that whenever it holds for some n it also holds for $s(n)$, then it holds for all natural numbers. Let's try to apply this here:

Proof. ($\Leftarrow$) We proceed by induction on n. Let $\varphi(n)$ be the statement "$\forall m\,(m \leq n \to m \subseteq n)$.

Base Case: $\varphi(0)$ holds since $m \leq 0 := \emptyset$ implies that $m = 0$ (since $m < 0$, i.e. $m \in \emptyset$, is never true), so in particular $m \subseteq 0$.

Induction Hypothesis: Assume $\varphi(n)$ holds for a given n, i.e. for any m, whenever $m \leq n$ then $m \subseteq n$.

Induction Step: We wish to prove $\varphi(s(n))$, i.e. for any $m \in \mathbb{N}$, whenever $m \leq s(n)$, we have $m \subseteq s(n)$. Suppose $m \leq s(n)$. Then, either $m = s(n)$ or $m < s(n)$, which by Lemma 4.6 means that $m \leq n$. If

$m = s(n)$, then $m \subseteq s(n)$. If $m \leq n$, then by the induction hypothesis, $m \subseteq n \subseteq n \cup \{n\} = s(n)$. So in either case, we establish $\varphi(s(n))$, which completes the induction step and thereby the proof of this direction.

($\Rightarrow$): We again proceed by induction on n. Let $\varphi(n)$ be the statement "$\forall m\,(m \subseteq n \to m \leq n)$".

Base Case: $\varphi(0)$ holds vacuously since $m \subseteq 0 := \emptyset$ is never true.

Induction Hypothesis: Assume $\varphi(n)$ holds for a given n, i.e. for any m, whenever $m \subseteq n$ then $m \leq n$.

Induction Step: We wish to prove $\varphi(s(n))$, i.e. for any $m \in \mathbb{N}$, whenever $m \subseteq s(n)$, we have $m \leq s(n)$. Suppose $m \subseteq s(n) := n \cup \{n\}$. If $n \notin m$, then $m \subseteq n$, which by the inductive hypothesis implies that $m < n$ or $m = n$, and therefore $m \in n \cup \{n\} =: s(n)$. The remaining case is when $n \in m$, i.e. $n < m$. By the first direction of this proof, this implies that $n \subseteq m$. Then, every element of n is in m as well as $n \in m$, so that $s(n) =: n \cup \{n\} \subseteq m$. Together with the starting assumption that $m \subseteq s(n)$, this implies $m = s(n)$, which in particular means $m \leq n$, completing the induction step. □

You should imagine a proof by induction as a domino effect; if the first domino tile falls and each domino tile that falls knocks down the subsequent one, then all the tiles fall. Except that now, we have infinitely many tiles, but any specific tile can be knocked down after a finite amount of time. Here are some more intuitive examples of proofs by induction. We will see mathematical induction applied in many different contexts throughout this course.

Exercise 4.10. *Without using the Axiom of Regularity implicitly or explicitly, show by induction on n that $m < n$ implies $m \neq n$ for all natural numbers m and n (c.f. Exercise 4.4)*

Corollary 4.11. *For all natural number n, m, and k, we have*

- *$n \leq n$ (this is called reflexivity of $\leq$);*
- *if $m \leq n$ and $n \leq m$, then $n = m$ (this is called antisymmetry of $\leq$);*
- *if $m \leq n$ and $n \leq k$, then $m \leq k$ (this is called transitivity of $\leq$);*
- *if $m < n$ and $n < k$, then $m < k$ (this is called reflexivity of $<$).*

Exercise 4.12. *Prove Corollary 4.11.*

Lemma 4.13. *If $m < n$ for some natural numbers m and n, then $s(m) < s(n)$*

Proof. We proceed by induction on n. Let $\varphi(n)$ be the statement "$\forall m \in \mathbb{N}(m < n \to s(m) < s(n))$".

Base Case: $\varphi(0)$ is vacuously true since $m < 0 := \emptyset$ is never true.

Induction Hypothesis: Assume $\varphi(n)$, i.e. for a given $n \in \mathbb{N}$, suppose that for any $m \in \mathbb{N}$ we have $s(m) < s(n)$ whenever $m < n$.

Induction Step: We want to show that for any $m \in \mathbb{N}$ whenever $m < s(n)$, we have $s(m) < s(s(n))$. So let us assume $m < s(n)$. By Lemma 4.6, we have $m < n$ or $m = n$. By the induction hypothesis, if $m < n$, then $s(m) < s(n)$ and $s(n) < s(s(n))$ (any number is less than its successor), so $s(m) < s(s(n))$ as desired. On the other hand, if $m = n$, then $s(m) = s(n)$ and again $s(n) < s(s(n))$, so $s(m) < s(s(n))$. This completes the induction step. □

Proposition 4.14. *For any two natural numbers m and n, exactly one of the following statements hold: $m < n$, $n < m$, or $n = m$ (this is called a* trichotomy *of $<$).*

Proof. By Proposition 4.9 and Exercise 4.10, at most one of the three possibilities can hold. To show that at least one of them holds, we proceed by induction on n. Let $\varphi(n)$ be the statement

$$\forall m \in \mathbb{N}\,[(m < n) \vee (m = n) \vee (n < m)].$$

Base Case: if $n = 0$, then $n < m$ for all $m \in \mathbb{N}$, which can be proved by a quick induction on m (Exercise). So, $\varphi(0)$ holds.

Induction Hypothesis: For a given $n \in \mathbb{N}$, suppose that any $m \in \mathbb{N}$ satisfies $m = n$, $m < n$, or $n < m$.

Induction Step: We want to show that any $m \in \mathbb{N}$ satisfies $m = s(n)$, $m < s(n)$, or $s(n) < m$. By the induction hypothesis, we have three cases:

- $m < n$, in which case $m < s(n)$ since $n < s(n)$.
- $m = n$, in which case again $m < s(n)$ since $n < s(n)$.
- $n < m$. Then, $s(n) < s(m)$ by Lemma 4.13, which by Lemma 4.6 implies that $s(n) < m$ or $s(n) = m$.

In all cases, we achieve one of the three possibilities, so our induction is complete. □

Definition 4.15. Given a subset $A \subseteq \mathbb{N}$, a *least* element of A is a natural number $n \in A$ such that, for all $m \in A$, we have $n \leq m$.

Theorem 4.16 (Well-Ordering Principle)**.** *Every nonempty subset of* $\mathbb{N}$ *contains a least element.*

Proof. We prove the contrapositive: if $A \subseteq \mathbb{N}$ contains no least element, then $A = \emptyset$. Let $\varphi(n)$ be the statement "for all $m \leq n$, $m \notin A$". To establish that A is empty, it is enough to show that $\varphi(n)$ holds for all $n \in \mathbb{N}$, which we prove by induction on n.

Base Case: $\varphi(0)$ holds since if $0 \in A$, then 0 is a least element, contradicting our assumption that no such element exists.

Induction Hypothesis: Assume $\varphi(n)$ holds, i.e. all natural numbers less than or equal to n are not in A.

Induction Step: Let's show that all numbers less than or equal to $s(n)$ are not in A, which by Lemma 4.6 is equivalent to showing that all numbers less than n are not in A (which we know from the induction hypothesis) and that $s(n) \notin A$. But, if $s(n) \in A$, we claim that $s(n)$ would be a least element; indeed, if $m < s(n)$ (i.e. $m \leq n$ again by Lemma 4.6) and $m \in A$, which would imply that $\varphi(n)$ is false, contradicting the induction hypothesis. Therefore, $s(n) \notin A$, and our induction is complete. □

Now, let's define arithmetic operations on the natural numbers. We begin with addition:

Definition 4.17. [12] Let $+ : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ be a function defined *recursively*[13] as follows (it is customary to use the notation $a + b = c$ instead of the usual function notation $+(a, b) = c$, so we follow that custom): for every $a, b \in \mathbb{N}$,

- $a + 0 = a$
- $a + s(b) = s(a + b)$.

[12] The deligent reader is invited to compare this definition with the $pq-$system defined in the Introduction Section.

[13] the fact that such a definition is valid is non-trivial. It is a consequence of Theorem 4.29, which the interested reader can read at the end of this section.

Example 4.18. Taking $b = 1$, we get $s(a) = s(a + 0) = a + s(0) = a + 1$, so from now on we can use $s(a)$ or $a + 1$ interchangeably.

Example 4.19. Say, we want to compute $4 + 3$. We can find the value of this as follows:

$$4 + 3 = 4 + s(2) = s(4 + 2).$$

But

$$4 + 2 = 4 + s(1) = s(4 + 1).$$

And

$$4 + 1 = 4 + s(0) = s(4 + 0) = s(4)$$

Therefore,

$$4 + 3 = s(4 + 2) = s(s(4 + 1)) = s(s(s(4))) = s(s(5)) = s(6) = 7.$$

From that While, of course, we all knew the answer right away, the definition of $+$ we gave only allows us to perform one of two moves in every step. But we would like to have more than just these two moves whenever we want to perform addition.

Lemma 4.20. *For all natural numbers $a, b \in \mathbb{N}$, we have*

- $0 + b = b$.
- $s(a) + b = s(a + b)$.

Proof.

- Let $\varphi(n)$ be the predicate "$0 + n = n$". By Definition 4.17, we know that $\varphi(0)$ holds, i.e. $0 + 0 = 0$. Next, suppose that $\varphi(n)$ holds for a given $n \in \mathbb{N}$, i.e. $0 + n = n$. We wish to show that, under this assumption, $\varphi(n+1)$ also holds, i.e. $0+s(n) = s(n)$. Indeed, by Definition 4.17, $0+s(n) = s(0+n)$, and by our assumption $0+n = n$, so that $s(0+n) = s(n)$, which together show that $0+s(n) = s(n)$, i.e. $\varphi(n + 1)$ holds. It follows by the Principle of Mathematical Induction, that $\varphi(b)$ holds for all natural numbers $b \in \mathbb{N}$.
- We proceed again by induction on b. Let $\varphi(n)$ be the predicate "$s(a) + n = s(a + n)$. We know by Definition 4.17 that $s(a) + 0 = s(a) = s(a + 0)$, i.e. $\varphi(0)$ holds. Now, assume $\varphi(n)$ holds for a given $n \in \mathbb{N}$, i.e. $s(a) + n = s(a + n)$. We want to show, under this assumption that $s(a) + s(n) = s(a + s(n))$. But we have

  $$s(a + s(n)) = s(s(a + n)) = s(s(a) + n) = s(a) + s(n),$$

  where the first and last equalities are by Definition 4.17 and the second equality is by applying our assumption. Thus, we showed that $\varphi(n) \to \varphi(n + 1)$, whence it follows by the Principle of Mathematical Induction that $\varphi(b)$ holds for all $b \in \mathbb{N}$.

□

Exercise 4.21. *Prove $a + b = b + a$ for all natural numbers a and b, i.e. addition is commutative. Hint: use Lemma 4.20 and induction on b.*

Exercise 4.22. *Given any natural numbers $a, b, c \in \mathbb{N}$, prove that $(a + b) + c = a + (b + c)$ (i.e. addition is associative). Hint: induct on c.*

Definition 4.23. Let $\cdot : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ be a function defined recursively as follows (as with $+$, we use the notation $a \cdot b = c$ instead of the function notation $\cdot(a, b) = c$): for every $a, b \in \mathbb{N}$,

- $a \cdot 0 = 0$
- $a \cdot (b + 1) = (a \cdot b) + a$.

Remark 4.24. We shall use the convention that multiplication occurs before addition unless parentheses indicate differently. We shall also often omit $\cdot$, writing ab rather than $a \cdot b$ whenever no ambiguity may occur.

Proposition 4.25. *For all natural numbers n, we have $n \cdot 1 = 1 \cdot n = n$.*

Proof. First note that

$$n \cdot 1 = n(0 + 1) := n \cdot 0 + n := 0 + n = n + 0 := n,$$

where the second to last equality follows by Exercise 4.21 and all other equalities follow from the definitions of addition and multiplication. Thus, we only need to prove that $1 \cdot n = n$. This is proved by induction on n as follows:

Base Case: $1 \cdot 0 = 0$ by the definition of multiplication.

Induction Hypothesis: suppose $1 \cdot n = n$.

Induction Step: Then, $1 \cdot (n+1) := 1 \cdot n + 1 = n + 1$, where the first equality is by definition of multiplication and the second is by the induction hypothesis. □

Proposition 4.26. *For all natural numbers a, b, and c, we have $(a + b) \cdot c = ac + bc$.*

Proof. We induct on c.

Base Case: when $c = 0$ we get $(a + b) \cdot 0 := 0$, and $ac + bc = a \cdot 0 + b \cdot 0 := 0 + 0 = 0$.

Induction Hypothesis: suppose $(a + b)c = ac + bc$ for all $a, b \in \mathbb{N}$.

Induction Step: Then,

$$(a + b)(c + 1) := (a + b)c + (a + b) = (ac + bc) + (a + b) = (ac + a) + (bc + b) := a(c + 1) + b(c + 1),$$

where the first and last equalities are by definition of multiplication, the second is by the induction hypothesis, and the third is by associativity of addition. □

Proposition 4.27. *Prove $ab = ba$ for all natural numbers a and b, i.e. multiplication is commutative.*

Proof. We proceed by induction on b.

Base Case: $a \cdot 0 = 0$ by the definition of multiplication. and $0 \cdot a = 0$ by a quick induction on a (Exercise).

Induction Hypothesis: suppose $ab = ba$ for all $a \in \mathbb{N}$.

Induction Step: Then, $a(b + 1) := ab + a = ba + a = ba + 1 \cdot a = (b + 1)a$, where the second equality is by the induction hypothesis, the third is by Proposition 4.25, and the last by Proposition 4.26. This completes the induction step. □

Exercise 4.28. *Show that for all natural numbers m ,n, and k, the following identities hold:*

(1) $(mn)k = m(nk)$ (i.e. multiplication is associative).
(2) if $m < n$, then $m + k < n + k$.

(3) if $m < n$ and $k \neq 0$, then $mk < nk$.
(4) if $mk = nk$ and $k \neq 0$, then $m = n$.
(5) if $m + k = n + k$ then $m = n$.
(6) if $mn = 0$ then $m = 0$ or $n = 0$.
*(7) if $m \leq n$, then there exists a **unique** $d \in \mathbb{N}$ such that $m + d = n$.*

FIGURE 6. Guiseppe Peano, who wrote the standard axiomatization of the natural numbers which we followed in this section.

The remainder of this section consists of **optional** material that the curious reader can learn, but which will not be part of our course. The reason we were able to define addition and multiplication recursively as we did is because of the following theorem.

Theorem 4.29 (Recursion Theorem)**.** *Let A be any set, a be an element of A, and $r : \mathbb{N} \times A \to A$ be a function. There exists a function $f : \mathbb{N} \to A$ satisfying $f(0) = a$ and $f(n + 1) = r(n, f(n))$ for all $n \in \mathbb{N}$.*

Proof Sketch. Let $f = \bigcap\{S \subseteq \mathbb{N} \times A : ((0, a) \in S) \wedge \forall n \in \mathbb{N} \forall x \in A\ [(n, x) \in S \to (n + 1, r(n, x)) \in S\} \subseteq \mathbb{N} \times A$. This is a set by the Power Set Axiom, the Axiom of Restricted Comprehension, and Exercise 3.21. Then, $(0, a) \in f$ (i.e. $f(0) = a$) and whenever $(n, x) \in f$ then $(n + 1, r(n, x)) \in f$, so a quick induction shows that f satisfies the conditions we want.

