An Introduction to Proof via Inquiry-Based Learning

Dana C. Ernst, PhD
Northern Arizona University

Version Fall 2021

This book is intended to be a task sequence for an introduction to proof course that utilizes an inquiry-based learning (IBL) approach. You can find the most up-to-date version of these notes on GitHub:

http://dcernst.github.io/IBL-IntroToProof/

I would be thrilled if you used these notes and improved them. If you make any modifications, you can either make a pull request on GitHub or submit the improvements via email. You are also welcome to fork the source and modify the notes for your purposes as long as you maintain the license below.

Below is a partial list of people (alphabetical by last name) that I need to thank for supplying content, advice, and feedback.

- Joshua Bowman (Pepperdine University). The Preface is a modified version of Joshua's *An IBL preface*.

- Paul Ellis (Manhattanville College). Paul has provided lots of useful feedback and several suggestions for improvements. Paul suggested problems for Chapter 4 and provided an initial draft of Section 7.4: Images and Inverse Images.

- Jason Grout (Bloomberg, L.P.). I'm extremely grateful to Jason for feedback on early versions of this material, as well as helping me with a variety of technical aspects of writing these notes.

- Anders Hendrickson (St. Norbert College). Anders is the original author of the content in Appendix A: Elements of Style for Proofs. The current version in Appendix A is a result of modifications made by myself with some suggestions from David Richeson.

- Rebecca Jayne (Hampden–Sydney College). The current version of Section 4.3: Complete Induction is a derivative of content contributed by Rebecca.

- Matthew Jones (CSU Dominguez Hills) and Stan Yoshinobu (Cal Poly). A few of the sections were originally adaptations of notes written by Matt and Stan. Early versions of these notes relied heavily on their work. Moreover, Matt and Stan were two of the key players that contributed to shaping my approach to teaching.

- T. Kyle Petersen (DePaul University) and Bridget Tenner (DePaul University). Modifications that Kyle and Bridget made to the book inspired me to streamline some of the exposition, especially in the early chapters.

- David Richeson (Dickinson College). David is responsible for much of the content in Appendix B: Fancy Mathematical Terms and Appendix D: Definitions in Mathematics. In addition, the current version of Chapter 5: Three Famous Theorems is heavily based on content contributed by David.

- Carol Schumacher (Kenyon College). When I was transitioning to an IBL approach to teaching, Carol was one of my mentors and played a significant role in my development as a teacher. Moreover, this work is undoubtably influenced my Carol's excellent book *Chapter Zero: Fundamental Notions of Advanced Mathematics*, which I used when teaching my very first IBL course.

- Josh Wiscons (CSU Sacramento). Josh contributed the content in Section 6.4: Modular Arithmetic.

Contents

Preface

You are the creators. This book is a guide.

This book will not show you how to solve all the problems that are presented, but it should *enable* you to find solutions, on your own and working together. The material you are about to study did not come together fully formed at a single moment in history. It was composed gradually over the course of centuries, with various mathematicians building on the work of others, improving the subject while increasing its breadth and depth.

Mathematics is essentially a human endeavor. Whatever you may believe about the true nature of mathematics—does it exist eternally in a transcendent Platonic realm, or is it contingent upon our shared human consciousness?—our *experience* of mathematics is temporal, personal, and communal. Like music, mathematics that is encountered only as symbols on a page remains inert. Like music, mathematics must be created in the moment, and it takes time and practice to master each piece. The creation of mathematics takes place in writing, in conversations, in explanations, and most profoundly in the mental construction of its edifices on the basis of reason and observation.

To continue the musical analogy, you might think of these notes like a performer's score. Much is included to direct you towards particular ideas, but much is missing that can only be supplied by you: participation in the creative process that will make those ideas come alive. Moreover, your success will depend on the pursuit of both *individual* excellence and *collective* achievement. Like a musician in an orchestra, you should bring your best work and be prepared to blend it with others' contributions.

In any act of creation, there must be room for experimentation, and thus allowance for mistakes, even failure. A key goal of our community is that we support each other—sharpening each other's thinking but also bolstering each other's confidence—so that we can make failure a *productive* experience. Mistakes are inevitable, and they should not be an obstacle to further progress. It's normal to struggle and be confused as you work through new material. Accepting that means you can keep working even while feeling stuck, until you overcome and reach even greater accomplishments.

This book is a guide. You are the creators.

Chapter 1

Introduction

1.1 What is This Course All About?

The foundations of mathematics refers to logic and set theory; the axioms of number and space. Also, it refers to an introduction to the techniques of proof, and at a larger level the process of *doing Mathematics*. Proof is central to doing mathematics.

Up to this point, it is likely that your experience of mathematics has been about using formulas and algorithms. That is only one part of mathematics. Mathematicians do much more than just use formulas. Mathematicians experiment, make conjectures, write definitions, and prove theorems. In this class, then, we will learn about doing all of these things.

What will this class require? Daily practice. Just like learning to play an instrument or sport, you will have to learn new skills and ideas. Sometimes you'll feel good, sometimes frustrated. You'll probably go through a range of feelings from being exhilarated, to being stuck. Figuring it out, victories, defeats, and all that is part of real life is what you can expect. Most importantly it will be rewarding. Learning mathematics requires dedication. It will require that you be patient despite periods of confusion. It will require that you persevere in order to understand. As the instructor, I am here to guide you, but I cannot do the learning for you, just as a music teacher cannot move your fingers and your heart for you. Only you can do that. I can give suggestions, structure the course to assist you, and try to help you figure out how to think through things. Do your best, be prepared to put in a lot of time, and do all the work. Ask questions in class, ask questions in office hours, and ask your classmates questions. When you work hard and you come to understand, you feel good about yourself. In the meantime, you have to believe that your work will pay off in intellectual development.

How will this class be organized? You have probably heard that mathematics is not a spectator sport. Our focus in this class is on learning to DO mathematics, not learning to sit patiently while others do it. Therefore, class time will be devoted to working on problems, and especially on students presenting conjectures and proofs to the class, asking questions of presenters in order to understand their work and their thinking, and sharing and clarifying our thinking and understanding of each other's ideas.

The class is fueled by your ability to prove theorems and share your ideas. As we progress, you will find that you have ideas for proofs, but you are unsure of them. In that case, you can either bring your idea to the class, or you can bring it to office hours. By coming to office hours, you have a chance to refine your ideas and get individual feedback before bringing them to the class. The more you use office hours, the more you will learn. If the whole class is stuck, we can work on some ego-booster problems to get your ideas flowing.

Finally, this is a very exciting time in your mathematical career. It's where you learn what mathematics is really about!

> The mathematician does not study pure mathematics because it is useful; he studies it because he delights in it, and he delights in it because it is beautiful.
>
> *Henri Poincaré*

1.2 An Inquiry-Based Approach

This is not a lecture-oriented class or one in which mimicking prefabricated examples will lead you to success. You will be expected to work actively to construct your own understanding of the topics at hand with the readily available help of me and your classmates. Many of the concepts you learn and problems you work on will be new to you and ask you to stretch your thinking. You will experience *frustration* and *failure* before you experience *understanding*. This is part of the normal learning process. If you are doing things well, you should be confused at different points in the semester. The material is too rich for a human being to completely understand it immediately. Your viability as a professional in the modern workforce depends on your ability to embrace this learning process and make it work for you.