It remains to show that $f : \mathbb{N} \to A$ is a function, i.e. that $f(n)$ is defined for all $n \in \mathbb{N}$ and that whenever $(n, x) \in f$ and $(n, y) \in f$, we must have $x = y$. Both of which can be proved by induction on n. □

Exercise 4.30. *Fill out the details in the sketch given to prove Theorem 4.29.*

Corollary 4.31. *The function $+$ defined by Definition 4.17 is well-defined.*

Proof. First, we define a function which adds m to any given natural number: let $f_m : \mathbb{N} \to \mathbb{N}$ be the function given by $f_m(0) = m$ and $f_m(n+1) = f_m(n) + 1$, which exists by Theorem 4.29. Next, we let $m + n := f_m(n)$, which defines addition in the same way as Definition 4.17. □

Exercise 4.32. *Mimic the proof of Corollary 4.31 to prove that the function $\cdot$ defined by Definition 4.23 is well-defined.*

Homework:

- Prove Corollary 4.11. [10 pts.]
- Solve Exercise 4.22. [5 pts.]
- Solve Exercise 4.28. [35 pts.]

5. Applications of Mathematical Induction

So far, we have only used mathematical induction to prove properties about the natural numbers. But it is such a versatile proof technique that we will dedicate this section to looking at some of its countless applications, as well as continue to see more applications in future sections too.

Recall that a proof by induction goes as follows: **To prove a claim $\varphi(n)$ for all $n \in \mathbb{N}$,**

(1) **base case:** Prove the claim $\varphi(0)$;
(2) **Induction hypothesis:** Assume the claim $\varphi(n)$ holds for a generic n;
(3) **Induction Step:** Using the induction hypothesis (and anything else we know to be true already), prove that $\varphi(n+1)$ holds.

However, there is really no reason we have to start our induction with $n = 0$, we can start the base case, for example, at $n = 1$, noting that the claim proved will hold for all natural numbers $n \geq 1$. More generally, we can start from any base case $b \in \mathbb{N}$ we like, i.e. **to prove a claim $\varphi(n)$ for all natural numbers $n \geq b$,**

(1) **base case:** Prove the claim $\varphi(b)$;
(2) **Induction hypothesis:** Assume the claim $\varphi(n)$ holds for a generic n;
(3) **Induction Step:** Using the induction hypothesis (and anything else we know to be true already), prove that $\varphi(n+1)$ holds.

Let us apply this "new" version of induction to a simple fun formula.

Proposition 5.1 (Gauss's Summation Formula)**.** *For any natural number $n \geq 1$, we have*

$$2(1 + 2 + 3 + \cdots + n) = n(n+1).$$

Proof. We proceed by induction on n. For the base case, if $n = 1$, the left-hand side is $2 \cdot (1) = 2$ and the right-hand side is $1 \cdot (1+1) = 2$, so the claim holds when $n = 1$. Assume it holds for some given $n \in \mathbb{N}$. Then,

$$2(1 + 2 + \cdots + n + (n+1)) = 2(1 + 2 + \cdots + n) + 2(n+1) = n(n+1) + 2(n+1) = (n+1)(n+2),$$

where we used the induction hypothesis for the second equality (and distributivity for the other two equalities). This completes the induction step, so the formula holds for all $n \geq 1$. □

Definition 5.2. A *sequence* $\{a_i\}_{i \in \mathbb{N}}$ of elements of X is a function $a : \mathbb{N} \to X$, and the *terms* of the sequence $a_i := a(i)$.

Example 5.3. The sequence $\{2^i\}_{i \in \mathbb{N}}$ is the function $a : \mathbb{N} \to \mathbb{N}$ given by $a(i) = 2^i$; its first few terms are $1, 2, 4, 8, \ldots$. [14]

Notation 5.4. Sometimes it is more convenient to write sums of terms of a sequence like $1 + 2 + \cdots + n$ in a more concise way as follows:

$$\sum_{i=1}^{n} a_i := a_1 + a_2 + \cdots + a_n,$$

[14] As you probably know, we define m^n as the product of m with itself n times, and $m^0 := 1$.

where each $\{a_i\}_{i\in\mathbb{N}}$ is a given sequence. Here i is a variable that ranges from 1 to n iteratively. Analogously for the product, we define

$$\prod_{i=1}^{n} a_i := a_1 \cdot a_2 \cdot \cdots \cdot a_n.$$

We also define the operations of repeated unions $\bigcup_{i=1}^{n}$ and intersections $\bigcap_{i=1}^{n}$ for sets similarly.

Let's try these out in another induction proof

Example 5.5. For any $n \in \mathbb{N}$, we have

$$\sum_{i=0}^{n} 2^i = 2^{n+1} - 1.$$

Proof. We proceed by induction on n. When $n = 0$, the left-hand side is $2^0 = 1$, and the right-hand side is $2^1 - 1 = 1$, so the formula holds. Assume that it holds for some $n \in \mathbb{N}$. Then,

$$\sum_{i=1}^{n+1} 2^i = 2^{n+1} + \sum_{i=1}^{n} 2^i \overset{\text{by Ind. Hyp.}}{=} 2^{n+1} + 2^{n+1} - 1 = 2 \cdot 2^{n+1} - 1 = 2^{n+2} - 1,$$

so the formula works for $n + 1$ too, completing our induction. □

Remark 5.6. As is illustrated by the previous two examples, induction does not help us figure out the formula, but merely allows us to prove a conjecture we already guessed.

Exercise 5.7. *Conjecture and prove a formula for the sum of the first n odd*[15] *natural numbers.*

Exercise 5.8. *Show that, for any natural number $n \geq 1$, we have* $6\sum_{i=1}^{n} i^2 = n(n+1)(2n+1)$.

Induction is also sometimes helpful to prove inequalities. For example,

Proposition 5.9. *For all natural numbers $n \geq 4$, we have $2^n < n!$, (where $n! := \prod_{i=1}^{n} i$).*

Proof. We induct on n. Our base case is $n = 4$, in which $2^4 = 16 < 24 = 4!$, so the claim holds. Suppose it holds for some given $n \geq 4$. Then,

$$2^{n+1} = 2 \cdot 2^n < (n+1)2^n < (n+1)n! = (n+1)!,$$

where the first inequality is because $n + 1 \geq 5 > 2$ and the second is by the Induction hypothesis. □

We can also use induction to prove results about sets. For example,

Proposition 5.10 (Generalized De Morgan's Law)**.** *Given any sets $A_1, A_2, \ldots, A_n$ with $n \geq 2$, we have*

$$\left(\bigcap_{i=1}^{n} A_i\right)^c = \bigcup_{i=1}^{n} A_i^c.$$

[15] A natural number k is odd if there exists $m \in \mathbb{N}$ such that $k = 2m + 1$.

Proof. We proceed by induction on n. Our base case is $n = 2$, where the statement is exactly De Morgan's Law's (Exercise 3.18). Suppose it holds for some n. Then,

$$\begin{aligned}\left(\bigcap_{i=1}^{n+1} A_i\right)^c &= \left(\left(\bigcap_{i=1}^{n} A_i\right) \cap A_{n+1}\right)^c \\ &= \left(\bigcap_{i=1}^{n} A_i\right)^c \cup A_{n+1}^c \\ &= \left(\bigcup_{i=1}^{n} A_i^c\right) \cup A_{n+1}^c \\ &= \bigcup_{i=1}^{n+1} A_i^c,\end{aligned}$$

where the second equality is by the base case and the third is by the induction hypothesis. This completes the induction step. □

Exercise 5.11. *Prove the for any sets $A, B_1, B_2, \ldots, B_n$, where $n \geq 2$, we have*

$$A \cup \left(\bigcap_{i=1}^{n} B_i\right) = \bigcup_{i=1}^{n} (A \cap B_i) \quad \textit{and} \quad A \cap \left(\bigcup_{i=1}^{n} B_i\right) = \bigcap_{i=1}^{n} (A \cup B_i).$$

There are also many more "wilder" applications of induction, including geometric ones! Let's examine some of them now. [16]

Proposition 5.12. *Let us call a configuration of lines in the plane "generic" if no two lines are parallel and no three lines meet at a common point. Every generic configuration of n lines in the plane split the plane into $(n^2 + n + 2)/2$ regions.*

Proof. We proceed by induction on n. If $n = 1$, we have a single line which splits the plane into $2 = (1^2 + 1 + 2)/2$ regions, so our base case hold. Assume every generic configuration on n lines splits the plane into $(n^2 + n + 2)/2$ regions. Then, imagine drawing one more line *slowly*. Every time the new line meets one of the n old lines, it splits one of the old regions into two. Moreover, after meeting every line, the unbounded portion of the new line extending to infinity splits one of the outer regions into two. So, in total, $n + 1$ new regions were created upon drawing the last line: n for every intersection with old lines (since every two lines meet exactly once in a generic configuration) plus one unbounded region going towards infinity. By induction hypothesis, we had $(n^2 + n + 2)/2$ old regions, so in total, we have

$$\frac{n^2 + n + 2}{2} + n + 1 = \frac{n^2 + 3n + 4}{2} = \frac{(n+1)^2 + (n+1) + 2}{2} \text{ regions},$$

which concludes the induction step. □

[16] We will not define all of these geometric notions rigorously as we did for the natural numbers, for example, but since these applications will not be used in the sequel, we need not be scared about our lack of rigor affecting future results. The goal here is to illustrate the various flavors of induction proofs.

Exercise 5.13. *We call a configuration of circles in the plane "generic" if every two circles meet at exactly two points and no three circles have a point in common. Conjecture and prove a formula for the number of regions created by a generic configuration of circles in the plane.*

Example 5.14. Given a generic configuration of circles in the plane, there is a coloring of the regions with two colors such that no two regions sharing a common arc have the same color.

Proof. We induct on the number n of circles. If $n = 1$, we color the inside white and the outside black. Suppose an admissible coloring exists for the regions created by any configuration of n circles. Suppose now that we are given a generic configuration of $n + 1$ circles in the plane. Deleting one of the circles produces a generic configuration of n circles so we may color it by our hypothesis. Now, if we draw the deleted circle again, we can invert the colors of all the regions inside the new circle and leave the regions outside it unchanged. Then, suppose two regions are neighbors (i.e. sharing a common arc) in this new configurations. We have three cases: **Case I:** (both regions are outside) in this case, the old configuration hasn't changed so they must be differently colored.

Case II: (both regions are inside) in this case, both regions' colors got switched, and since they were differently colored, they remain so.

Case III: (one region is inside and one is outside) in this case, the two regions share an arc along the new circle (since the configuration is generic). Thus, prior to drawing that circle, both regions were one and the same (in particular colored similarly). So upon changing the color of only the inside region switched colors, and so the two regions are again colored differently.

It follows that, in all cases, the new configuration is still admissible, completing the induction step. □

Example 5.15. Any $2^n \times 2^n$ checkerboard with a 1×1 square missing can be tiled with triominoes (i.e. a 2×2 square with one 1×1 square removed as shown in the figure below).

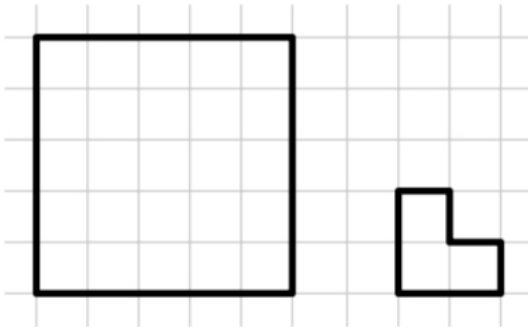


FIGURE 7. A triomino on a grid

Proof. We proceed by induction on n. If $n = 1$, we have a 2×2 board with one square removed, which is the same shape as a triomino, so we tile it with one. Suppose that every $2^n \times 2^n$ grid with one square removed can be tiles with triominoes.

Then, given a $2^{n+1} \times 2^{n+1}$ board with one square removed, we split it into four quarters to produce 4 distinct $2^n \times 2^n$ sub-boards, with only one of them missing a square. Without loss of generality, by rotating

the board, we may assume that the top-right sub-board is the one missing a square, and hence can be tiled with triominoes by the induction hypothesis. By inserting a single triomino covering the top-right, top-left, and bottom-right squares of the bottom-left, bottom-right, and top-left sub-boards respectively, we are left with three more sub-boards missing a square each which now need to be tiled. But a tiling of each of them is again guaranteed by the induction hypothesis. □

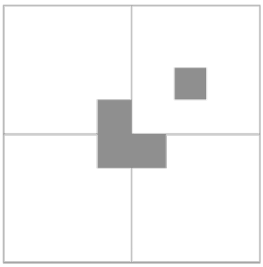


FIGURE 8. The induction step for tiling $2^{n+1} \times 2^{n+1}$ board with a missing square with triominoes.

Sometimes a variant of the method of induction is useful for some applications.

Theorem 5.16 (Strong Induction)**.** *Suppose $\varphi(n)$ is a predicate with variable $n \in \mathbb{N}$. Suppose further that*

- *$\varphi(0)$ holds;*
- *$\forall k \geq 1 \ \ [(\varphi(0) \wedge \varphi(1) \wedge \ldots \varphi(k-1)) \to \varphi(k)]$.*

Then, $\varphi(n)$ holds for all $n \in \mathbb{N}$.

Before we prove this theorem, let us see how it can be helpful in some applications.

Example 5.17. Every amount of postage of 12 cents or more can be formed using only 4-cent and 5-cent stamps.

Proof. Let $\varphi(n)$ be the statement that a postage of n cents can be formed using 4-cent and 5-cent stamps. We proceed by strong induction on n. As our base case, let's consider $\varphi(12)$, $\varphi(13)$, $\varphi(14)$, and $\varphi(15)$; in each of these cases we can form the desired amount as follows:

$$12 = 4 + 4 + 4$$
$$13 = 4 + 4 + 5$$
$$14 = 4 + 5 + 5$$
$$15 = 5 + 5 + 5.$$

Now suppose every postage amount n with $16 \leq n < k$ can be formed for some given $k \geq 16$. Then, in particular, we can form a postage of $k - 4$ since $\varphi(k-4)$ holds (because $12 \leq k - 4 < k$). Adding a 4-cent stamp to the $k - 4$ postage gives us the desired postage for k, which completes our induction step. □

Remark 5.18. The reason it is called "strong" induction is because our induction hypothesis is logically stronger: we are assuming that $\varphi(n)$ holds for $n = 1, 2, 3, \ldots, k-1$ instead of just assuming $\varphi(k-1)$ holds.

However, it's not actually a stronger because as we will see presently, we can prove strong induction using regular induction.

Proof of Theorem 5.16. Suppose as in the Theorem's premises that $\varphi(0)$ holds and whenever $\varphi(0) \wedge \varphi(1) \wedge \cdots \wedge \varphi(k-1)$, then so does $\varphi(k)$. Define a new predicate $\psi(k) := \varphi(0) \wedge \varphi(1) \wedge \cdots \wedge \varphi(k)$ for each $k \in \mathbb{N}$. To prove that $\varphi(n)$ holds for all $n \in \mathbb{N}$, it suffices to prove that $\psi(n)$ holds for all $n \in \mathbb{N}$, which we proceed to show by induction on n.