> Don't fear failure. Not failure, but low aim, is the crime. In great attempts it is glorious even to fail.
>
> *Bruce Lee*

In order to promote a more active participation in your learning, we will incorporate ideas from an educational philosophy called inquiry-based learning (IBL). Loosely speaking, IBL is a student-centered method of teaching mathematics that engages students in sense-making activities. Students are given tasks requiring them to solve problems, conjecture, experiment, explore, create, and communicate. Rather than showing facts or a clear, smooth path to a solution, the instructor guides and mentors students via well-crafted problems through an adventure in mathematical discovery. According to Laursen and Rasmussen (2019), the Four Pillars of IBL are:

- Students engage deeply with coherent and meaningful mathematical tasks.
- Students collaboratively process mathematical ideas.
- Instructors inquire into student thinking.
- Instructors foster equity in their design and facilitation choices.

Much of the course will be devoted to students presenting their proposed solutions or proofs on the board and a significant portion of your grade will be determined by how much mathematics you produce. I use the word *produce* because I believe that the best way to learn mathematics is by doing mathematics. Someone cannot master a musical instrument or a martial art by simply watching, and in a similar fashion, you cannot master mathematics by simply watching; you must do mathematics!

In any act of creation, there must be room for experimentation, and thus allowance for mistakes, even failure. A key goal of our community is that we support each other—sharpening each other's thinking but also bolstering each other's confidence—so that we can make failure a productive experience. Mistakes are inevitable, and they should not be an obstacle to further progress. It's normal to struggle and be confused as you work through new material. Accepting that means you can keep working even while feeling stuck, until you overcome and reach even greater accomplishments.

> You will become clever through your mistakes.
>
> *German Proverb*

Furthermore, it is important to understand that solving genuine problems is difficult and takes time. You shouldn't expect to complete each problem in 10 minutes or less. Sometimes, you might have to stare at the problem for an hour before even understanding how to get started.

In this course, everyone will be required to

- read and interact with course notes and textbook on your own;
- write up quality solutions/proofs to assigned problems;
- present solutions/proofs on the board to the rest of the class;
- participate in discussions centered around a student's presented solution/proof;
- call upon your own prodigious mental faculties to respond in flexible, thoughtful, and creative ways to problems that may seem unfamiliar on first glance.

As the semester progresses, it should become clear to you what the expectations are.

> Tell me and I forget, teach me and I may remember, involve me and I learn.
>
> *Benjamin Franklin*

1.3 Rights of the Learner

As a student in this class, you have the right:

1. to be confused,
2. to make a mistake and to revise your thinking,
3. to speak, listen, and be heard, and
4. to enjoy doing mathematics.

> You may encounter many defeats, but you must not be defeated.
>
> *Maya Angelou*

1.4 Your Toolbox, Questions, and Observations

Throughout the semester, we will develop a list of *tools* that will help you understand and do mathematics. Your job is to keep a list of these tools, and it is suggested that you keep a running list someplace.

Next, it is of utmost importance that you work to understand every proof. (Every!) Questions are often your best tool for determining whether you understand a proof. Therefore, here are some sample questions that apply to any proof that you should be prepared to ask of yourself or the presenter:

- What method(s) of proof are you using?
- What form will the conclusion take?
- How did you know to set up that [equation, set, whatever]?
- How did you figure out what the problem was asking?
- Was this the first thing you tried?
- Can you explain how you went from this line to the next one?
- What were you thinking when you introduced this?
- Could we have ... instead?
- Would it be possible to ...?
- What if ...?

Another way to help you process and understand proofs is to try and make observations and connections between different ideas, proof statements and methods, and to compare approaches used by different people. Observations might sound like some of the following:

- When I tried this proof, I thought I needed to ... But I didn't need that, because ...
- I think that ... is important to this proof, because ...
- When I read the statement of this theorem, it seemed similar to this earlier theorem. Now I see that it [is/isn't] because ...

1.5 Rules of the Game

You should *not* look to resources outside the context of this course for help. That is, you should not be consulting the Internet, other texts, other faculty, or students outside of our course. On the other hand, you may use each other, the course notes, me, and your own intuition. In this class, earnest failure outweighs counterfeit success; you need not feel pressure to hunt for solutions outside your own creative and intellectual reserves. For more details, check out the Syllabus.

1.6 Structure of the Notes

As you read the notes, you will be required to digest the material in a meaningful way. It is your responsibility to read and understand new definitions and their related concepts. However, you will be supported in this sometimes difficult endeavor. In addition, you will be asked to complete problems aimed at solidifying your understanding of the material. Most importantly, you will be asked to make conjectures, produce counterexamples, and prove theorems.

The items labeled as **Definition** and **Example** are meant to be read and digested. However, the items labeled as **Problem**, **Theorem**, and **Corollary** require action on your part. Items labeled as **Problem** are sort of a mixed bag. Some Problems are computational in nature and aimed at improving your understanding of a particular concept while others ask you to provide a counterexample for a statement if it is false or to provide a proof if the statement is true. Items with the **Theorem** and **Corollary** designation are mathematical facts and the intention is for you to produce a valid proof of the given statement. The main difference between a **Theorem** and a **Corollary** is that corollaries are typically statements that follow quickly from a previous theorem. In general, you should expect corollaries to have very short proofs. However, that doesn't mean that you can't produce a more lengthy yet valid proof of a corollary.

It is important to point out that there are very few examples in this book. This is intentional. One of the goals of the items labeled as **Problem** is for you to produce the examples. Lastly, there are many situations where you will want to refer to an earlier definition or theorem/corollary/problem. In this case, you should reference the statement by number. For example, you might write something like, "By Theorem 2.14, we see that...."

1.7 Some Minimal Guidance

Especially in the opening sections, it won't be clear what facts from your prior experience in mathematics we are "allowed" to use. Unfortunately, addressing this issue is difficult and is something we will sort out along the way. However, in general, here are some minimal and vague guidelines to keep in mind.

First, there are times when we will need to do some basic algebraic manipulations. You should feel free to do this whenever the need arises. But you should show sufficient work along the way. You do not need to write down justifications for basic algebraic manipulations (e.g., adding 1 to both sides of an equation, adding and subtracting the same amount on the same side of an equation, adding like terms, factoring, basic simplification, etc.).

On the other hand, you do need to make explicit justification of the logical steps in a proof. When necessary, you should cite a previous definition, theorem, etc. by number.

Unlike the experience many of you had writing proofs in geometry, our proofs will be written in complete sentences. You should break sections of a proof into paragraphs and use proper grammar. There are some pedantic conventions for doing this that I will point out along the way. Initially, this will be an issue that most students will struggle with, but after a few weeks everyone will get the hang of it.

Ideally, you should rewrite the statements of theorems before you start the proof. Moreover, for your sake and mine, you should label the statement with the appropriate number. I will expect you to indicate where the proof begins by writing "*Proof.*" at the beginning. Also, we will conclude our proofs with the standard "proof box" (i.e., $\square$ or $\blacksquare$), which is typically right-justified.