We know $\psi(0) := \varphi(0)$ holds by assumption. Assume $\psi(k-1) := \varphi(0) \wedge \varphi(1) \wedge \cdots \wedge \varphi(k-1)$ holds; this implies that $\varphi(k)$ holds, via our second assumption. Thus, $\psi(k) := \varphi(0) \wedge \varphi(1) \wedge \cdots \wedge \varphi(k-1) \wedge \varphi(k)$ also holds, which completes our induction step. This shows that $\psi(n)$ holds for every $n \in \mathbb{N}$ and hence the same is true of $\varphi(n)$. □

Exercise 5.19. *Prove the following generalized form of strong induction (with an arbitrary base): Suppose $\varphi(n)$ is a predicate with variable $n \in \mathbb{N}$. Suppose further that*

- *$\varphi(b)$ holds;*
- *$\forall k \geq b \ [(\varphi(b) \wedge \varphi(b+1) \wedge \ldots \varphi(k-1)) \to \varphi(k)]$.*

Then, $\varphi(n)$ holds for all $n \in \mathbb{N}$. Hint: mimic the proof of Theorem 5.16.

Example 5.20. Consider the following game of "Nim" played by two players. There are two identical piles of sticks each. Each move a player is allowed to remove any number of stick from one of the two piles. Whoever takes the last stick wins.

Claim: *The player who goes second always can always win.*

Proof. We proceed by strong induction on the number n of sticks. If $n = 1$, then the first player is forced to take one stick from either pile leaving the (last) stick of the other pile for the second player, thus winning.

Suppose that for every such game of nim with the number of sticks per pile is at most n, the second player has a winning strategy.

Now, consider a game with $n+1$ sticks per pile. Suppose the first player removes r sticks from some pile. Then, by removing r sticks from the other pile, the second player has now forced us to go back to the beginning position of a game with $n+1-r \leq n$ sticks per pile, where again the first player will play first. By the induction hypothesis, the second player can win this game, thus completing the induction step. □

Another important application of (strong) induction is proving explicit formulas for a given recursive pattern.

Proposition 5.21. *Let $\{a_i\}_{i \in \mathbb{N}}$ be the sequence defined recursively as follows: $a_0 = 1$, $F_1 = 1$, and for all $n \geq 2$, we have $a_n = 5a_{n-1} - 6a_{n-2}$. Then, for all $n \in \mathbb{N}$, $a_n = 2^{n+1} - 3^n$.*

Proof. We proceed by strong induction on n. We have $1 = a_0 = 2^{0+1} - 3^0$ and $1 = a_1 = 2^{1+1} - 3^1$, so the formula holds for $n = 0$ and $n = 1$. Suppose $a_n = 2^{n+1} - 3^n$ for $0 \leq n \leq k$. Then,

$$\begin{aligned} a_{k+1} = 5a_k - 6a_{k-1} &\overset{\text{I.H.}}{=} 5(2^{k+1} - 3^k) - 6(2^k - 3^{k-1}) \\ &= 5 \cdot 2^{k+1} - 5 \cdot 3^k - 3 \cdot 2^{k+1} + 2 \cdot 3^k = 2 \cdot 2^{k+1} - 3 \cdot 3^k = 2^{k+2} - 3^{k+1}. \end{aligned}$$

Thus the formula holds for $n = k+1$ too, completing the induction step. □

The following examples illustrates common pitfalls in proofs by induction.

Exercise 5.22. *Find the mistakes in each of the examples below.*

Example 5.23. **Claim:** all horses have the same color. *"Proof":* Each horse has the same color as themself (base case). Suppose every n horses have the same color (induction hypothesis). Then, consider $n+1$ horses; each n horses among them have the same color by assumption, therefore they all have the same color (induction step). Obviously, this is a wrong proof, so where did we go wrong? Hint: Does our induction step work for all n?

Example 5.24. **Claim:** $n = n+1$ for every $n \in \mathbb{N}$. *"Proof:"* Suppose $k = k+1$ for some natural number k. Then, adding 1 to both sides, we get $k+1 = k+2$ completing the induction step.

Example 5.25. **Claim:** Every set of n lines of the plane, no two of which are parallel, meet at one common point. *"Proof":* The claim holds for $n = 2$. Suppose every k lines no two of which are parallel meet at a common point. Then, if we have $n+1$ lines, numbering them 1 through $n+1$, the first n meet at some point p, and the last n meet at some point q by the induction hypothesis. If p and q were different points, all lines containing both of them must be the same line because two points determine a line. This contradicts our assumption that all these lines are distinct. Thus, p and q are the same point. We conclude that the point $p = q$ lies on all $k+1$ lines.

Homework 5. Read from [DW] pp. 51-71 then solve the following exercises from [DW]: 3.4, 3.10, 3.11, 3.19, 3.39, 3.41 (replace $\mathbb{R}$ with $\mathbb{N}$ throughout this problem), 3.47 (it should say for all $n > 0$), 3.55, 3.56, 3.62.

6. Functions, Bijections, and Cardinality

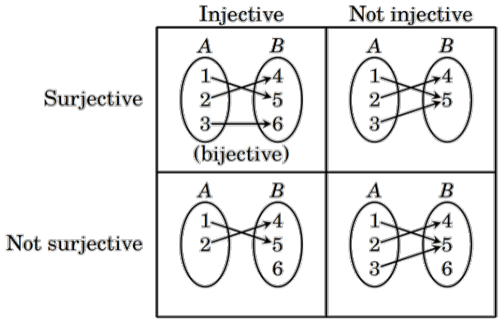
So far, we learned about natural numbers which formalized our intuitive ideas of counting. In this section, we would like to push this idea of counting further; more precisely, we want to compare the sizes of different sets, including infinite ones. In doing so, we will rediscover Cantor's great ideas on the different sizes of infinity.

Our main technical tool for comparing the sizes of sets will be functions and certain properties thereof. Recall that a *function* $f : A \to B$ from a set A to a set B is a rule that assigns to **every** element (called *input*) of the domain A **exactly one** element (called *output*) of the codomain B.[17] The set of all outputs of f is called the *image/range* of f.

Definition 6.1. A function $f : A \to B$ is called

- *injective* if it maps every two inputs of A to distinct outputs in B, i.e. $f(x) \neq f(y)$ whenever $x \neq y$ for all $x, y \in A$.
- *surjective* if every element of B is the output to some input of A, i.e. for all $b \in B$, we have some $a \in A$ such that $b = f(a)$. Equivalently, $B = \mathrm{Im}\,(f)$.
- bijective if it is both injective and surjective

Example 6.2. The following figure illustrates the difference between (non-)injectivity/(non-)surjectivity:



Intuitively speaking, one can see that if a function $f : A \to B$ is injective, we assign to elements of A some elements of B without repetition. So, intuitively, if there is an injective function $f : A \to B$, then A must have "at most as many elements as" B. Conversely, if $f : A \to B$ is surjective, then all elements of B come from distinct elements of A; and so, A has "at least as many elements as" B if a surjection $f : A \to B$ exists. If A and B are in bijection, i.e. there is a bijective function $f : A \to B$, they must be "of the same size". Indeed, we take this intuition to be our definition of size:

Definition 6.3. Given sets A and B,

- we say A has smaller *cardinality/size* than B (denoted $|A| \leq |B|$) if there exists an injective function $f : A \to B$;
- we say A has larger *cardinality/size* than B (denoted $|A| \geq |B|$) if there exists a surjective function $f : A \to B$;

[17] This is a paraphrasing of Definition 3.28, which is perhaps more intuitive.

- we say A has the same *cardinality/size* than B (denoted $|A| = |B|$) if there exists a bijection $f : A \to B$.

Remark 6.4. *A priori* it is not at all clear that $|A| = |B|$ is equivalent to $|A| \leq |B|$ and $|B| \leq |A|$. Indeed, the question is the following: suppose there is an injective function $f : A \to B$ and another injective function $g : B \to A$ (i.e. $|A| \leq |B|$ and $|B| \leq |A|$). Does there exist a bijection $h : A \to B$? It turns out that the answer is yes, but the proof is far from obvious. This is the famous Cantor-Berstein-Schröder Theorem.

Exercise 6.5. *Find two sets A and B and two injective function $f : A \to B$ and $g : B \to A$ neither of which is a bijection.*

Theorem 6.6 (Cantor-Bernstein-Schröder)**.** *Given sets A and B, if there are injective functions $f : A \to B$ and $g : B \to A$, then there exists a bijective function $h : A \to B$. In other words, if $|A| \leq |B|$ and $|B| \leq |A|$ then $|A| = |B|$.*

This is a somewhat difficult theorem to prove, and we will skip the proof and take it on faith, but the interested reader is encouraged to look at the proof in [DW], Theorem 4.47.

Remark 6.7. It is even less clear that $|A| = |B|$ is equivalent to $|A| \leq |B|$ and $|A| \geq |B|$ since the former says there is a bijection $f : A \to B$, whereas the latter says there is an injection $f : A \to B$ and a surjection $g : B \to A$ but f and g need not be the same. In fact these two different conditions are equivalent if and only if we assume the Axiom of Choice holds!

Exercise 6.8. *Find two sets A and B, with an injection which is not surjective $f : A \to B$ and a surjection which is not injective $g : A \to B$.*

Definition 6.9. Given two functions $f : A \to B$ and $g : B \to C$, we define their *composition* as the function $h : A \to C$ given by $h(a) := g(f(a))$ for every $a \in A$, and we write $h = g \circ f$.

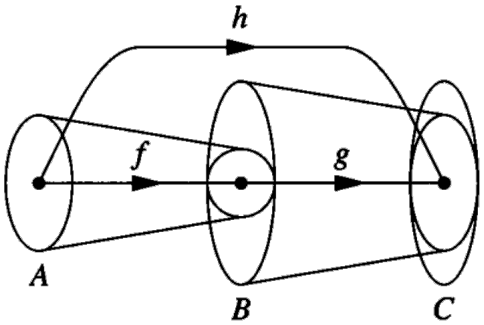


FIGURE 9. composition of functions

Exercise 6.10. *Given functions $f : A \to B$, $g : B \to C$ and $h : C \to D$, prove that $h \circ (g \circ f) = (h \circ g) \circ f$, i.e. function composition is associative.*

Exercise 6.11. *Find functions $f : A \to B$ and $g : B \to A$ such that $f \circ g \neq g \circ f$, i.e. function composition is **not** commutative.*

Recall that for a given set A, the identity function $\mathrm{Id}_A : A \to A$ is the function given by $\mathrm{Id}_A(a) = a$ for all $a \in A$.

Proposition 6.12. *Given sets $A \neq \emptyset$ and B and functions $f : A \to B$,*

- *f is injective if and only if there exists a function $g : B \to A$ such that $g \circ f = \mathrm{Id}_A$.*
- *f is surjective if and only if there exists a function $g : B \to A$ such that $f \circ g = \mathrm{Id}_B$.*

In particular, f is bijective if and only if there exists $g : A \to B$ such that $g \circ f = \mathrm{Id}_A$ and $f \circ g = \mathrm{Id}_B$.

Proof.
- Suppose f is injective, and define $g : B \to A$ as follows. Given $b \in \mathrm{Im}(f) \subseteq B$, then there exists $a_b \in A$ with $f(a_b) = b$; moreover, such a_b must be unique by injectivity of f, thus, we may define $g(b) = a_b$. Fix If $b \in B \setminus \mathrm{Im}(f)$, we define $g(b) = *$ where $*$ is any fixed element of A (which exists as $A \neq \emptyset$. This defines f on all of B, and guarantees that for any $a \in A$, we have $g(f(a)) = a$ by construction.

  Conversely, suppose there is a $g : B \to A$ satisfying $g \circ f = \mathrm{Id}_A$. To show that f is injective, we wish to prove that if $x \neq y$ then $f(x) \neq f(y)$. We prove the contrapositive. Suppose $f(x) = f(y)$ and apply g to both sides. We get $x = g(f(x)) = g(f(y)) = y$, so f is injective as desired.
- Suppose f is surjective, and define $g : B \to A$ as follows. Take $g(b)$ to be any of the elements $a \in A$ with $f(a) = b$, which exist by surjectivity (although, perhaps not unique). Then, $f(g(b)) = b$ by construction.

  Conversely, if we have a function $g : B \to A$ satisfying $f \circ g = \mathrm{Id}_B$, then, for any $b \in B$, we have $f(g(b)) = b$, whence $b \in \mathrm{Im}(f)$ (it is the output for input $g(b)$). Thus, f is surjective.

□

Definition 6.13. If $f : A \to B$ is a bijection and $g : B \to A$ is a function satisfying $g \circ f = \mathrm{Id}_A$ and $f \circ g = \mathrm{Id}_B$, then g is called *the inverse* of f, and we write $g = f^{-1}$.

The word "the" in the definition of the inverse of a bijective function requires justification, because it implies that such a function is unique.

Exercise 6.14. *Show that if $f : A \to B$ is a bijection and $g : B \to A$ and $h : B \to A$ are functions satisfying $g \circ f = \mathrm{Id}_A$ and $f \circ g = \mathrm{Id}_B$ and $h \circ f = \mathrm{Id}_A$ and $f \circ h = \mathrm{Id}_B$, then $g = h$. In other words, there is a* unique *inverse of any given bijection.*

Exercise 6.15. *Given bijective functions $f : A \to B$ and $g : B \to C$, prove that $g \circ f$ is also a bijection with inverse $f^{-1} \circ g^{-1}$.*

Now we are well-equipped to start thinking about sizes of infinite sets. The notion of size behaves very strangely for infinite sets unlike finite ones, as demonstrated by the following example.

Example 6.16 (Hilbert's Hotel). In Hilbert's hotel, there are infinitely many rooms numbered by the natural numbers. A new guest arrives and finds that all rooms are occupied. Can we accommodate them? The answer is yes! we can ask each guest in room number n to move to room number $n + 1$, which clears the room number 0 for the new guest. In disguise, we just proved that the sets $\mathbb{N}$ and $\mathbb{N} \cup \{*\}$ are in bijection!

Exercise 6.17. *A bus with seats numbered by the natural numbers carrying infinitely many guests arrive to Hilbert's hotel which was already fully booked. How can we accommodate all the new guests?*

Definition 6.18. A set A is called

- *finite* if $|A| = |n|$ for some $n \in \mathbb{N}$;
- *infinite* if $|\mathbb{N}| \leq |A|$;
- *countably infinite* if $|\mathbb{N}| = |A|$;
- *uncountable* if $|\mathbb{N}| \leq |A|$ and $|\mathbb{N}| \neq |A|$.

So far, Example 6.16 and Exercise 6.17 seem to suggest that all infinities are equally big. But Definition 6.18 seems to suggest otherwise; namely, we defined uncountable sets to be strictly bigger than the natural numbers, which are already infinite. So a natural question arises: "are there any uncountable sets"? Let's try to find one. Perhaps, as a first candidate, we can try two copies of the natural numbers; intuitively, it feels like it should be of a larger cardinality than just one copy of $\mathbb{N}$, but the next proposition shows this is not the case!