Lastly, every time you write a proof, you need to make sure that you are making your assumptions crystal clear. Sometimes there will be some implicit assumptions that we can omit, but at least in the beginning, you should get in the habit of stating your assumptions up front. Typically, these statements will start off "Assume..." or "Let...".

This should get you started. We will discuss more as the semester progresses. Now, go have fun and start exploring mathematics!

> If you want to sharpen a sword, you have to remove a little metal.
>
> *Unknown*

Chapter 2

Mathematics and Logic

Before you get started, make sure you have read Chapter 1, which sets the tone for the work we will begin doing here.

2.1 A Taste of Number Theory

It is important to point out that we are diving in head first here. As we get started, we are going to rely on your intuition and previous experience with proofs. This is intentional. What you will likely encounter is a general sense of what a proof entails, but you may not be able to articulate the finer details that you do and do not comprehend. There are going to be some subtle issues that you will be confronted with and one of our goals will be to elucidate as many of them as possible. We need to calibrate and develop an intellectual need for structure. You are encouraged to just try your hand at writing proofs for the problems in this section without too much concern for whether you are "doing it the right way." In Section 2.2, we will start over and begin to develop a formal foundation for the material in the remainder of the book. Once you have gained more experience and a better understanding of what a proof entails, you should consider returning to this section and reviewing your first attempts at writing proofs. In the meantime, see what you can do!

Here are a few small tips to get you started with the proofs that you will write in this section.

- You should indicate where your proof begins by writing "*Proof.*".
- Make it clear to yourself and the reader what your assumptions are at the very beginning of your proof. Typically, these statements will start off "Assume…" or "Let…". Sometimes there will be some implicit assumptions that we can omit, but at least in the beginning, you should get in the habit of stating your assumptions up front.
- Carefully consider the order in which you write your proof. Loosely speaking, each sentence should follow from an earlier sentence in your proof or possibly a result you have already proved.

- If something follows from a definition or previous result, you should say so. For example, you could write, "By the definition of divides (Definition 2.5), it follows that..." or "By the theorem that states that if n is an even integer, n^2 is also an even integer, we see that...". While it is preferable to give the reader an indication of the content of the result you are citing, it is common to simply cite things by number. For example, you might write, "By Definition 2.1, it follows that..." or "According to Theorem 2.2, we see that...". One thing worth pointing out is that if we are citing a definition, theorem, or problem by number, we should capitalize Definition, Theorem, or Problem, respectively (e.g., "According to Theorem 2.2"). Otherwise, we do not capitalize these words (e.g., "By the definition of divides").

- Similar to making it clear where your proof begins, you should indicate where it ends. It is common to conclude a proof with the standard "proof box" (□ or ■). This little square at end of a proof is sometimes called a **tombstone** or **Halmos symbol** after Hungarian-born American mathematician Paul Halmos (1916–2006).

In this section, we will introduce the basics of a branch of mathematics called **number theory**, which is devoted to studying the properties of the integers. The integers is the set of numbers given by

$$\boxed{\mathbb{Z} := \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}}.$$

The collection of positive integers also have a special name. The set of **natural numbers** is given by

$$\boxed{\mathbb{N} := \{1, 2, 3, \ldots\}}.$$

Some mathematicians (set theorists, in particular) include 0 in $\mathbb{N}$, but this will not be our convention. If you look closely at the two sets we defined above, you will notice that we wrote $\boxed{:=}$ instead of $=$. We use $:=$ to mean that the symbol or expression on the left is defined to be equal to the expression on the right.

Because you are so familiar with many of the properties of the integers, one of the issues that we will bump into is knowing which facts we can take for granted. As a general rule of thumb, you should attempt to use the definitions provided without relying too much on your prior knowledge. The order in which we develop things is important.

It is common practice in mathematics to use the symbol "$\in$" as an abbreviation for the phrase "is an element of" or sometimes simply "in." For example, the mathematical expression "$n \in \mathbb{Z}$" means "n is an element of the integers." However, some care should be taken in how this symbol is used. We will only use the symbol "$\in$" in expressions of the form $\boxed{a \in A}$, where A is a set and a is an element of A. We will write expressions like $\boxed{a, b \in A}$ as shorthand for "$a \in A$ and $b \in A$." We should avoid writing phrases such as "a is a number $\in A$" and "$n \in$ integers".

We will now encounter our very first definition. In mathematics, a **definition** is a precise and unambiguous description of the meaning of a mathematical term. It characterizes the meaning of a word by giving all the properties and only those properties that must be true. Check out Appendix B for a list of other mathematical terms that we should be familiar with.

Definition 2.1. An integer n is **even** if $n = 2k$ for some $k \in \mathbb{Z}$. An integer n is **odd** if $n = 2k + 1$ for some $k \in \mathbb{Z}$.

Notice that we framed the definition of "even" in terms of multiplication as opposed to division. When tackling theorems and problems involving even or odd, be sure to make use of our formal definitions and not some of the well-known divisibility properties. For now, you should avoid arguments that involve statements like, "even numbers have no remainder when divided by two" or "the last digit of an even number is 0, 2, 4, 6, or 8." Also notice that the notions of even and odd apply to zero and negative numbers. In particular, zero is even since $0 = 2 \cdot 0$, where it is worth emphasizing that the occurrence of 0 on the righthand side of equation is an integer. As another example, we see that -1 is odd since $-1 = 2(-1) + 1$. Despite the fact that $-1 = 2(-1/2)$, this does not imply that -1 is also even since $-1/2$ is not an integer. For the remainder of this section, you may assume that every integer is either even or odd but never both.

Our first theorem concerning the integers is stated below. A **theorem** is a mathematical statement that is proved using rigorous mathematical reasoning.

Theorem 2.2. If n is an even integer, then n^2 is an even integer.

One crux in proving the next theorem involves figuring out how to describe an arbitrary pair of consecutive integers.

Theorem 2.3. The sum of two consecutive integers is odd.

One skill we will want to develop is determining whether a given mathematical statement is true or false. In order to verify that a mathematical statement is false, we should provide a specific example where the statement fails. Such an example is called a **counterexample**. Notice that it is sufficient to provide a single example to verify that a general statement is not true. On the other hand, if we want to prove that a general mathematical statement is true, it is usually not sufficient to provide just a single example, or even a hundred examples. Such examples are just evidence that the statement is true.

Problem 2.4. Determine whether each of the following statements is true or false. If a statement is true, prove it. If a statement is false, provide a counterexample.

(a) The product of an odd integer and an even integer is odd.

(b) The product of an odd integer and an odd integer is odd.

(c) The product of an even integer and an even integer is even.

(d) The sum of an even integer and an odd integer is odd.

For the statements that were true in the previous problem, you may cite them later in a future proof as if they are theorems.

Definition 2.5. Given $n, m \in \mathbb{Z}$, we say that n **divides** m, written $\boxed{n|m}$, if there exists $k \in \mathbb{Z}$ such that $m = nk$. If $n|m$, we may also say that m **is divisible by** n.

Problem 2.6. For $n, m \in \mathbb{Z}$, how are the following mathematical expressions similar and how are they different? In particular, is each one a sentence or simply a noun?

(a) $n|m$

(b) $\dfrac{m}{n}$

(c) m/n

In this section on number theory, we allow addition, subtraction, and multiplication of integers. In general, we avoid division since an integer divided by an integer may result in a number that is not an integer. The upshot is that we will avoid writing $\frac{m}{n}$. When you feel the urge to divide, switch to an equivalent formulation using multiplication. This will make your life much easier when proving statements involving divisibility.

Theorem 2.7. The sum of any three consecutive integers is always divisible by three.

Problem 2.8. Let $a, b, n, m \in \mathbb{Z}$. Determine whether each of the following statements is true or false. If a statement is true, prove it. If a statement is false, provide a counterexample.

(a) If $a|n$, then $a|mn$.

(b) If 6 divides n, then 2 divides n and 3 divides n.

(c) If ab divides n, then a divides n and b divides n.

A theorem that follows almost immediately from another theorem is called a **corollary**. See if you can prove the next result quickly using a previous result. Be sure to cite the result in your proof.

Corollary 2.9. If $a, n \in \mathbb{Z}$ such that a divides n, then a divides n^2.

The next two theorems are likely familiar to you.

Theorem 2.10. If $a, n \in \mathbb{Z}$ such that a divides n, then a divides $-n$.

Theorem 2.11. If $a, n, m \in \mathbb{Z}$ such that a divides m and a divides n, then a divides $m + n$.

Notice that we have been tinkering with statements of the form "If…, then…". Statements of this form are called **conditional propositions**, which we revisit in the next section. The phrase that occurs after "If" but before "then" is called the **hypothesis** while the phrase that occurs after "then" is called the **conclusion**. For example, in Problem 2.8(a), "$a|n$" is the hypothesis while "$a|mn$" is the conclusion. Note that conditional propositions can also be written in the form "… if …", where the conclusion is written before "if" and the hypothesis after. For example, we can rewrite Problem 2.8(a) as "$a|mn$ if $a|n$". While the order of the hypothesis and conclusion have been reversed in the sentence, their roles have not.

Whenever we encounter a conditional statement in mathematics, we want to get in the habit of asking ourselves what happens when we swap the roles of the hypothesis and the conclusion. The statement that results from reversing the roles of the hypothesis and conclusion in a conditional statement is called the **converse** of the original statement. For example, the converse of Problem 2.8(a) is "If $a|mn$, then $a|n$", which happens to be false. The converse of Theorem 2.2 is "If n^2 is an even integer, then n is an even integer". While this statement is true it does *not* have the same meaning as Theorem 2.2.

Problem 2.12. Determine whether the converse of each of Corollary 2.9, Theorem 2.10, and Theorem 2.11 is true. That is, for $a, n, m \in \mathbb{Z}$, determine whether each of the following statements is true or false. If a statement is true, prove it. If a statement is false, provide a counterexample.

(a) If a divides n^2, then a divides n. (Converse of Corollary 2.9)

(b) If a divides $-n$, then a divides n. (Converse of Theorem 2.10)

(c) If a divides $m+n$, then a divides m and a divides n. (Converse of Theorem 2.11)

Once we have proved a few theorems, we should be on the look out to see if we can utilize any of our current results to prove new results. There is no point in reinventing the wheel if we do not have to. Try to use a couple of our previous results to prove the next theorem.

Theorem 2.13. If $a, n, m \in \mathbb{Z}$ such that a divides m and a divides n, then a divides $m-n$.

The next theorem is often referred to as the **transitivity of division of integers**.

Theorem 2.14. If $a, b, c \in \mathbb{Z}$ such that a divides b and b divides c, then a divides c.

2.2 Introduction to Logic

After getting our feet wet in the previous section, let's take a step back and do a more careful examination of what it is we are actually doing.

Definition 2.15. A **proposition** (or **statement**) is a sentence that is either true or false but not both. The **truth value** (or **logical value**) of a proposition refers to its attribute of being true or false.

For example, the sentence "All dogs have four legs" is a false proposition. However, the perfectly good sentence "$x = 1$" is *not* a proposition all by itself since we don't actually know what x is.

Problem 2.16. Determine whether each of the following is a proposition. Explain your reasoning.

(a) All cars are red.

(b) Every person whose name begins with J has the name Joe.

(c) $x^2 = 4$.

(d) There exists a real number x such that $x^2 = 4$.

(e) For all real numbers x, $x^2 = 4$.

(f) $\sqrt{2}$ is an irrational number.

(g) p is prime.

(h) Led Zeppelin is the best band of all time.

Given two propositions, we can form more complicated propositions using logical connectives.

Definition 2.17. Let A and B be propositions.

(a) The proposition "**not** A" is true if A is false; expressed symbolically as $\boxed{\neg A}$ and called the **negation** of A.

(b) The proposition "A **and** B" is true if both A and B are true; expressed symbolically as $\boxed{A \wedge B}$ and called the **conjunction** of A and B.

(c) The proposition "A **or** B" is true if at least one of A or B is true; expressed symbolically as $\boxed{A \vee B}$ and called the **disjunction** of A and B.

(d) The proposition "**If** A**, then** B" is true if both A and B are true, or A is false; expressed symbolically as $\boxed{A \implies B}$ and called a **conditional proposition** (or **implication**). In this case, A is called the **hypothesis** and B is called the **conclusion**. Note that $A \implies B$ may also be read as "A implies B", "A only if B", or "B if A".

(e) The proposition "A **if and only if** B" is true if both A and B have the same truth value; expressed symbolically as $\boxed{A \iff B}$. If $A \iff B$ is true, we say that A and B are **logically equivalent**.

Each of the propositions in the previous definition is called a **compound proposition**, where A and B are referred to as the **components** of the compound proposition. We can form complicated compound propositions with several components by combining logical connectives.

Problem 2.18. Let A represent "6 is an even integer" and B represent "4 divides 6." Express each of the following compound propositions in an ordinary English sentence and then determine its truth value.

(a) $A \wedge B$

(b) $A \vee B$

(c) $\neg A$

(d) $\neg B$

(e) $\neg(A \land B)$

(f) $\neg(A \lor B)$

(g) $A \implies B$

Definition 2.19. A **truth table** for a compound proposition is a table that illustrates all possible combinations of truth values for the components of the compound proposition together with the resulting truth value for each combination.

Example 2.20. If A and B are propositions, then the truth table for the conjunction $A \land B$ is given by the following.

A	B	$A \land B$
T	T	T
T	F	F
F	T	F
F	F	F

Notice that we have columns for each of A and B. The rows for these two columns correspond to all possible combinations of truth values for A and B. The third column yields the truth value of $A \land B$ given the possible truth values for A and B.

Each component of a compound proposition has two possible truth values, namely true or false. Thus, if a compound proposition is built from n component propositions, then the truth table will require 2^n rows.

Problem 2.21. Create a truth table for each of the following compound propositions. You should add additional columns to your tables as needed to assist you with intermediate steps. For example, you might need four columns for the third and fourth compound proposition below.