Proposition 6.19. $\mathbb{N} \times \{0, 1\}$ *is countable.*

Proof. We construct a bijection $f : \mathbb{N} \times \{0, 1\} \to \mathbb{N}$. Define

$$f(n, i) = \begin{cases} 2n & \text{if } i = 0 \\ 2n + 1 & \text{if } i = 1 \end{cases}.$$

Next, define a function $g : \mathbb{N} \to \mathbb{N} \times \{0, 1\}$ by

$$g(n) = \begin{cases} (n/2, 0) & \text{if } n \text{ is even} \\ (\frac{n-1}{2}, 1) & \text{if } n \text{ is odd} \end{cases}.$$

To show that f is a bijection, it suffices to show that g is an inverse of f, i.e. $g \circ f = \mathrm{Id}_{\mathbb{N}\times\{0,1\}}$ and $f \circ g = \mathrm{Id}_{\mathbb{N}}$. Indeed, for any $(n, i) \in \mathbb{N} \times \{0, 1\}$, we have

$$g(f(n, i)) = \begin{cases} g(2n) = (n, 0) & \text{if } i = 0 \\ g(2n + 1) = (n, 1) & \text{if } i = 1 \end{cases} = (n, i),$$

and for any $n \in \mathbb{N}$, we have

$$f(g(n)) = \begin{cases} f(n/2, 0) & \text{if } n \text{ is even} \\ f(\frac{n-1}{2}, 1) & \text{if } n \text{ is odd} \end{cases} = n.$$

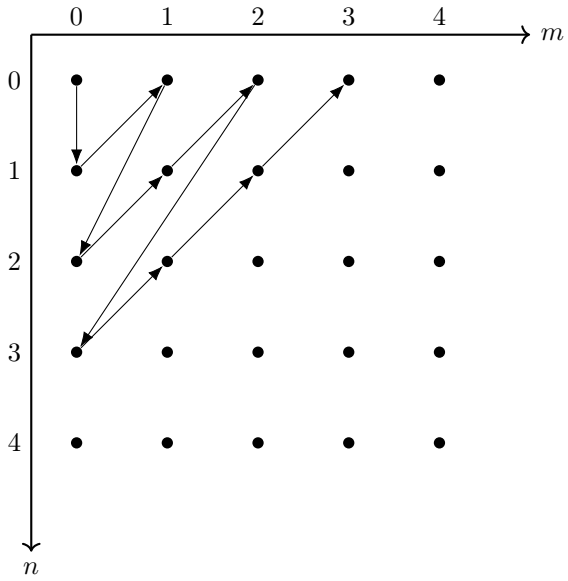
□

Our next candidate for a potentially larger set is $\mathbb{N} \times \mathbb{N}$. This feels like it should be even larger, since intuitively it is "two-dimensional". But again our intuition fails in this case as well!

Exercise 6.20. *Show that if A and B are two countably infinite sets, then so is $A \cup B$.*

Proposition 6.21. $|\mathbb{N} \times \mathbb{N}| = |\mathbb{N}|$.

Proof. Finding a bijection from $f : \mathbb{N} \to \mathbb{N}\times\mathbb{N}$ is the same as "counting" the elements of $\mathbb{N}\times\mathbb{N}$, i.e. assigning an element of $\mathbb{N} \times \mathbb{N}$ to be the $f(0)$ and another to be $f(1)$, and $f(2)$, and so on. This can be done by by taking $f(0) = (0, 0)$, then $f(1) = (1, 0)$, and $f(2) = (0, 1)$, $f(3) = (2, 0)$, and so on going over each diagonal one by one as in the following diagram:



Clearly, such enumeration will eventually get to every element of $\mathbb{N} \times \mathbb{N}$ so f is surjective. Moreover, it is also clearly injective since our snake pattern never crosses the same place twice. □

The previous ingenious proof is due to cantor and is famously known as **Cantor's Diagonalization Argument**. It can be made completely formal by defining the function f with a formula as we're used to, which is illustrated in the following exercise.

Exercise 6.22. *Define the Cantor Pairing Function $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ by $f(0, 0) = 0$ and*

$$f(m, n) = \frac{(m + n)(m + n + 1)}{2} + m$$

for all $(m, n) \in \mathbb{N} \setminus \{(0, 0)\}$. Prove that f is a bijection.

Hint: Define the following "order" on pairs (m, n): we say $(m, n) \prec (m', n')$ if either $m + n < m' + n'$ or if $m + n = m' + n'$ but $n < n'$. Now, to prove that f is injective, it's enough to that whenever $(m, n) \prec (m', n')$ then $f(m, n) < f(m', n')$ (why?). To prove surjectivity, proceed by induction: assume $k = f(m, n)$. Now, find a pair (m', n') with $f(m', n') = k + 1$ by contemplating the picture.

Corollary 6.23. *Given a countably infinite set $\mathscr{A} = \{A_0, A_1, A_2, A_3, \dots\}$ such that A_i is a countably infinite set for each $i \in \mathbb{N}$. Then, $\bigcup \mathscr{A} =: \bigcup_{i=0}^{\infty} A_i$ is countably infinite.*

Proof. First, observe that since A_i is countably infinite, we have $|A_i| = |\mathbb{N}| = |\mathbb{N} \times \{i\}|$, where the last equality is because the function $f_i : NN \to \mathbb{N} \times \{i\}$ given by $n \mapsto (n, i)$ is clearly a bijection. It follows that

$$\left|\bigcup_{i=0}^{\infty} A_i\right| = \left|\bigcup_{i=0}^{\infty} \mathbb{N} \times \{i\}\right| = |\mathbb{N} \times \mathbb{N}| = |\mathbb{N}|.$$

□

The last line of the previous proof makes use of the following fact (why?):

Exercise 6.24. *Suppose $|A| = |B|$ and $|B| = |C|$. Prove that $|A| = |C|$.*

Exercise 6.25. *Now, countably infinitely many busses each containing countably infinitely many passengers arrive to the fully booked Hilbert Hotel from Example 6.16. How can we accommodate all the new and old guests?*

We also cannot increase the cardinality by taking more and more Cartesian products!

Definition 6.26. Given a set A, define $A^1 := A$, and $A^n = A^{n-1} \times A$ for all natural numbers $n > 1$. Equivalently, A^n is the n-fold Cartesian product of A by itself.

Exercise 6.27. *Prove that $\mathbb{N}^n$ is countably infinite for all $n \geq 1$. Hint: Induction.*

The key to finding a genuinely larger cardinality than that of $\mathbb{N}$ is to consider power sets of infinite sets.

Lemma 6.28. *Let $\mathbb{B} := \{a : \mathbb{N} \to \{0, 1\}\}$ be the set of infinite binary sequences. Then, $|\mathbb{B}| = |\wp(\mathbb{N})|$.*

Proof. We construct a bijection $S : \mathbb{B} \to \wp(\mathbb{N})$ and an inverse $T : \wp(\mathbb{N}) \to \mathbb{B}$ for it as follows. Given a sequence $a \in \mathbb{B}$, let

$$S(a) = \{n \in \mathbb{N} \ : \ a(n) = 1\},$$

and let $T(A) : \mathbb{N} \to \{0, 1\}$ be the function defined by

$$T(A)(n) = \begin{cases} 1 & \text{if } n \in A \\ 0 & \text{if } n \notin A \end{cases}.$$

Then,

$$S(T(A)) = \{n \in \mathbb{N} \ : \ T(A)(n) = 1\} = \{n \in \mathbb{N} \ : \ n \in A\} = A,$$

and

$$T(S(a))(n) = \begin{cases} 1 & \text{if } n \in S(a) \\ 0 & \text{if } n \notin S(a) \end{cases} = \begin{cases} 1 & \text{if } a(n) = 1 \\ 0 & \text{if } a(n) = 0 \end{cases} = a(n).$$

Thus, $S \circ T = \mathrm{Id}_{\wp(\mathbb{N})}$ and $T \circ S = \mathrm{Id}_{\mathbb{B}}$, whence S and T are mutually inverse bijections. □

Proposition 6.29. *$\wp(\mathbb{N})$ is uncountable.*

Proof. We know by Lemma 6.28 that $|\wp(\mathbb{N})| = |\mathbb{B}|$, so we prove that $\mathbb{B}$ is uncountable. Suppose towards a contradiction that we have a bijection $f : \mathbb{N} \to \mathbb{B}$. Such a bijection constitutes a "list" of all the elements of $\mathbb{B}$, numbered by natural numbers as follows: $a_0 := f(0)$, $a_1 := f(1)$, $a_2 := f(2)$, etc., where $\{a_i\}_{i \in \mathbb{N}} \in \mathbb{B}$ is

a complete list of all the elements of $\mathbb{B}$. We will get a contradiction by exhibiting an element of $\mathbb{B}$, which is not in our list.

Write out each sequence $a_i \in \mathbb{B}$ with bits as $a_i = a_{i,0}\ a_{i,1}\ a_{i,2}\ a_{i,3}\ \ldots$, where each $a_{i,j} \in \{0, 1\}$. Then, our supposedly complete list of elements of $\mathbb{B}$ looks like the following:

$$\begin{aligned} f(0) = a_0 &= a_{0,0}\ a_{0,1}\ a_{0,2}\ a_{0,3}\ \ldots \\ f(1) = a_1 &= a_{1,0}\ a_{1,1}\ a_{1,2}\ a_{1,3}\ \ldots \\ f(2) = a_2 &= a_{2,0}\ a_{2,1}\ a_{2,2}\ a_{2,3}\ \ldots \\ f(3) = a_3 &= a_{3,0}\ a_{3,1}\ a_{3,2}\ a_{3,3}\ \ldots \\ &\vdots \end{aligned}$$

Now, consider the sequence $x = x_0\ x_1\ x_2\ x_3\ \cdots \in \mathbb{B}$ given by $x_i \neq a_{i,i}$, i.e. it differs from the sequence a_i in the i^{th} bit (i.e. binary bit). Therefore, the sequence $x \in \mathbb{B}$ is not in our list since it differs from every sequence in our list in at least one bit, contradicting that our list is complete. □

Confusingly enough, the proof technique above is also known as **Cantor's diagonalization argument**.

Exercise 6.30. *Define a* **finite** sequence of natural numbers *to be a function $a : n \to \mathbb{N}$ for some $n \in \mathbb{N}$. Prove that the set of all such sequences is countably infinite. Hint: use Corollary 6.23.*

Exercise 6.31. *Prove that the set $A := \{a : \mathbb{N} \to \mathbb{N}\}$ of all infinite sequences of natural numbers is uncountable. Hint: Use Cantor-Bernstein-Schröder Theorem 6.6.*

This idea of taking power sets to get a larger cardinality is, in fact, far stronger than just finding one cardinality larger than that of $\mathbb{N}$. Cantor's remarkable theorem illustrates this:

Theorem 6.32 (Cantor's Theorem)**.** *Given any set A, there is no surjective function $f : A \to \wp(A)$. Therefore, $|A| \neq |\wp(A)|$*

Proof. Let $f : A \to \wp(A)$ be any function. Define a subset $S \subseteq A$ by

$$S := \{a \in A\ :\ a \notin f(a)\}.$$

We claim that S cannot be in the image of f, and thus f is not surjective. Indeed, suppose to the contrary that there is some $x \in A$ with $f(x) = S$. Then, $x \in S$ if an only if $x \notin f(x) = S$, which is a contradiction. □

Exercise 6.33. *Show that there is an injective function $A \to \wp(A)$ for any set A. Together with Cantor's Theorem, this shows that $|A|$ is strictly smaller than $|\wp(\mathbb{N})|$.*

Cantor's theorem and Exercise 6.33 show that we have infinitely many distinct infinite cardinalities[18]:

$$|\mathbb{N}| < |\wp(\mathbb{N})| < |\wp(\wp(\mathbb{N}))| < |\wp(\wp(\wp(\mathbb{N})))| < \ldots$$

But is there some cardinalities that we don't get in this way? Cantor conjectured that there are not:

Continuum Hypothesis (CH): There is no set A whose cardinality is strictly between $|\mathbb{N}|$ and $|\wp(\mathbb{N})|$.

[18] in fact, the collection of all cardinalities is too large to even be a set! It is what we call a *proper class*.

It turns out CH is undecidable under the ZFC Axioms. In other words, one can prove that one cannot prove that whether CH is true or false within ZFC Axioms. Indeed, Kurt Gödel showed in 1930 that CH is consistent with ZFC and Paul Cohen showed in 1960 that ¬CH is also consistent with ZFC (assuming ZFC itself is consistent, which cannot be demonstrated within ZFC according to Gödel's 2^{nd} Incompleteness Theorem)!

There is a more general version of the CH, which is also known to be undecidable in ZFC:

Generalized Continuum Hypothesis (GCH): There is no set A whose cardinality is strictly between $|X|$ and $|\wp(X)|$ for any set X.

FIGURE 10. Kurt Gödel (left), the father mathematical logic, and Paul Cohen (right).

Homework:

- Solve the following exercises above: 6.5, 6.14, 6.22, 6.24, 6.27, 6.30, 6.31
- Solve the following exercises from [DW]: 4.34, 4.37, 4.45

7. Set Quotients: constructing $\mathbb{Z}$, $\mathbb{Z}/n\mathbb{Z}$, and $\mathbb{Q}$

The goal of this section is to define the sets of all integers and of rational numbers and extend the arithmetic of the natural numbers to them. In doing so, we will encounter one of the most important construction in all of set theory and mathematics proper: quotients of sets by an equivalence relation. Let us begin by a motivating example.

Definition 7.1. If $a, b \in \mathbb{N}$ with $b \neq 0$ and $a = mb$ for some $m \in \mathbb{N}$, we say that a *is divisible by* b or b *divides* a (denoted $b \mid a$). We call b a *divisor* or a *factor* of a.

Example 7.2. $28 = 4 \cdot 7$, so 7 and 4 are factors dividing 28.

Exercise 7.3. *Suppose $a \mid m$ and $a \mid n$. Show that $a \mid m + n$ and $a \mid mn$.*

Definition 7.4. Fix some number $n \in \mathbb{N}$ with $n \geq 2$. We say two numbers $a, b \in \mathbb{N}$ are *congruent modulo* n if $n \mid (a - b)$, and we denote this by $a \equiv b \mod n$. The set of all numbers in $\mathbb{N}$ which are congruent to a modulo n is called *the congruence class of* a modulo n, and is denoted by $(\overline{a})_n$ or simply $\overline{a}$ when n is clear from context.

Example 7.5. The numbers $2, 7, 12, 17, \ldots$ are all congruent modulo 5. They are the congruence class $\overline{2} = \{2 + 5k : k \in \mathbb{N}\}$. Other congruence classes modulo 5 are $\overline{0} = \{5k : k \in \mathbb{N}\}$, $\overline{1} = \{1 + 5k : k \in \mathbb{N}\}$, $\overline{3} = \{3 + 5k : k \in \mathbb{N}\}$, and $\overline{4} = \{4 + 5k : k \in \mathbb{N}\}$. Together, they give us all natural numbers, i.e. $\mathbb{N} = \overline{0} \cup \overline{1} \cup \overline{2} \cup \overline{3} \cup \overline{4}$.

This congruence relation is an example of a more general phenomenon, which we now explain.

Definition 7.6. A *partition* of a set S is a family of **pairwise disjoint** subsets (called *classes*) whose union is S.