(a) $\neg A$

(b) $A \lor B$

(c) $\neg(A \land B)$

(d) $\neg A \land \neg B$

Problem 2.22. A coach promises her players, "If we win tonight, then I will buy you pizza tomorrow." Determine the cases in which the players can rightly claim to have been lied to. If the team lost the game and the coach decided to buy them pizza anyway, was she lying?

Problem 2.23. Use Definition 2.17(d) to construct a truth table for $A \implies B$. Compare your truth table with Problem 2.22. The combination you should pay particular attention to is when the hypothesis is false while the conclusion is true.

In accordance with Definition 2.17(d), a conditional proposition $A \implies B$ is only false when the hypothesis is true and the conclusion is false. Perhaps you are bothered by the fact that $A \implies B$ is true when A is false no matter what the truth value of B is. The thing to keep in mind is that the truth value of $A \implies B$ relies on a very specific definition and may not always agree with the colloquial use of "If…, then…" statements that we encounter in everyday language. For example, if someone says, "If you break the rules, then you will be punished", the speaker likely intends the statement to be interpreted as "You will be punished if and only if you break the rules." In logic and mathematics, we aim to remove such ambiguity by explicitly saying exactly what we mean.

We can often prove facts concerning logical statements using truth tables. Recall that two propositions P and Q (both of which might be complicated compound propositions) are logically equivalent if $P \iff Q$ is true (see Definition 2.17(e)). This happens when P and Q have the same truth value. We can verify whether P and Q have the same truth value by constructing a truth table that includes columns for each of the components of P and Q, listing all possible combinations of their truth values, together with columns for P and Q that lists their resulting truth values. If the truth values in the columns for P and Q agree, then P and Q are logically equivalent, and otherwise they are not logically equivalent. When constructing truth tables to verify whether P and Q are logically equivalent, you should add any necessary intermediate columns to aid in your "calculations". Use truth tables when attempting to justify the next few problems.

Theorem 2.24. If A is a proposition, then $\neg(\neg A)$ is logically equivalent to A.

The next theorem, referred to as DeMorgan's Law, provides a method for negating a conjunction.

Theorem 2.25 (DeMorgan's Law)**.** If A and B are propositions, then $\neg(A \wedge B)$ is logically equivalent to $\neg A \vee \neg B$.

Problem 2.26. Let A and B be propositions. Conjecture a statement similar to Theorem 2.25 for the proposition $\neg(A \vee B)$ and then prove it. This is also called DeMorgan's Law.

We will make use of both versions DeMorgan's Law on on a regular basis. Sometimes conjunctions and disjunctions are "buried" in a mathematical statement, which makes negating statements tricky business. Keep this in mind when approaching the next problem.

Problem 2.27. Let x be your favorite real number. Negate each of the following statements. Note that the statement in part (b) is cleverly disguised as a conjunction.

(a) $x < -1$ or $x \geq 3$.

(b) $0 \leq x < 1$.

We already introduced the following notion in the discussion following Theorem 2.11

Definition 2.28. If A and B are propositions, then the **converse** of $A \implies B$ is $B \implies A$.

Problem 2.29. Provide an example of a true conditional proposition whose converse is false.

Definition 2.30. If A and B are propositions, then the **inverse** of $A \implies B$ is $\neg A \implies \neg B$.

Problem 2.31. Provide an example of a true conditional proposition whose inverse is false.

Based on Problems 2.29 and 2.32, we can conclude that the converse and inverse of a conditional proposition do not necessarily have the same truth value as the original statement. Moreover, the converse and inverse of a conditional proposition do not necessarily have the same truth value as each other.

Problem 2.32. Provide an example of a conditional proposition whose converse is true but whose inverse is false.

What if we swap the roles of the hypothesis and conclusion of a conditional proposition *and* negate each?

Definition 2.33. If A and B are propositions, then the **contrapositive** of $A \implies B$ is $\neg B \implies \neg A$.

Problem 2.34. Let A and B represent the statements from Problem 2.18. Express each of the following in an ordinary English sentence.

(a) The converse of $A \implies B$.

(b) The contrapositive of $A \implies B$.

Problem 2.35. Find the converse and the contrapositive of the following statement: "If Dana lives in Flagstaff, then Dana lives in Arizona."

Use a truth table to prove the following theorem.

Theorem 2.36. If A and B are propositions, then $A \implies B$ is logically equivalent to its contrapositive.

Each of the theorems that we proved in Section 2.1 are examples of conditional propositions. However, some of the statements were disguised as such. For example, Theorem 2.3 states, "The sum of two consecutive integers is odd." We can reword this theorem as, "If $n \in \mathbb{Z}$, then $n+(n+1)$ is odd."

Problem 2.37. Reword Theorem 2.7 so that it explicitly reads as a conditional proposition.

The proofs of each of the theorems in Section 2.1 had the same format, which we refer to as a **direct proof**.

Skeleton Proof 2.38 (Proof of $A \implies B$ by direct proof)**.** If you want to prove the implication $A \implies B$ via a direct proof, then the structure of the proof is as follows.

Proof. *[State any upfront assumptions.]* Assume A.

… *[Use definitions and known results to derive B]* …

Therefore, B. □

Take a few minutes to review the proofs that you wrote in Section 2.1 and see if you can witness the structure of Skeleton Proof 2.38 in your proofs. The upshot of Theorem 2.36 is that if you want to prove a conditional proposition, you can prove its contrapositive instead. This approach is called a **proof by contraposition**.

Skeleton Proof 2.39 (Proof of $A \implies B$ by contraposition)**.** If you want to prove the implication $A \implies B$ by proving its contrapositive $\neg B \implies \neg A$ instead, then the structure of the proof is as follows.

Proof. *[State any upfront assumptions.]* We will prove this by contraposition. Assume $\neg B$.

… *[Use definitions and known results to derive ¬A]* …

Therefore, $\neg A$. We have proved the contrapositive, and hence if A, then B. □

We have introduced the logical symbols $\wedge$, $\vee$, $\implies$, $\iff$, and $\neg$ since is provides a convenient way of discussing the formality of logic. However, when writing mathematical proofs, you should avoid using these symbols.

Problem 2.40. Consider the following statement:

Assume $x \in \mathbb{Z}$. If x^2 is odd, then x is odd.

The items below can be assembled to form a proof of this statement, but they are currently out of order. Put them in the proper order.

1. Assume that x is an even integer.
2. We will prove this by contraposition.
3. Thus, x^2 is twice an integer.
4. Since $x = 2k$, we have that $x^2 = (2k)^2 = 4k^2$.
5. Since k is an integer, $2k^2$ is also an integer.
6. By the definition of even, there is an integer k such that $x = 2k$.
7. We have proved the contrapositive, and hence the desired statement is true.
8. Assume $x \in \mathbb{Z}$.
9. By the definition of even integer, x^2 is an even integer.

10. Notice that $x^2 = 2(2k^2)$.

Prove each of the next three theorems by proving the contrapositive of the given statement.

Theorem 2.41. Assume $x \in \mathbb{Z}$. If x^2 is even, then x is even.