Example 7.7. The set $\{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1}\}$ of congruence classes modulo n is a partition of $\mathbb{N}$ since they are pairwise disjoint and their union is all of $\mathbb{N}$.

Definition 7.8. An *equivalence relation* on a set S is a subset R of $S \times S$ satisfying the following three conditions:

- Reflexivity: $\forall x \in S,\ (x, x) \in R$;
- Symmetry: if $(x, y) \in R$ then $(y, x) \in R$;
- Transitivity: if $(x, y) \in R$ and $(y, z) \in R$, then $(x, z) \in R$.

When $(x, y) \in R$, we say x is related to y by R (sometimes denoted xRy or $x \sim_R y$ or simply $x \sim y$ when R is understood from context). The *equivalence class* of $x \in S$ under an equivalence relation R is the set $\overline{x} := \{y \in S : (x, y) \in R\}$.

Exercise 7.9. *Decide with proof which of the following is an equivalence relation and identify the equivalence classes when it is.*

- *A relation on $\mathbb{N}$ defined by $x \sim y$ if $x \mid y$*
- *A relation on the set of humans defined by $x \sim y$ if x and y are born on the same day of the week.*
- *A relation on the set of humans defined by $x \sim y$ if x and y have the same citizenship*

Proposition 7.10. *Given an equivalence relation $\sim$ on a set S, the set of equivalence classes under $\sim$ is a partition of S. Conversely, every partition of S arises in this way.*

Proof. Let P denote the set of all equivalence classes under $\sim$, and let $A, B \in P$ be two such equivalence classes. Suppose that there is some $x \in A \cap B$. Then, for any $a \in A$ and any $b \in B$, we have $a \sim x$ and $b \sim x$ (and hence $x \sim b$ by symmetry), so by transitivity $a \sim b$, so that $A = B$; hence, any two equivalence classes are disjoint. To see that $\bigcup P = S$, simply observe that any $x \in S$ lies in $\overline{x} := \{y \in S : x \sim y\} \in P$ by reflexivity.

Conversely, let P be a partition of S, i.e. a set of disjoint classes whose union is all of S. Then, we can define a relation $\sim$ on S by $x \sim y$ if both x and y lie in some common $A \in P$. It is easy to check that this is an equivalence relation. □

Definition 7.11. The *quotient* $S/\sim$ of a S by an equivalence relation $\sim$ is the set of its equivalence classes.

Example 7.12. If $\sim$ is the relation of congruence modulo n, then $\mathbb{N}/\sim = \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1}\}$.

Definition 7.13. Define an equivalence relation on $\mathbb{N} \times \{0, 1\}$ by $(n, s) \sim (m, t)$ if $n = m = 0$ or if $(n, s) = (m, t)$. The quotient set $\mathbb{Z} := \mathbb{N}/\sim$ is the set of *integers*. We also define the set of *positive integers* and the set of *negative integers* as $\mathbb{Z}_+ := \{\overline{(n,0)} \ : \ n \in \mathbb{N}, n \neq 0\}$ and $\mathbb{Z}_- = \{\overline{(n,1)} \ : \ n \in \mathbb{N}, n \neq 0\}$, respectively.

As a shorthand, if $k := \overline{(n, j)} \in \mathbb{Z}$, we let by $-k := \overline{(n, 1-j)} \in \mathbb{Z}$ (notice that our relation says nothing more than $0 \sim -0$ in this notation). Furthermore, we extend the arithmetic of $\mathbb{N}$ to $\mathbb{Z}$ by the following axioms:

- $k + (-k) = 0 = (-k) + k$ for all $k \in \mathbb{Z}$;
- $(-1) \cdot k = -k = k \cdot (-1)$ for all $k \in \mathbb{Z}$.

Exercise 7.14. *Check that the relation defining $\mathbb{Z}$ is an equivalence relation.*

Exercise 7.15. *Show that $k + 0 = k = 0 + k$ and that $k \cdot 1 = k = 1 \cdot k$ for all $k \in \mathbb{Z}$*

Exercise 7.16. *Show that $+$ and $\cdot$ are commutative and associative operations on $\mathbb{Z}$ and $\cdot$ distributes over $+$.*

Remark 7.17. Henceforth, we will not distinguish between $\mathbb{N}$ and $\mathbb{Z}_+ \cup \{\overline{(0,0)}\} \subseteq \mathbb{Z}$ even though they are technically different sets. For example, we will abuse notation and talk about an integer $k = \overline{(n, i)}$ being a natural number when $i = 0$ or $n = 0$, and we will write $k \in \mathbb{N}$ when we really mean $n \in \mathbb{N}$.

Notation 7.18. We denote by $a - b := a + (-b)$ for any $a, b \in \mathbb{Z}$ and $|a| = \begin{cases} -a & \text{if } a \in \mathbb{Z}_- \\ a & \text{otherwise} \end{cases}$.

Definition 7.19. We extend the order relation $<$ from $\mathbb{N}$ to $\mathbb{Z}$ by

- $-a < b$ when $a \in \mathbb{Z}_+$ and $b \in \mathbb{N}$;
- $-a < -b$ when $b < a$ for all $a, b \in \mathbb{Z}$.

Exercise 7.20. *Show that for all $a, b, c \in \mathbb{Z}$, we have*

- *if $a < b$ and $b < c$ then $a < c$*

- *exactly one of statements "$a = b$", "$a < b$" and "$b < a$" holds.*

We can extend the notions of divisibility of natural numbers and congruence modulo a natural number to all integers in the same fashion.

Definition 7.21. If $a, b \in \mathbb{Z}$ with $b \neq 0$ and $a = mb$ for some $m \in \mathbb{Z}$, we say that a *is divisible by* b, denoted $b \mid a$. We say two numbers $a, b \in \mathbb{Z}$ are *congruent modulo* n if $n \mid (a - b)$, and we denote this by $a \equiv b \mod n$.

Example 7.22. The congruence classes modulo 3 in $\mathbb{Z}$ are $\{\overline{0}, \overline{1}, \overline{2}\}$, where $\overline{k} = \{k + 3n \ : \ n \in \mathbb{Z}\}$. For example, $\overline{2} = \{\ldots, -7, -4, -1, 2, 5, 8\}$.

Exercise 7.23. *Fix a natural number $n \in \mathbb{N}$ with $n \geq 1$. Show that the congruence relation defined by $a \sim b$ if $a \equiv b \mod n$ is an equivalence relation on all of $\mathbb{Z}$, and identify its equivalence classes.*

Definition 7.24. Let $\mathbb{Z}/n\mathbb{Z}$ denote the quotient of $\mathbb{Z}$ by the equivalence relation on $\mathbb{Z}$ of congruence modulo n.

We would like to extend the arithmetic of $\mathbb{Z}$ to its quotients $\mathbb{Z}/n\mathbb{Z}$. The obvious way is to define $\overline{a}+\overline{b} = \overline{a+b}$ and $\overline{a} \cdot \overline{b} = \overline{a \cdot b}$. For example, if $n = 5$, we define $\overline{2} + \overline{4}$ to be $\overline{2+4} = \overline{1}$. But then we have to worry a little bit. What if we choose different elements from the same classes (i.e. different representatives of $\overline{2}$ and $\overline{4}$ such as 7 and 14 and add these instead? Do we get the same answer? In this case, the answer is yes since $\overline{7+14} = \overline{21} = \overline{1}$. But we would like to ensure that this works for any choice of representatives since otherwise our operations cannot be defined in this way. If this is the case, we say our operations are *well-defined* on the quotient set.

Remark 7.25. Every time you define an operation/function on a quotient of a set S by some relation $\sim$ using an operation/function on the original set S, you have to ensure that the operation is *well-defined*; that is, you have to ensure that different representative of the same equivalence class give the same answer.

Theorem 7.26. *The operations $+ : \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ and $\cdot : \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ given by $\overline{a} + \overline{b} = \overline{a+b}$ and $\overline{a} \cdot \overline{b} = \overline{a \cdot b}$ are well-defined, commutative, and associative.*

Proof for addition. To check that addition is well-defined, suppose $a \equiv a' \mod n$ and $b \equiv b' \mod n$. We need to check that $a + b$ and $a' + b'$ belong to the same congruence class, so that it does not matter which representative we picked to define addition. In other words we wish to show that $a + b \equiv a' + b' \mod n$. Indeed, since $n \mid (a - a')$ and $n \mid (b - b')$, there are integers j and k such that $a - a' = jn$ and $b - b' = kn$. Adding the two equations, we get

$$(a + b) - (a' + b') = a - a' + b - b' = jn + kn = (j + k)n,$$

whence $n \mid ((a + b) - (a' + b'))$, or equivalently, $a + b \equiv a' + b' \mod n$. This proves that addition is well-defined on $\mathbb{Z}/n\mathbb{Z}$.

To see that addition is commutative and associative, observe that

$$\overline{a} + \overline{b} := \overline{a+b} = \overline{b+a} =: \overline{b} + \overline{a}$$

$$(\overline{a} + \overline{b}) + \overline{c} := (\overline{a+b}) + \overline{c} := \overline{(a+b)+c} = \overline{a+(b+c)} =: \overline{a} + (\overline{b+c}) =: \overline{a} + (\overline{b} + \overline{c}),$$

where the middle equalities are by commutativity and associativity of addition in $\mathbb{Z}$. □

Exercise 7.27. *Complete the proof of Theorem 7.26 by showing that multiplication is well-defined, commutative, and associative.*

Definition 7.28. The set $\mathbb{Q}$ of *rational numbers* is defined as the quotient of $\mathbb{Z} \times \mathbb{Z}_+$ by the equivalence relation given by $(a, b) \sim (c, d)$ if $ad = bc$. We represent rational numbers by *fractions* $\frac{a}{b} := \overline{(a, b)}$. Moreover, we endow the rational numbers with the operations addition $+ : \mathbb{Q} \times \mathbb{Q} \to \mathbb{Q}$ and multiplication $\cdot : \mathbb{Q} \times \mathbb{Q} \to \mathbb{Q}$ defined by

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}, \qquad \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}.$$

We also extend $<$ from $\mathbb{Z}$ to $\mathbb{Q}$ by declaring

$$\frac{a}{b} < \frac{c}{d} \quad \text{in } \mathbb{Q} \iff ad < bc \quad \text{in } \mathbb{Z}.$$

Remark 7.29. An integer $n \in \mathbb{Z}$ can be thought of as the rational number $\frac{n}{1} \in \mathbb{Q}$, so we will once again abuse notation and consider them to be one and the same, thinking of $\mathbb{Z}$ as a subset of $\mathbb{Q}$.

Proposition 7.30. *The operations $+$ and $\cdot$ of Definition 7.28 are well-defined on $\mathbb{Q}$.*

Proof. Suppose $\frac{a}{b} = \frac{a'}{b'}$ and $\frac{c}{d} = \frac{c'}{d'}$. Then, by definition of the equivalence relation defining $\mathbb{Q}$, we have

$$ab' = a'b \tag{1}$$

$$cd' = c'd \tag{2}$$

and . Note that addition is well-defined if and only if

$$\frac{a}{b} + \frac{c}{d} := \frac{ad + bc}{bd} = \frac{a'd' + b'c'}{b'd'} =: \frac{a'}{b'} + \frac{c'}{d'} \iff b'd'(ad + bc) = bd(a'd' + b'c'),$$

so we wish to prove the latter. Indeed,

$$b'd'(ad + bc) = (ab')(dd') + (bb')(cd') = (a'b)(dd') + (bb')(c'd) = bd(a'd' + b'c'),$$

where the middle equality is by (1) and (2), and the first and last equalities follow by commutativity, associativity and distributivity of a addition and multiplication of integers.

Similarly, multiplication is well-defined if and only if

$$\frac{a}{b} \cdot \frac{c}{d} := \frac{ac}{bd} = \frac{a'c'}{b'd'} =: \frac{a'}{b'} \cdot \frac{c'}{d'} \iff acb'd' = a'c'bd,$$

but the last equation simply follows by multiplying equations (1) and (2) together and rearranging by commutativity of multiplication of integers. □

Exercise 7.31. *Show that the operation $\frac{a}{b} \# \frac{c}{d} := \frac{a + b}{c + d}$ is not well-defined on $\mathbb{Q}$.*

Exercise 7.32. *Show that $\mathbb{Q}$ is countably infinite.*

Definition 7.33. A *field* $(\mathbb{F}, +, \cdot, 1, 0)$ is a set $\mathbb{F}$ together with elements $0, 1 \in \mathbb{F}$ and operations $+ : \mathbb{F} \times \mathbb{F} \to \mathbb{F}$ and $\cdot : \mathbb{F} \times \mathbb{F} \to \mathbb{F}$ satisfying the following axioms:

- *additive identity*: $\forall x \in \mathbb{F}\ ,\ x + 0 = x = 0 + x$;

- addition is associative: $\forall x, y, z \in \mathbb{F}\ ,\ (x + y) + z = x + (y + z)$;
- addition is commutative: $\forall x, y \in \mathbb{F}\ ,\ x + y = y + x$;
- additive inverses: $\forall x \in \mathbb{F}\ \exists y \in \mathbb{F}\ ,\ x + y = 0 = y + x$;
- *multiplicative identity*: $\forall x \in \mathbb{F}\ ,\ x \cdot 1 = x = 1 \cdot x$;
- multiplication is associative: $\forall x, y, z \in \mathbb{F}\ ,\ (x \cdot y) \cdot z = x \cdot (y \cdot z)$;
- multiplication is commutative: $\forall x, y \in \mathbb{F}\ ,\ x \cdot y = y \cdot x$;
- multiplicative inverses: $\forall x \in \mathbb{F} \setminus \{0\}\ ,\ \exists y \in \mathbb{F}\ ,\ x \cdot y = 1 = y \cdot x$;
- distibutivity: $\forall x, y, z \in \mathbb{F}\ ,\ x \cdot (y + z) = x \cdot y + x \cdot z$

Exercise 7.34. *Prove that* $(\mathbb{Q}, +, \cdot, 1, 0)$ *is a field.*

Exercise 7.35. *Give a positive integer* n *such that* $\mathbb{Z}/n\mathbb{Z}$ *is a field and another when it is not. Which of the field axioms fails?*

Now that we finally have a field, we can do a lot of mathematics in it. Still, some things which we wish were numbers are not (or at least, not yet) as the following example shows:

Proposition 7.36. *There is no rational number* x *satisfying* $x^2 = 2$.

First Proof. Suppose towards a contradiction that such a number $x = \dfrac{a}{b} \in \mathbb{Q}$ exists. We may assume that a and b share no common divisors since we can simply reduce the fraction to its simplest form. Then, we get

$$2 = x^2 = \frac{a^2}{b^2} \implies a^2 = 2b^2 \implies 2 \mid a^2.$$

but the only way a^2 is even is if a itself is even (prove it!), so

$$2 \mid a \implies a = 2k \implies 2b^2 = (2k)^2 = 4k^2 \implies 2 \mid b^2 \implies 2 \mid b.$$

But this shows that 2 is a common divisor of a and b contradicting our assumption. □

Second Proof. Suppose towards a contradiction that such a number $x = \dfrac{a}{b} \in \mathbb{Q}$ exists. We may assume that b is as small as possible. We shall arrive at a contradiction by finding a fraction $\dfrac{a'}{b'} = x$ with $b' < b$. Since $x^2 = 2$ and $1^2 = 1$ and $2^2 = 4$, it follows that $1 < x < 2$ as squaring positive integers preserves the order of inequalities. Now,

$$1 < \frac{a}{b} < 2 \implies b < a < 2b \implies 0 < a - b < b.$$

So, setting $a' = 2b - a$ and $b' = a - b$, we get

$$\frac{a'}{b'} = \frac{2b - a}{a - b} = \frac{b(2b - a)}{b(a - b)} = \frac{2b^2 - ab}{b(a - b)} = \frac{a^2 - ab}{b(a - b)} = \frac{a(a - b)}{b(a - b)} = \frac{a}{b} = x,$$

where we used $x^2 = 2 \iff a^2 = 2b^2$ in the fourth equality. But now $\dfrac{a'}{b'}$ is a fraction with denominator $b' = a - b < b$, contradicting our assumption. □

Remark 7.37. The second proof above is an example of the so-called **proof by infinite descent**. We assume something exists and we show something smaller exists (in this case a fraction with a smaller denominator). But if we know we cannot keep decreasing forever (in this case because the denominator is a positive integer), we get a contradiction.

Exercise 7.38. *Show that*

- *there are no rational numbers x such that $x^3 = 2$.*
- *there are no rational numbers x such that $x^2 = 3$.*

Exercise 7.39. *Show that for any positive integer n, we can find a rational number q such that $|q^2 - 2| < \frac{1}{n}$. In other words, there are rational numbers whose square is **arbitrarily close** to 2.*

Proposition 7.36 and Exercise 7.39 really show that if we arrange the rational numbers on a line using the $<$ relation, there is really a "hole" at $\sqrt{2}$. We can get as close as we want to it, but no rational number sits there. In Section 9, we will see how to fill all these holes in $\mathbb{Q}$.

Homework:

- Solve the following exercises above: 7.3, 7.9, 7.14, 7.15, 7.23, 7.27, 7.31, 7.32, 7.35, 7.38, 7.39.

8. Prime Numbers: an Invitation to Number Theory

Definition 8.1. A natural number other than 1 is called *prime* if its only factors are 1 and itself.

The first few prime numbers are $2, 3, 5, 7, 11, 13, 17, 19, \ldots$. The number 1 also has no divisors other than itself, but we don't consider it a prime. One may wonder if this sequence is infinite, and the answer is yes as was proved by Euclid (see Theorem 8.15 below).

Definition 8.2. Two integers m and n are called *coprime* or *relatively prime* if they have no common divisor greater than 1. For two integers m and n, we denote by $\gcd(m, n)$ the greatest common divisor of m and n. Thus, m and n are, by definition coprime if and only if $\gcd(m, n) = 1$.

Example 8.3. 4 is coprime with 21 since $\gcd(4, 21) = 1$, but 4 and -6 are not coprime since $\gcd(4, -6) = 2$.

Theorem 8.4 (Bézout)**.** *If a and b are coprime integers, there exists integers m and n such that $ma+nb = 1$.*

Proof. Since m and n are allowed to be negative and multiplying by -1 does not affect the condition of being coprime, we may assume that a and b are positive. Assume without loss of generality that $a \geq b$ (since otherwise, we can simply switch a and b). When $a = b$ or when $b = 0$, the numbers are not coprime unless $a = 1$; so we can simply take $(m, n) = (1, 0)$ in this case.

Next, we proceed by strong induction on $a + b$ to prove the remaining cases. We already proved the result when $a + b = 1$. Assume the claim holds for all pairs (a, b) with $a + b < k$ for some $k \in \mathbb{N}$, and let us consider a pair (a, b) satisfying $a + b = k$. We already dealt with the case when $b = 0$, so let us assume further that $b > 0$. Note that the pair $(b, a - b)$ is coprime if (a, b) is: indeed, if $d \mid b$ and $d \mid (a - b)$ then $d \mid a$ as well. Moreover, $b + (a - b) = a < a + b = k$, so by our induction hypothesis, there exists integers m and n with $mb + n(a - b) = 1$. But then, we get $na + (m - n)b = 1$, which is the desired expression. This completes the induction step. □

Corollary 8.5. *Given integers a and n, if $\gcd(a, n) = 1$, then there exists $b \in \mathbb{Z}$ satisfying $ab \equiv 1 \mod n$ (in this case, $\overline{b}$ is called the multiplicative inverse of $\overline{a}$ in $\mathbb{Z}/n\mathbb{Z}$).*

Proof. Conversely, if $\gcd(a, n) = 1$, then by Theorem 8.4, we have some integers $b, k \in \mathbb{Z}$ satisfying $ba+kn = 1$, or equivalently, $ba - 1 = kn$ so $ab \equiv 1 \mod n$. □

Definition 8.6. For fixed $a, b \in \mathbb{Z}$, the set of *integer combinations* of a and b is the set $\{ma + nb : m, n \in \mathbb{Z}\}$.

Theorem 8.7 (Generalized Bézout's Lemma)**.** *The set of integer combinations of a and b is the set of multiples of $\gcd(a, b)$.*

Proof. Let $d = \gcd(a, b)$, and let $T := \{kd : k \in \mathbb{Z}\}$ be the set of multiples of d. Further, denote the set of integer combinations of a and b by $S := \{ma + nb : m, n \in \mathbb{Z}\}$.

First, we prove $S \subseteq T$. Since d divides both a and b, we have integers $j, k \in \mathbb{Z}$ such that $a = jd$ and $b = kd$. Thus,

$$ma + nb = mjd + nkd = (mj + nk)d,$$

so any integer combination of a and b is indeed a multiple of d.

To prove $T \subseteq S$, note that a/d and b/d, have no divisors in common greater than 1 since if they did, that would imply that d was not the *greatest* common divisor; so a/d and b/d are coprime. By Theorem 8.4, we have $m, n \in \mathbb{Z}$ such that

$$ma/d + nb/d = 1 \implies ma + nb = d \implies (km)a + (kn)b = kd,$$

for any $k \in \mathbb{Z}$ and hence any multiple kd of d can be expressed as an integer combination of a and b. □

Exercise 8.8. *Prove the converse of Corollary 8.5: if $\overline{a}$ has a multiplicative inverse in $\mathbb{Z}/n\mathbb{Z}$, then a and n are coprime.*

Exercise 8.9. *$\mathbb{Z}/n\mathbb{Z}$ is a field if and only if n is prime.*

Lemma 8.10. *If a and b are coprime and $a \mid qb$ then $a \mid q$.*

Proof. By Theorem 8.4, we have $m, n \in \mathbb{Z}$ such that $ma + nb = 1$. Thus, $q = maq + nbq$. But then a divides both terms on the right-hand side (since a divides itself as well as bq), and hence a also divides their sum q. □

Proposition 8.11. *If p is a prime which divides the product $a_1 a_2 \dots a_k$ of k integers, then $p \mid a_i$ for some i*

Proof. We proceed by induction on k. The statement is trivial when $k = 1$. Assume the claim holds for a given $k \geq 1$, and now suppose $p \mid a_1 a_2 \dots a_k a_{k+1}$. Let $q = a_1 a_2 \dots a_k$ and $b = a_{k+1}$, so that $p \mid qb$. If $p \mid b = a_{k+1}$, we are done; otherwise, by Lemma 8.10, $p \mid q = a_1 a_2 \dots a_k$, so by our induction hypothesis, p divides a_i for some $i \in \{1, 2, \dots, k\}$, and we are also done. □

Definition 8.12. A *prime factorization* of n is an expression $n = p_1^{\nu_1} p_2^{\nu_2} \dots p_k^{\nu_k}$ of n as a product of powers of distinct primes $p_1, p_2, \dots, p_k$. We call ν_i the multiplicity of p_i in n.

Theorem 8.13 (The Fundamental Theorem of Arithmetic)**.** *Every positive integer has a prime factorization which is unique, up to reordering of the factors.*

Proof. We proceed by strong induction on n. For $n = 1$, we can write n as the empty product, i.e. the product of no integers is, by convention, 1. Assume every positive integer less than k has a unique prime factorization. Let S be the set of integer divisors of k larger than 1. Since S is nonempty (e.g. $k \in S$), there is a smallest element p of S by the Well-Ordering Principle (Theorem 4.16); moreover, p must be prime since otherwise, p has a smaller divisor, which would also divide k.

By Proposition 8.11, p appears in every prime factorization of k. Thus, every prime factorization of k consists of p and a prime factorization for k/p. But, by the induction hypothesis, a unique prime factorization for k/p exists. Hence, there's exactly one prime factorization of k, namely, the one acquired by adding 1 to the multiplicity of p in the unique prime factorization of k/p. □

Exercise 8.14. *If a and b are coprime integers, both dividing some $n \in \mathbb{Z}$. Show that $ab \mid n$.*

Theorem 8.15 (Euclid)**.** *There are infinitely many prime numbers.*

Proof. Assume towards a contradiction that we have a finite set $P = \{p_1, p_2, \dots, p_n\}$ of all prime numbers. Now consider the number $N = 1 + \prod_{i=1}^{n} p_i$. Observe that $N \equiv 1 \mod p_i$ for every $p_i \in P$. Thus, $N > 1$ is has no prime divisors, contradicting Theorem 8.13. □

Theorem 8.7 tells us that we can find a pair of integers m and n such that $ma + nb = \gcd(a, b)$ for any integers a, b. However, it does not tell us how to find such numbers. The following result will help us figure out an algorithm for finding this integer combination.

Lemma 8.16. *Given any integers a, b, and k, we have* $\gcd(a, b) = \gcd(a - kb, b)$.

Proof. If $d \mid a$ and $d \mid b$, then $d \mid a - kb$. Conversely, if $d \mid a - kb$ and $d \mid b$, then $d \mid (a - kb) + kb = a$. Thus, the greatest common divisor of the pair (a, b) is the same as that of $(a - kb, b)$. □

Exercise 8.17. *If a and b are integers with $b \neq 0$, there there is a unique integer pair q, r such that $a = qb + r$ and $0 \leq r \leq |b| - 1$.*

Euclidean Algorithm: To find $\gcd(a, b)$ for two integers a and b not both zero:

(1) if either a or b is zero, return the other number as the output;
(2) otherwise, replace the maximum of a and b by its remainder upon division by the other number to get a new pair (a', b') and go back to step (1).

Example 8.18. Let's find $\gcd(154, 35)$.

$$\begin{aligned} &\gcd(154, 35) && 154 = 4 \cdot 35 + 14 \\ =&\gcd(14, 35) && 35 = 2 \cdot 14 + 7 \\ =&\gcd(14, 7) && 14 = 2 \cdot 7 + 0 \\ =&\gcd(0, 7) = 7 \end{aligned}$$

Now, observe that working backwards, we get the the integer combination we want:

$$7 = 35 - 2 \cdot 14 = 35 - 2 \cdot (154 - 4 \cdot 35) = (-2) \cdot 154 + 9 \cdot 35.$$

Exercise 8.19. *Find the greatest common divisor of $a = 261$ and $b = 54$ using the Euclidean algorithm, and reverse your steps to express it as an integer combination of a and b.*

Theorem 8.20. *The Euclidean algorithm applied to $a \geq b \geq 0$ with $a \neq 0$ terminates in a finite number of steps and outputs the* $\gcd(a, b)$.

Proof. We proceed by strong induction on b, the smaller of the two integers of the input. If $b = 0$, the algorithm returns $a = \gcd(a, b)$. Suppose, that the algorithm terminates and returns the greatest common divisor whenever the smaller input is less than b.

Now, consider the input $a \geq b \geq 1$. Let $a = kb + r$ with $r < b$ (possible by Exercise 8.17). Then, by the induction hypothesis, the algorithm eventually terminates and computes $\gcd(r, b) = \gcd(a - kb, b)$, which is the same as $\gcd(a, b)$ by Lemma 8.16. □

Some Applications and Examples:

Example 8.21.

Homework:

- Read [DW] pp. 123–128 and pp. 142-145 (stop at "applications")
- Solve the following exercises from [DW]: 6.16, 6.18, 6.28, 6.29, 7.3, 7.8, 7.19, 7.23, 7.24, 7.30
- **Optional:** Solve the following exercises above: 8.9

9. The Real Numbers

Recall from Section 7, we showed that, even though there are rational numbers whose square arbitrarily close to 2, no rational number exists whose square is exactly equal to 2. The same is true if we replace 2 by $3, 5, 6, \ldots$, or if we replace "square root" by "cube root or higher radicals. Visualizing the rational numbers as sitting on a line using the order relation $<$, we see that the are a lot of missing numbers or "holes" on the line. In fact, between any two rational numbers, there is such a hole (in fact, there are infinitely many such holes). For example, between $\frac{1}{2} = \frac{1}{\sqrt{4}}$ and $\frac{1}{3} = \frac{1}{\sqrt{9}}$ we have holes at $\frac{1}{\sqrt{5}}$, $\frac{1}{\sqrt{6}}$, $\frac{1}{\sqrt{7}}$, $\frac{1}{\sqrt{8}}$, $\frac{1}{\sqrt{5}}$ and also at $\frac{2}{\sqrt{21}}$, $\frac{2}{\sqrt{22}}$, $\ldots$.

Exercise 9.1. *Show that $\frac{1}{\sqrt{5}}$ is irrational; that is show that there is no $r \in \mathbb{Q}$ satisfying $\frac{1}{r^2} = 5$.*

One way to formalize the existence of such holes is by noting that there are subsets of $\mathbb{Q}$ such as $\{r \in \mathbb{Q} : r^2 < 2\}$ whose boundary is missing. Our goal in this section is to *complete* the field of rational numbers by creating a extension of $\mathbb{Q}$ which contains all these missing boundary points.

Definition 9.2 (Dedekind Cuts)**.** A *cut* in $\mathbb{Q}$ is an ordered pair $A|B$ of subsets $A, B \subseteq \mathbb{Q}$:

(1) A and B are disjoint nonempty subsets of $\mathbb{Q}$ with $A \cup B = \mathbb{Q}$
(2) if $a \in A$ and $b \in B$ then $a < b$,
(3) A contains no largest element.

We call A the left-hand part of the cut and B the right-hand part.

Making a semantic leap, we make the following definition:

Definition 9.3. A *real number* is defined as a cut in $\mathbb{Q}$. The set of all real numbers is denoted $\mathbb{R}$.[19]

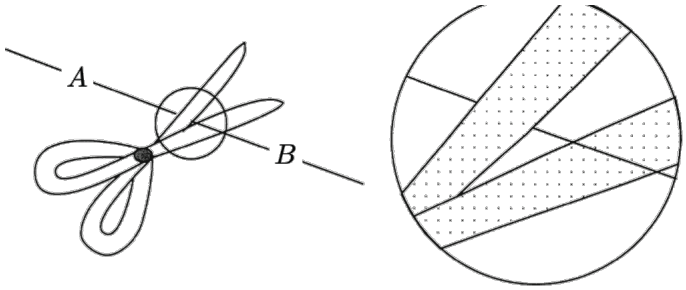


Figure 11. A Dedekind cut on the rational number line

Two basic examples of cuts are:

(1) The rational cut at 1: $\{r \in \mathbb{Q} : r < 1\} \mid \{r \in \mathbb{Q} : r \geq 1\}$.
(2) The cut that corresponds to $\sqrt{2}$:

$$\{r \in \mathbb{Q} : r \leq 0 \text{ or } r^2 < 2\} \mid \{r \in \mathbb{Q} : r > 0 \text{ and } r^2 \geq 2\}.$$

[19] A different (but equivalent) standard approach for defining $\mathbb{R}$ is via Cauchy sequences, typically treated in a course in real analysis.