Theorem 2.42. Assume $x, y \in \mathbb{Z}$. If xy is odd, then both x and y are odd.

Theorem 2.43. Assume $x, y \in \mathbb{Z}$. If xy is even, then x or y is even.

2.3 Negating Implications and Proof by Contradiction

So far we have discussed how to negate propositions of the form A, $A \wedge B$, and $A \vee B$ for propositions A and B. However, we have yet to discuss how to negate propositions of the form $A \implies B$. Prove the following result with a truth table.

Theorem 2.44. If A and B are propositions, then the implication $A \implies B$ is logically equivalent to the disjunction $\neg A \vee B$.

The next result follows quickly from Theorem 2.44 together with DeMorgan's Law. You can also verify this result using a truth table.

Corollary 2.45. If A and B are propositions, then $\neg(A \implies B)$ is logically equivalent to $A \wedge \neg B$.

Problem 2.46. Let A and B be the propositions "$\sqrt{2}$ is an irrational number" and "Every rectangle is a trapezoid," respectively.

(a) Express $A \implies B$ as an English sentence involving the disjunction "or."

(b) Express $\neg(A \implies B)$ as an English sentence involving the conjunction "and."

Problem 2.47. It turns out that the proposition "If $.\overline{99} = \frac{9}{10} + \frac{9}{100} + \frac{9}{1000} + \cdots$, then $.\overline{99} \neq 1$" is false. Write its negation as a conjunction.

Recall that a proposition is exclusively either true or false—it can never be both.

Definition 2.48. A compound proposition that is always false is called a **contradiction**. A compound proposition that is always true is called a **tautology**.

Theorem 2.49. If A is a proposition, then the proposition $\neg A \wedge A$ is a contradiction.

Problem 2.50. Provide an example of a tautology using arbitrary propositions and any of the logical connectives $\neg$, $\wedge$, and $\vee$. Prove that your example is in fact a tautology.

Suppose that we want to prove some proposition P (which might be something like $A \implies B$ or even more complicated). One approach, called **proof by contradiction**, is to assume $\neg P$ and then logically deduce a contradiction of the form $Q \wedge \neg Q$, where Q is some proposition (possibly equal to P). Since this is absurd, the assumption $\neg P$ must have been false, so P is true. The tricky part about a proof by contradiction is that it is not usually obvious what the statement Q should be.

Skeleton Proof 2.51 (Proof of P by contradiction)**.** Here is what the general structure for a proof by contradiction looks like if we are trying to prove the proposition P.

> *Proof.* *[State any upfront assumptions.]* For sake of a contradiction, assume $\neg P$.
>
> … *[Use definitions and known results to derive some Q and its negation $\neg Q$.]* …
>
> This is a contradiction. Therefore, P. □

Proof by contradiction can be useful for proving statements of the form $A \implies B$, where $\neg B$ is easier to "get your hands on," because $\neg(A \implies B)$ is logically equivalent to $A \wedge \neg B$ (see Corollary 2.45).

Skeleton Proof 2.52 (Proof of $A \implies B$ by contradiction)**.** If you want to prove the implication $A \implies B$ via a proof by contradiction, then the structure of the proof is as follows.

> *Proof.* *[State any upfront assumptions.]* For sake of a contradiction, assume A and $\neg B$.
>
> … *[Use definitions and known results to derive some Q and its negation $\neg Q$.]* …
>
> This is a contradiction. Therefore, if A, then B. □

Problem 2.53. Assume that $x \in \mathbb{Z}$. Consider the following proposition: If x is odd, then 2 does not divide x.

(a) Prove the contrapositive of this statement.

(b) Prove the statement using a proof by contradiction.

Prove the following theorem via contradiction. Afterward, consider the difficulties one might encounter when trying to prove the result more directly.

Theorem 2.54. Assume that $x, y \in \mathbb{N}$.[1] If x divides y, then $x \leq y$.

Oftentimes a conditional proposition can be proved via a direct proof and by using a proof by contradiction. Most mathematicians view a direct proof to be more elegant than a proof by contradiction. When approaching the proof of a conditional proposition, you should strive for a direct proof. In general, if you are attempting to prove $A \implies B$ using a proof by contradiction and you end up with $\neg B$ and B (which yields a contradiction), then this is evidence that a proof by contradiction was unnecessary. On the other hand, if you end up with $\neg Q$ and Q, where Q is not the same as B, then a proof by contradiction is a reasonable approach.

[1] The given statement is not true if we replace $\mathbb{N}$ with $\mathbb{Z}$. Do you see why?

2.4 Introduction to Quantification

The sentence "$x > 0$" is not itself a proposition because its truth value depends on x. In this case, we say that x is a **free variable**. A sentence with at least one free variable is called a **predicate**. To turn a predicate into a proposition, we must either substitute values for each free variable or "quantify" the free variables. We will use notation such as $\boxed{P(x)}$ and $\boxed{Q(a,b)}$ to represent predicates with free variables x and a,b, respectively. The letters "P" and "Q" that we used in the previous sentence are not special; we can use any letter or symbol we want. For example, each of the following represents a predicate with the indicated free variables.

- $S(x) :=$ "$x^2 - 4 = 0$"
- $L(a,b) :=$ "$a < b$"
- $F(x,y) :=$ "x is friends with y"

Note that we used quotation marks above to remove some ambiguity. What would $S(x) = x^2 - 4 = 0$ mean? It looks like $S(x)$ equals 0, but actually we want $S(x)$ to represent the whole sentence "$x^2 - 4 = 0$". Also, notice that the order in which we utilize the free variables might matter. For example, compare $L(a,b)$ with $L(b,a)$.

One way we can make propositions out of predicates is by assigning specific values to the free variables. That is, if $P(x)$ is a predicate and x_0 is specific value for x, then $P(x_0)$ is now a proposition (and is either true or false).

Problem 2.55. Consider $S(x)$ and $L(a,b)$ as defined above. Determine the truth values of $S(0)$, $S(-2)$, $L(2,1)$, and $L(-3,-2)$. Is $L(2,b)$ a proposition or a predicate?

Besides substituting specific values for free variables in a predicate, we can also make a claim about which values of the free variables apply to the predicate.

Problem 2.56. Both of the following sentences are propositions. Decide whether each is true or false. What would it take to justify your answers?

(a) For all $x \in \mathbb{R}$, $x^2 - 4 = 0$.[2]

(b) There exists $x \in \mathbb{R}$ such that $x^2 - 4 = 0$.

Definition 2.57. "For all" is the **universal quantifier** and "there exists…such that" is the **existential quantifier**.

We can replace "there exists…such that" with phrases like "for some" (possibly with some other tweaking to the sentence). Similarly, "for all", "for any", "for every" are used interchangeably in mathematics (even though they might convey slightly different meanings in colloquial language). It is important to note that the existential quantifier is making a claim about "at least one" *not* "exactly one."

[2] The symbol $\mathbb{R}$ denotes the set of all real numbers.

Variables that are quantified with a universal or existential quantifier are said to be **bound**. To be a proposition, *all* variables must be bound. That is, in a proposition all variables are quantified.