It is convenient to call a cut of type (1) a *rational cut*. If $c \in \mathbb{Q}$ let c^* denote the rational cut at c, i.e.

$$c^* := \{r \in \mathbb{Q} : r < c\}|\{r \in \mathbb{Q} : r \geq c\}$$

Identifying c with c^* embeds the ordered field $\mathbb{Q}$ inside $\mathbb{R}$. Thus, we think of the sets of numbers we defined so far as embedded within each other as usual:

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

There is an obvious order relation $x \leq y$ on cuts defined as follows:

Definition 9.4. If $x = A|B$ and $y = C|D$ are real numbers, we say $x \leq y$ if $A \subset C$. We say $x < y$ if $x \leq y$ and $x \neq y$.

Note that if $r, s \in \mathbb{Q}$ and $r < s$ is $\mathbb{Q}$, then it remains true that $r^* < s^*$ in $\mathbb{R}$. So the order relation of $\mathbb{R}$ extends that of $\mathbb{Q}$.

Definition 9.5. A subset $S \subseteq \mathbb{R}$ is called *bounded above* if there exists $M \in \mathbb{R}$ such that for all $x \in S$, we have $x \leq M$. Such M is called an *upper bound* for S. A *least upper bound* or a *supremum* is an upper bound which is smaller than all other upper bounds.

Exercise 9.6. *Find with proof the supremum of each of the following subsets of* $\mathbb{R}$ *if they exist:*

- $\{x \in \mathbb{R} : x < r^*\}$ *for some fixed* $r \in \mathbb{Q}$.
- $\{x \in \mathbb{R} : x \leq r^*\}$ *for some fixed* $r \in \mathbb{Q}$.
- $\{x \in \mathbb{R} : x < \sqrt{2}\}$ *where* $\sqrt{2} := \{r \in \mathbb{Q} : r \leq 0 \text{ or } r^2 < 2\} \mid \{r \in \mathbb{Q} : r > 0 \text{ and } r^2 \geq 2\}$.
- $\mathbb{Z}_+$.
- $\mathbb{Z}_-$.

Theorem 9.7 (Least Upper Bound Property)**.** *The set* $\mathbb{R}$ *is* complete *in the following sense: if* $S \subseteq \mathbb{R}$ *is nonempty and bounded above then* S *has a least upper bound in* $\mathbb{R}$.

Proof. Let $\mathscr{C} \subseteq \mathbb{R}$ be a nonempty collection of cuts bounded above by some cut $X|Y$. Define

$$C := \{a \in \mathbb{Q} : a \in A \text{ for some } A|B \in \mathscr{C}\}$$

and let D be the complement of C in $\mathbb{Q}$. Then $z = C|D$ is a cut. For every member $A|B \in \mathscr{C}$ we have $A \subseteq C$, so z is an upper bound of $\mathscr{C}$. If z' is any other upper bound of $\mathscr{C}$, with $z' = C'|D'$, then, for each $A|B \in \mathscr{C}$, we have $A \subseteq C'$ since z', hence $C = \bigcup_{x=A|B\in\mathscr{C}} A \subseteq C'$, so $z \leq z'$. Thus z is the least upper bound. □

The simplicity of this proof is why cuts are a very effective way to define $\mathbb{R}$. This least upper bound property really shows that we do indeed have no holes in $\mathbb{R}$. The following exercise shows that this property does not hold for $\mathbb{Q}$.

Exercise 9.8. *Find with proof a subset* $S \subseteq \mathbb{Q}$ *such that there is an infinite sequence of rational upper bounds* $M_1 > M_2 > M_3 > \ldots$ *with* $x \leq M_i$ *for all* $x \in \mathbb{Q}$*, but there is no smallest rational upper bound* $M \in \mathbb{Q}$ *with* $M < M_i$ *for all* $i \in \mathbb{Z}_+$. *Hint: Take* $S = \{r \in \mathbb{Q} : r^2 < 2\}$

After filling all these holes, how much did we add. It turns out, we actually had to add uncountably many numbers! The following exercise demonstrates this

Exercise 9.9. *(1) Find an injective function $\alpha : \mathbb{R} \to \wp(\mathbb{Q})$.*
(2) Deduce that $|\mathbb{R}| \leq |\wp(\mathbb{N})|$.
(3) Consider the set $I \subset \mathbb{R}$ given by $I := \{x \in \mathbb{R} : 0^* \leq x \leq 1^*\}$. Let $\mathbb{B} = \{\{a_i\}_{i\in\mathbb{N}} : a_i \in \{0,1\}\}$ be the set of all infinite binary sequences. Define a function $f : \mathbb{N} \times \{0,1\} \to \mathbb{Q}$ by

$$f(i,a) = \begin{cases} \frac{1}{2^i} & a = 1 \\ 0 & a = 0 \end{cases}.$$

Now, define a function $\beta : \mathbb{B} \to \mathbb{R}$ by taking $\beta(\{a_i\}_{i\in\mathbb{N}}) := A|B$ where

$$A := \left\{ r \in \mathbb{Q} : \exists N \in \mathbb{N},\ r < \sum_{i=0}^{N} f(i,a_i) \right\} \quad B := \mathbb{Q} \setminus A.$$

Show that β is injective.
(4) Using Lemma 6.28, deduce that $|\mathbb{R}| = |\wp(\mathbb{N})|$, it particular, $\mathbb{R}$ is uncountable.
(5) Deduce that the set $\mathbb{R} \setminus \mathbb{Q}$ of irrational numbers *is uncountable.*

This really shows how unimaginably (quite literally) huge the real numbers are. In fact, given any language that has a finite number of symbols in it, all sentences of that language form a countably infinite set; it follows that most real numbers are literally indescribable by any human language!

Our next task is to extend the arithmetic operations of $\mathbb{Q}$ to $\mathbb{R}$.

Definition 9.10. Given real numbers $x = A|B$ and $y = C|D$ define their sum $x + y := E|F$ by

$$E := \{r \in \mathbb{Q} : \exists a \in A,\ \exists c \in C, r = a + c\}$$

$$F := \{r \in \mathbb{Q} : \exists b \in B,\ \exists d \in D, r = b + d\}$$

Exercise 9.11. *Given rational numbers $r, s \in \mathbb{Q}$ show that $r^* + s^* = (r + s)^*$. In other words, addition in $\mathbb{R}$ extends addition in $\mathbb{Q}$.*

Proposition 9.12. *Given any $x, y \in \mathbb{R}$ we have $x + y = y + x$, i.e. addition in $\mathbb{R}$ is commutative*

Proof. Let $x = A|B$ and $y = C|D$. Given a rational number $r \in \mathbb{Q}$, r is in the left cut of $x + y$ if and only if $r = a + c = c + a$ for some $a \in A$ and $c \in C$ if and only if it is in the left cut of $y + x$. □

Exercise 9.13. *Prove that for any $x, y, z \in \mathbb{R}$, we have $x + (y + z) = (x + y) + z$.*

Proposition 9.14. *For any $x \in \mathbb{R}$, we have $x + 0^* = x = 0^* + x$, i.e. 0^* is an additive identity for $\mathbb{R}$.*

Proof. Let $x = A|B$ be any cut in $\mathbb{Q}$. By definition,

$$x + 0^* = E|F, \text{ where } E = \{a + r \in \mathbb{Q} : a \in A, r < 0\} \text{ and } F = \{b + r \in \mathbb{Q} : b \in B, r \geq 0\}.$$

Since adding a negative number to an element of A makes it smaller, it still gives something in A, so we have $E \subseteq A$. Conversely, given any $a \in A$, we have some $a' \in A$ satisfying $a < a'$ since A has no largest element by definition of a cut; taking $r = a - a' < 0$, we see that $a = a' + r \in E$, so $A \subseteq E$. This proves that $A = E$.

Similarly, adding a positive number to anything in B only makes it larger and so is still in B, so $F \subset B$. And any $b \in B$ can be written as $b + 0 \in F$, so $B = F$. Thus, $x = A|B = E|F = x + 0^* = 0^* + x$, where the last equality follows by commutativity of addition. □

Definition 9.15. Given a real number $x = A|B$, define its negative $-x := -B| - A$, where

$$-B = \{r \in \mathbb{Q} : \exists b \in B,\, r = -b\}$$
$$-A = \{r \in \mathbb{Q} : \exists a \in A,\, r = -a\}$$

We further define $x - y := x + (-y)$.

Exercise 9.16. *Show that for any real number x, we have $x + (-x) = (-x) + x = 0^*$.*

Defining multiplication is trickier due to the fact that Dedekind cuts are not so well-behaved when it comes to negative numbers, so we have to be careful.

Definition 9.17. We say a real number x is *positive* if $0^* < x$ and *negative* if $x < 0^*$. We denote by $\mathbb{R}_+$ and $\mathbb{R}_-$ the sets of all positive and negative real numbers, respectively.

Definition 9.18. Given real numbers $x = A|B$ and $y = C|D$, we define their product $x \cdot y$ as follows:

- if $x, y \in \mathbb{R}_+$, let $x \cdot y := E|F$, where
$$E := \{r \in \mathbb{Q} : r \leq 0 \text{ or } \exists a \in A,\, \exists c \in C \text{ such that } a > 0, c > 0, \text{ and } r = ac\}$$
$$F := \mathbb{Q} \setminus E;$$
- if $x \in \mathbb{R}_+$ and $y \in \mathbb{R}_-$, let $x \cdot y := -(x \cdot (-y))$;
- if $x \in \mathbb{R}_-$ and $y \in \mathbb{R}_+$, let $x \cdot y := -((-x) \cdot y)$;
- if $x, y \in \mathbb{R}_-$, let $x \cdot y := (-x) \cdot (-y)$;
- if $x = 0$ or $y = 0$, let $x \cdot y = 0$.

The following exercise is a tedious check of many cases, but it is straightforward.

Exercise 9.19. *Show that multiplication in $\mathbb{R}$ is commutative, associative, distributive, and that 1^* is a multiplicative identity.*

What we have learned about the arithmetic of $\mathbb{R}$ so far can be summarized in the following theorem.

Theorem 9.20. *$\mathbb{R}$ is a field.*

The order relation on $\mathbb{R}$ enjoys some nice properties:

Proposition 9.21. *For any $x, y, z \in \mathbb{R}$,*

- *Transitivity: if $x < y$ and $y < z$ then $x < z$.*
- *Trichotomy: exactly one of the statements "$x < y$", "$y < x$", and "$x = y$" is true.*
- *Translation: if $x < y$, then $x + z < y + z$.*

Exercise 9.22. *Prove Proposition 9.21.*

Exercise 9.23 (The Triangle Inequality)**.** *For any real number x, define $|x| := \begin{cases} x & 0^* \leq x \\ -x & x < 0^* \end{cases}$. Show that for any $x, y \in \mathbb{R}$, we have $|x + y| \leq |x| + |y|$.*

These properties of $<$ mean that $\mathbb{R}$ is not only a field, but an *ordered field*. The following theorem shows that $\mathbb{R}$, despite being scary, is a canonical object in mathematics.

Theorem 9.24. $\mathbb{R}$ *is the unique complete (in the sense of Theorem 9.7) ordered field up to "isomorphism".*

We haven't defined what the word "isomorphism", but what we mean is that any other complete ordered field has to be in bijection with $\mathbb{R}$ in a way compatible with the arithmetic and order relations. To learn more about this notion, you should study some abstract algebra!

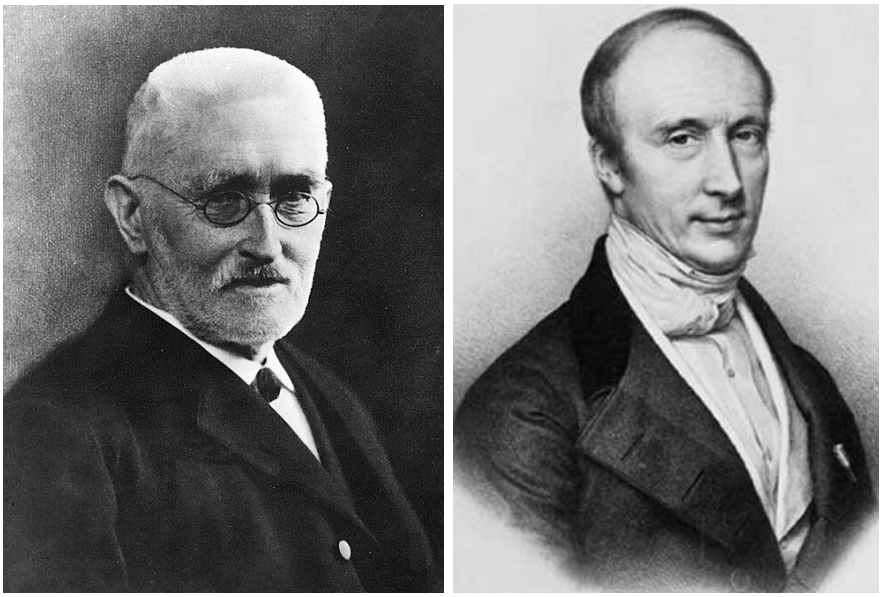


FIGURE 12. Richard Dedekind (left) and Augustin-Louis Cauchy (right) who first gave two different rigorous constructions of the real numbers.

Homework:

- Solve the following exercises above: 9.1, 9.6, 9.11, 9.16, 9.22

Optional/Bonus:

- Solve exercise 9.9 above
- Express Euler's constant e as a Dedekind cut (you may assume standard results from calculus).

Additional Problems

(1) State the definition of each of the following:
- a tautology; a contradiction; a logical equivalence; a logical implication
- The principle of deductive explosion
- Vaccuous truth
- The Axioms of Empty Set, Equality (aka. Extensionality), Pairing, Union, Restricted Comprehension, Infinity, Power Set, Regularity, Choice
- An inductive set
- The set of natural numbers
- The successor function
- Function
- Principle of mathematical induction
- The well-ordering principle
- The recursive definitions of addition and multiplication on $\mathbb{N}$
- The relation $<$ and $\leq$ on $\mathbb{N}$

(2) Given predicates $T(x, y)$: "x teaches y," and $S(y)$: "y is a student," express:
   (a) Every teacher teaches some student.
   (b) There is a student who is taught by every teacher.
   (c) Not every teacher teaches a student.

   Then, for each formula, write its formal negation and simplify.

(3) Let $P(x)$: "x is a prime number," and $E(x)$: "x is even." Formalize the statement:

"There exists exactly one even prime number."

(4) Translate the following logical formulas into precise, unambiguous English:
   (a) $\forall x(P(x) \to \exists y(B(y) \wedge R(x, y)))$
   (b) $\exists y(B(y) \wedge \forall x(P(x) \to R(x, y)))$
   (c) $\neg\exists x(S(x) \wedge \forall y\, \neg F(x, y))$

   (Here $P(x)$: person, $B(y)$: book, $R(x, y)$: x reads y, $S(x)$: student, $F(x, y)$: x fails y.)

(5) Translate the following compound statement into predicate logic:

   "If every philosopher who admires Socrates also admires Plato, then there exists someone whom every philosopher admires."

   Use:

$$P(x) : x \text{ is a philosopher},$$
$$A(x, y) : x \text{ admires } y,$$
$$s : \text{Socrates},$$
$$p : \text{Plato}.$$

(6) We consider an island inhabited by two types of people: 1) Knight: A person who *always tells the truth;* and 2) Knave: A person who *always lies.* Each inhabitant is one of these types. Determine all the possibilities of who is a knight and who is a knave whenever possible in the following situations.

   Hint: write a truth table.

   (a) You meet two people: X and Y.

X : "At least one of us is a knave."

Y says nothing.

(b) You meet a single person D, who says:

$$D: \text{“I am a knave or } 2+2=5\text{.”}$$

(c) You encounter P, Q, and R.

$$P: \text{“Exactly one of us is a knight.”}$$
$$Q: \text{“}R\text{ is a knave.”}$$
$$R: \text{“}P\text{ is a knight.”}$$

(d) Four islanders A, B, C, and D say:

$$A: \text{“}B\text{ is a knave.”}$$
$$B: \text{“}C\text{ is a knave.”}$$
$$C: \text{“}D\text{ is a knave.”}$$
$$D: \text{“}A\text{, }B\text{, and }C\text{ are all knaves.”}$$

(7) Express the proposition $P \wedge Q$ using only the connectives $\vee$ and $\neg$. Prove that your expression is logically equivalent to $P \wedge Q$ using 1) Truth tables, 2) a formal proof.

(8) Express the proposition $P \implies Q$ using only the connectives $\wedge$ and $\neg$. Prove that your expression is logically equivalent to $P \implies Q$ using 1) Truth tables, 2) a formal proof.

(9) Write a formal proof that $[(Q \vee \neg Q) \implies P] \equiv P$.

(10) Write a formal proof of the Principle of Deductive Explosion, i.e. $(Q \wedge \neg Q)$ implies P.

(11) For an implication $P \implies Q$, state
   (a) its *converse*
   (b) its *contrapositive*

   Decide which of them is equivalent to the original implication, and then,
   (a) prove that equivalence
   (b) show (via a counterexample) that the other one is not equivalent to them.

(12) Prove the identity $B \cap ((A \cap B)^c) = B - A$.

(13) Let $f : A \to B$ be a function, $X \subseteq A$, and $Y \subseteq B$. Recall that

$$f(X) := \{b \in B : \exists x \in X,\, b = f(x)\} \qquad \text{and} \qquad I_f(Y) := \{a \in A : f(a) \in Y\}.$$

   True/False:
   - $f(X^c) \subseteq f(X)^c$.
   - $f(X)^c \subseteq f(X^c)$.
   - $I_f(Y^c) \subseteq I_f(Y)^c$.
   - $I_f(Y)^c \subseteq I_f(Y^c)$.

(14) Describe the identity function $1_A : A \to A$ as a subset of $A \times A$.

(15) Define an operation on sets $A \oplus B := (A \cup B) - (A \cap B)$. Prove that $\oplus$ is associative, i.e. $(A \oplus B) \oplus C = A \oplus (B \oplus C)$

(16) State and prove de Morgan's law for sets.

(17) Let $P(x)$ be the assertion “x is odd” and $Q(x)$ be the assertion “x is a multiple of 3”. Determine whether the following statements are true:
   - $\forall x \in \mathbb{Z}\ [P(x) \implies Q(x)]$

- $[\forall x \in \mathbb{Z}\ P(x)] \implies [\forall x \in \mathbb{Z}\ Q(x)]$
- $\exists x \in \mathbb{Z}\ [Q(x) \implies P(x)]$

(18) Translate the following statements into formal logic (you may use symbols which were defined in class such as $\mathbb{N}$, $<$, $+$, etc.)
   (a) "Every natural number has a successor."
   (b) "Zero is not the successor of any natural number."
   (c) "Addition is commutative and associative for natural numbers."
   (d) "multiplication distributes over addition for natural numbers."

(19) Using induction and the recursive definitions of addition and multiplication, prove each of the following statements:
   (a) $\forall x \in \mathbb{N}\ (x + S(0) = S(x))$
   (b) $\forall x \in \mathbb{N}\ (x \cdot S(0) = x)$
   (c) $\forall x \in \mathbb{N}\ (x + 0 = 0 + x)$

(20) Prove that:
$$\forall x \in \mathbb{N} \forall y \in \mathbb{N} \forall z \in \mathbb{N}\ (x \cdot (y + z) = x \cdot y + x \cdot z).$$
Hint: Use induction on z.

(21) *Uniqueness of Zero:* Show that
$$\forall x \in \mathbb{N}\ (x + 0 = 0 \to x = 0).$$

(22) Define each of the following (as formal logic predicates using only $0, S, +, \cdot, =$):
   (a) "x is even."
   (b) "x divides y."
   (c) "x is prime."

(23) Show that for $a, b \in \mathbb{N}$, there is exactly one pair $k, r \in \mathbb{N}$ such that $0 \leq r \leq b - 1$ and $a = qb + r$.

(24) State and prove the Well-Ordering Principle for the natural numbers.

(25) State the definition of each of the following:
- Principle of mathematical induction
- Principle of strong induction
- Cantor-Schröder-Bernstein Theorem
- Cantor's Theorem
- The Continuum Hypothesis

(26) Prove that $\sum_{i=1}^{n} i^2 = \frac{n(n+1)(2n+1)}{6}$

(27) Prove that $\sum_{i=1}^{n} i^3 = \left(\frac{n(n+1)}{2}\right)^2$

(28) Guess and prove a formula for the following sum $\sum_{i=1}^{n} (-1)^i i$

(29) Prove by induction that the number of subsets of a set containing n elements is 2^n.

(30) Consider this variation of the game of Nim. The game begins with $n \geq 1$ matches. Two players take turns removing either one or two matches at a time. The player removing the last match loses. Prove by (strong) induction that if each player plays the best strategy possible, the first player wins if $n = 3j$ or $n = 3j - 1$, and the second player wins in the remaining case when $n = 3j - 2$, where $j \geq 1$ is some integer.

(31) Prove that any $n \times m$ chessboard can be tiled with 2×1 dominoes if and only if at least one of n and m is even.

(32) Prove the generalized de Morgan's Law for sets: $\bigcup_{i=1}^{n} A_i^c = (\bigcap_{i=1}^{n} A_i)^c$
(33) Given n (infinitely long) lines dividing the plane into regions, Prove that we can color the regions with two colors such that no two regions sharing a border are colored the same.
(34) Prove that the sum of interior angles in of convex[20] polygon with n sides is $(n-2)\pi$.
(Hint: draw a diagonal)
(35) Find an integer N such that $2^n > n^4$ for every positive integer $n > N$. Prove your result by induction.
(36) Consider the following game (called Chomp) where two players take turns eating a chocolate bar divided into a grid of $n \times m$ squared. The top-leftmost square (in position $(1,1)$ where positions increase going to the right and going downwards) is poisonous so whoever eats it loses. And whenever a player eats any square, they have to also eat everything below it or to its right (e.g. if I eat the square at $(4,5)$, I also have to eat $(4,6),(4,7),\dots,(5,5),(5,6),\dots,(6,5),(6,6),\dots$).
- Show that the first player has a winning strategy in an $n \times n$ game of Chomp (Hint: start by eating the square $(2,2)$ and the show by strong induction that whoever starts playing the resulting pattern loses).
- Show that the first player has a winning strategy in an $2 \times n$ game of Chomp (Hint: start by eating the square $(2,n)$ and the show by strong induction that whoever starts playing the resulting pattern loses).

(37) Find a function $f : \mathbb{N} \to \mathbb{N}$ which is 1) injective but not surjective, 2) surjective but not injective.
(38) Show that there is a bijection between the set of all functions $\{1,2,\dots,n\} \to A$ on the one hand and the set $A^n = A \times A \times \dots, \times A$ on the other.
(39) Let $f : \mathbb{N} \to \mathbb{N}$ be a given function satisfying $f(n) < f(m)$ whenever $n < m$. Prove that f is injective. Does the result hold when replacing $<$ by $\leq$, $>$, or $\geq$?
(40) Let $h = f \circ g$. Prove or disprove: h is a bijection if and only if f and g are bijections.(See Problem 4.34 of [DW] for a bunch of variants!)
(41) Show that the set of finite binary sequences is countably infinite.
(42) Show that the set of infinite binary sequences is uncountable.
(43) Show that the number of possible sentences in the english language (or any language with a finite alphabet) is countably infinite. Deduce that there are some infinite binary sequence which is literally indescribable by any human language!
(44) An invisible flea is jumping on the $\mathbb{Z} \times \mathbb{Z}$ points on the plane. It always jumps the same distance and in the same direction once every second. We can grasp any point in a given second. Can we catch the flea?
(45) Give an explicit family $\{A_0, A_1, A_2, \dots\}$ of subsets $A_i \subseteq \mathbb{N}$ such that $A_i \cap A_j = \emptyset$ for every $i \neq j$ and $\bigcup_{i=0}^{\infty} A_i = \mathbb{N}$.
(46) [DW] Exercise 3.63
(47) [DW] Exercise 4.21
(48) [DW] Exercise 4.24 (replace $\mathbb{Z}$ with $\mathbb{N}$ if you prefer)
(49) [DW] Exercise 4.33
(50) [DW] Exercise 4.35
(51) [DW] Exercise 4.36

[20] a polygon is called convex if all its interior angles are less than $\pi = 180^\circ$

(52) [DW] Exercise 4.40
(53) [DW] Exercise 4.41
(54) [DW] Exercise 4.42
(55) [DW] Exercise 4.46
(56) State the definition or Theorem for each of the following
- divisibility in $\mathbb{Z}$
- congruence modulo n
- equivalence relation
- quotient set $S/\sim$
- Dedekind cut
- addition and multiplication of cuts
- Bézout's Theorem
- Generalized Bézout Lemma
- Fundamental Theorem of Arithmetic
- The Euclidean Algorithm
- Least Upper Bound Property for $\mathbb{R}$ (a.k.a. Completeness of $\mathbb{R}$).

(57) Let $a, b, c \in \mathbb{N}$. Prove that if $a \mid b$ and $a \mid c$, then $a \mid (mb + nc)$ for any integers m, n.
(58) Let S be the set of all finite strings of lowercase English letters. Define $s \sim t$ iff s and t have the same length. Prove $\sim$ is an equivalence relation and describe $S/\sim$.
(59) Define $\overline{a} \diamond \overline{b} = \overline{ab + 2a}$ on $\mathbb{Z}/n\mathbb{Z}$. Determine whether $\diamond$ is well-defined.
(60) Let $S = \mathbb{Z} \times \mathbb{Z}$ and define $(a, b) \sim (c, d)$ iff $a - b = c - d$.
  (a) Prove $\sim$ is an equivalence relation.
  (b) Describe $S/\sim$.
(61) Define an equivalence relation on $\mathbb{Q}$ by $x \sim y$ iff $x - y \in \mathbb{Z}$. Describe the quotient $\mathbb{Q}/\sim$ and show that $\overline{x} + \overline{y} := \overline{x + y}$ is a well-defined operation on the quotient.
(62) Prove that between any two distinct rational numbers there are infinitely many rationals.
(63) Prove there is no rational x satisfying $x^3 = 4$.
(64) Compute $\gcd(345, 123)$ using the Euclidean algorithm and express it as an integer combination of 345 and 123.
(65) Find the exponent of the prime p in the prime factorization of $n!$ (try examples like exponent of 5 in the factorization of $6! = 720$).
(66) Let $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ be defined by $f(a, b) = 3^{a-1}(3b - 1)$. Is f injective? Is it surjective?
(67) If $\gcd(a, b) = 1$, prove that $\gcd(a, bc) = \gcd(a, c)$.
(68) Given coprime $a, b \in \mathbb{Z}$, show that a^n and b^n are coprime for every $n \in \mathbb{N}$.
(69) Solve $17x \equiv 1 \pmod{60}$.
(70) Show that if $ab \equiv ac \pmod{n}$ and $\gcd(a, n) = 1$, then $b \equiv c \pmod{n}$. Show that the same result need not hold if a and n are not coprime.
(71) Prove that if a and b are coprime, then the congruence $ax \equiv b \pmod{n}$ has a solution iff $\gcd(a, n) \mid b$.
(72) Show that if p is prime and $p \mid a^2$, then $p \mid a$.
(73) Let $n = p_1^{e_1} \cdots p_k^{e_k}$. Prove that the number of positive divisors of n is $(e_1 + 1) \cdots (e_k + 1)$.
(74) Prove there are infinitely many primes $p \equiv 2 \pmod{3}$. (Hint: Adopt Euclid's proof of the infinitude of primes considering the number $N = 3p_1 p_2 \dots p_n + 2$)

(75) Find with proof the set of all weights we can measure using a scale and an unlimited supply 2-pound weights and 3-pound weights. Repeat the same problem but now with 1/2-pound weights and 1/3-pound weights instead.
(76) Find all positive integers n so that the number obtained by erasing the last (least significant) digit is a divisor of n.
(77) Prove that the fraction $\dfrac{21n+4}{14n+3}$ is irreducible for every $n \in \mathbb{N}$.
(78) Prove that $n^5 - 5n^3 + 4n$ is divisible by 120 *(Hint: Factorize!)*
(79) Show that the cut
$$\{x = r \in \mathbb{Q} : r < 0 \text{ or } r^2 < 3\} \mid \{r > 0, r^2 \geq 3\}$$
is the cut defining $\sqrt{3}$, i.e. prove $x^2 = 3$.
(80) Show that $\sqrt{2}$ is the supremum of $\{x \in \mathbb{R} : x < \sqrt{2}\}$.
(81) If $x > 0$, prove $x + y > y$ using cut definitions only.
(82) Show that between any two real numbers there exists a rational.
(83) Determine whether
$$x := \{r \in \mathbb{Q} : r^3 < 5\}$$
is a Dedekind cut and, if so, prove/disprove that it satisfies $x^3 = 5$.
(84) Let x and y be Dedekind cuts with $x < y$. Prove that there exists $z \in \mathbb{R}$ such that $x < z < y$ and z is irrational, using cuts only.
(85) Given bounded above subsets $A, B \subseteq \mathbb{R}$, define $A + B := \{x \in \mathbb{R} : \exists a \in A, \exists b \in B,\ \ x = a + b\}$. Show that $A + B$ is also bounded above, and $\sup(A + B) = \sup(A) + \sup(B)$.

Best Wishes :)

References

[DW] J. D'Angelo, D. West. *Mathematical Thinking, Problem Solving, and Proofs*. 2nd Edition. Prentice Hall, 2000.
[E] Euclid. *Elements of Geometry*. J. Heiberg (Ed.) R. Fitzpatrick (Ed., Trans.), 2008.
[G] L. Gerstein. *Introduction to Mathematical Structures and Proofs*. Springer–Verlag, 1996.
[H] D. Hofstadter. *Gödel, Escher, Bach: an Eternal Golden Braid*. 2nd Edition. Basic Books, 1999.
[P] C. Pugh. *Real Mathematical Analysis*. 2nd Edition. Springer–Verlag, 2015.

M.A., Department of Mathematics, University of Oregon, Fenton Hall, Eugene, OR 97403, USA
Email address: malqady@uoregon.edu