We must take care to specify the collection of acceptable values for the free variables. Consider the sentence "For all x, $x > 0$." Is this sentence true or false? The answer depends on what set the universal quantifier applies to. Certainly, the sentence is false if we apply it for all $x \in \mathbb{Z}$. However, the sentence is true for all $x \in \mathbb{N}$. Context may resolve ambiguities, but otherwise, we must write clearly: "For all $x \in \mathbb{Z}$, $x > 0$" or "For all $x \in \mathbb{N}$, $x > 0$." The collection of intended values for a variable is called the **universe of discourse** (or simply **universe**).

Problem 2.58. Suppose our universe of discourse is the set of integers.

(a) Provide an example of a predicate $P(x)$ such that "For all x, $P(x)$" is true.

(b) Provide an example of a predicate $Q(x)$ such that "For all x, $Q(x)$" is false, but "There exists x such that $Q(x)$" is true.

If a predicate has more than one free variable, then we can build propositions by quantifying each variable. However, *the order of the quantifiers is extremely important!*

Problem 2.59. Let $P(x,y)$ be a predicate with free variables x and y in a universe of discourse U. One way to quantify the variables is "For all $x \in U$, there exists $y \in U$ such that $P(x,y)$." How else can the variables be quantified?

The next problem illustrates that at least some of the possibilities you discovered in the previous problem are *not* equivalent to each other.

Problem 2.60. Suppose the universe of discourse is the set of people and consider the predicate $M(x,y) :=$ "x is married to y". We can interpret the formal statement "For all x, there exists y such that $M(x,y)$" as meaning "Everybody is married to somebody." Interpret the meaning of each of the following statements in a similar way.

(a) For all x, there exists y such that $M(x,y)$.

(b) There exists y such that for all x, $M(x,y)$.

(c) For all x, for all y, $M(x,y)$.

(d) There exists x such that there exists y such that $M(x,y)$.

Problem 2.61. Suppose the universe of discourse is the set of real numbers and consider the predicate $F(x,y) :=$ "$x = y^2$". Interpret the meaning of each of the following statements.

(a) There exists x such that there exists y such that $F(x,y)$.

(b) There exists y such that there exists x such that $F(x,y)$.

(c) For all y, for all x, $F(x,y)$.

There are a couple of key points to keep in mind about quantification. To be a proposition, all variables must be quantified. This can happen in at least two ways:

- The variables are explicitly bound by quantifiers in the same sentence.
- The variables are implicitly bound by preceding sentences or by context. Statements of the form "Let $x = \ldots$" and "Assume $x \in \ldots$" bind the variable x and remove ambiguity.

Also, the order of the quantification is important. Reversing the order of the quantifiers can substantially change the meaning of a proposition.

Quantification and logical connectives ("and," "or," "If…, then…," and "not") enable complex mathematical statements. For example, if f is a function while c and L are real numbers, then the formal definition of $\lim_{x\to c} f(x) = L$, which you may have encountered in calculus, is:

> For all $\epsilon > 0$, there exists $\delta > 0$ such that for all x, if $0 < |x - c| < \delta$, then $|f(x) - L| < \epsilon$.

In order to study the abstract nature of complicated mathematical statements, it is useful to adopt some notation.

Definition 2.62. The universal quantifier "for all" is denoted $\boxed{\forall}$, and the existential quantifier "there exists…such that" is denoted $\boxed{\exists}$.

Using our abbreviations for the logical connectives and quantifiers, we can symbolically represent mathematical propositions. For example, the (true) proposition "There exists $x \in \mathbb{R}$ such that $x^2 - 1 = 0$" becomes "$(\exists x \in \mathbb{R})(x^2 - 1 = 0)$," while the (false) proposition "For all $x \in \mathbb{N}$, there exists $y \in \mathbb{N}$ such that $y < x$" becomes "$(\forall x)(x \in \mathbb{N} \implies (\exists y)(y \in \mathbb{N} \implies y < x))$" or "$(\forall x \in \mathbb{N})(\exists y \in \mathbb{N})(y < x)$."

Problem 2.63. Convert the following statements into statements using only logical symbols. Assume that the universe of discourse is the set of real numbers.

(a) There exists x such that $x^2 + 1$ is greater than zero.

(b) There exists a natural number n such that $n^2 = 36$.

(c) For every x, x^2 is greater than or equal to zero.

Problem 2.64. Express the formal definition of a limit (given above Definition 2.62) in logical symbols.

If you look closely, many of the theorems that we have encountered up until this point were of the form $A(x) \implies B(x)$, where $A(x)$ and $B(x)$ are predicates. For example, consider Theorem 2.2, which states, "If n is an even integer, then n^2 is an even integer." In this case, "n is an even integer" and "n^2 is an even integer" are both predicates. So, it would be reasonable to assume that the entire theorem statement is a predicate. However, it is standard practice to interpret the sentence $A(x) \implies B(x)$ to mean $(\forall x)(A(x) \implies B(x))$ (where the universe of discourse for x needs to be made clear). We can also retool such statements to "hide" the implication. In particular, $(\forall x)(A(x) \implies B(x))$ has the same meaning as $(\forall x \in U')B(x)$, where U' is the collection of items from the universe of discourse U that makes $A(x)$ true. For example, we could rewrite the statement of Theorem 2.2 as "For every even integer n, n^2 is even."

Problem 2.65. Find at least two instances of theorem statements that appeared earlier in the book and are written in the form $A(x) \implies B(x)$. Rewrite each in an equivalent way that makes the universal quantifier explicit while possibly suppressing the implication.

Problem 2.66. Consider the proposition "If $\epsilon > 0$, then there exists $N \in \mathbb{N}$ such that $1/N < \epsilon$." Assume the universe of discourse is the set $\mathbb{R}$.

(a) Express the statement in logical symbols. Is the statement true?

(b) Reverse the order of the quantifiers to get a new statement. Does the meaning change? If so, how? Is the new statement true?

The symbolic expression $(\forall x)(\forall y)$ can be abbreviated as $\boxed{\forall x, y}$ as long as x and y are elements of the same universe.

Problem 2.67. Express the statement "For all $x, y \in \mathbb{R}$ with $x < y$, there exists $m \in \mathbb{R}$ such that $x < m < y$" using logical symbols.

Problem 2.68. Rewrite each of the following propositions in words and determine whether the proposition is true or false.

(a) $(\forall n \in \mathbb{N})(n^2 \geq 5)$

(b) $(\exists n \in \mathbb{N})(n^2 - 1 = 0)$

(c) $(\exists N \in \mathbb{N})(\forall n > N)(\frac{1}{n} < 0.01)$

(d) $(\forall m, n \in \mathbb{Z})((2|m \wedge 2|n) \implies 2|(m+n))$

(e) $(\forall x \in \mathbb{N})(\exists y \in \mathbb{N})(x - 2y = 0)$

(f) $(\exists x \in \mathbb{N})(\forall y \in \mathbb{N})(y \leq x)$

To whet your appetite for the next section, consider how you might prove a statement of the form "For all $x \ldots$." If a statement is false, then its negation is true. How would you go about negating a statement involving quantifiers?

2.5 More About Quantification

When writing mathematical proofs, we do not explicitly use the symbolic representation of a given statement in terms of quantifiers and logical connectives. Nonetheless, having this notation at our disposal allows us to compartmentalize the abstract nature of mathematical propositions and provides us with a way to talk about the general structure involved in the construction of a proof.

Definition 2.69. Two propositions are **logically equivalent in a given universe of discourse** if and only if they have the same truth value in that universe. Two propositions are **logically equivalent** if and only if they are logically equivalent in every universe of discourse.

Problem 2.70. Consider the propositions $(\exists x \in U)(x^2 - 4 = 0)$ and $(\exists x \in U)(x^2 - 2 = 0)$, where U is the universe of discourse.

(a) Are these propositions logically equivalent if the universe of discourse is the set of real numbers?

(b) Provide an example of a universe of discourse such that the propositions yield different truth values.

(c) What can you conclude about the logical equivalence of these propositions?

It is worth pointing out an important distinction. Consider the propositions "All cars are red" and "All natural numbers are positive". Both of these are instances of the **logical form** $(\forall x)P(x)$. It turns out that the first proposition is false and the second is true; however, it does not make sense to attach a truth value to the logical form. A logical form is a blueprint for particular propositions. If we are careful, it makes sense to talk about whether two logical forms are logically equivalent. For example, $(\forall x)(P(x) \implies Q(x))$ is logically equivalent to $(\forall x)(\neg Q(x) \implies \neg P(x))$. For fixed $P(x)$ and $Q(x)$, these two forms will always have the same truth value independent of the universe of discourse. If you change $P(x)$ and $Q(x)$, then the truth value may change, but the two forms will still agree.

The next theorem tells us how to negate logical forms involving quantifiers.

Theorem 2.71. Let $P(x)$ be a predicate. Then

(a) $\neg(\forall x)P(x)$ is logically equivalent to $(\exists x)(\neg P(x))$

(b) $\neg(\exists x)P(x)$ is logically equivalent to $(\forall x)(\neg P(x))$.

Problem 2.72. Negate each of the following sentences. Disregard the truth value and the universe of discourse.

(a) $(\forall x)(x > 3)$

(b) $(\exists x)(x \text{ is prime} \wedge x \text{ is even})$

(c) All cars are red.

(d) Every Wookiee is named Chewbacca.

(e) Some hippies are Republican.

(f) Some birds are not angry.

(g) Not every video game will rot your brain.

(h) For all $x \in \mathbb{N}$, $x^2 + x + 41$ is prime.

(i) There exists $x \in \mathbb{Z}$ such that $1/x \notin \mathbb{Z}$.

(j) There is no function f such that if f is continuous, then f is not differentiable.

Using Theorem 2.71 and our previous results involving quantification, we can negate complex mathematical propositions by working from left to right. For example, if we negate the false proposition

$$(\exists x \in \mathbb{R})(\forall y \in \mathbb{R})(x + y = 0),$$

we obtain the proposition

$$\neg(\exists x \in \mathbb{R})(\forall y \in \mathbb{R})(x + y = 0),$$

which is logically equivalent to

$$(\forall x \in \mathbb{R})(\exists y \in \mathbb{R})(x + y \neq 0)$$

and must be true. For a more complicated example, consider the (false) proposition

$$(\forall x)[x > 0 \implies (\exists y)(y < 0 \wedge xy > 0)].$$

Then its negation

$$\neg(\forall x)[x > 0 \implies (\exists y)(y < 0 \wedge xy > 0)]$$

is logically equivalent to

$$(\exists x)[x > 0 \wedge \neg(\exists y)(y < 0 \wedge xy > 0)],$$

which happens to be logically equivalent to

$$(\exists x)[x > 0 \wedge (\forall y)(y \geq 0 \vee xy \leq 0)].$$

Can you identify the theorems that were used in the two examples above?

Problem 2.73. Negate each of the following propositions. Disregard the truth value and the universe of discourse.

(a) $(\forall n \in \mathbb{N})(\exists m \in \mathbb{N})(m < n)$

(b) For every $y \in \mathbb{R}$, there exists $x \in \mathbb{R}$ such that $y = x^2$.

(c) For all $y \in \mathbb{R}$, if y is not negative, then there exists $x \in \mathbb{R}$ such that $y = x^2$.

(d) For every $x \in \mathbb{R}$, there exists $y \in \mathbb{R}$ such that $y = x^2$.

(e) There exists $x \in \mathbb{R}$ such that for all $y \in \mathbb{R}$, $y = x^2$.

(f) There exists $y \in \mathbb{R}$ such that for all $x \in \mathbb{R}$, $y = x^2$.

(g) $(\forall x, y, z \in \mathbb{Z})((xy \text{ is even} \wedge yz \text{ is even}) \implies xz \text{ is even})$

(h) There exists a married person x such that for all married people y, x is married to y.

At this point, we should be able to use our understanding of quantification to construct counterexamples to complicated false propositions and proofs of complicated true propositions. Here are some general proof structures for various logical forms.

Skeleton Proof 2.74 (Direct Proof of $(\forall x)P(x)$)**.** Here is the general structure for a direct proof of the proposition $(\forall x)P(x)$. Assume U is the universe of discourse.

> *Proof.* *[State any upfront assumptions.]* Let $x \in U$.
>
> … *[Use definitions and known results.]* …
>
> Therefore, $P(x)$ is true. Since x was arbitrary, for all x, $P(x)$. □

Combining Skeleton Proof 2.74 with Skeleton Proof 2.38, we obtain the following skeleton proof.

Skeleton Proof 2.75 (Proof of $(\forall x)(P(x) \implies Q(x))$)**.** Below is the general structure for a direct proof of the proposition $(\forall x)(A(x) \implies B(x)$. Assume U is the universe of discourse.

> *Proof.* *[State any upfront assumptions.]* Let $x \in U$. Assume $A(x)$.
>
> … *[Use definitions and known results to derive $B(x)$]* …
>
> Therefore, $B(x)$. □

Skeleton Proof 2.76 (Proof of $(\forall x)P(x)$ by Contradiction)**.** Here is the general structure for a proof of the proposition $(\forall x)P(x)$ via contradiction. Assume U is the universe of discourse.

> *Proof.* *[State any upfront assumptions.]* For sake of a contradiction, assume that there exists $x \in U$ such that $\neg P(x)$.
>
> … *[Do something to derive a contradiction.]* …
>
> This is a contradiction. Therefore, for all x, $P(x)$ is true. □

Skeleton Proof 2.77 (Direct Proof of $(\exists x)P(x)$)**.** Here is the general structure for a direct proof of the proposition $(\exists x)P(x)$. Assume U is the universe of discourse.

> *Proof.* *[State any upfront assumptions.]* …
>
> … *[Use definitions and previous results to deduce that an x exists for which $P(x)$ is true; or if you have an x that works, just verify that it does.]* …
>
> Therefore, there exists $x \in U$ such that $P(x)$. □

Skeleton Proof 2.78 (Proof of $(\exists x)P(x)$ by Contradiction)**.** Below is the general structure for a proof of the proposition $(\exists x)P(x)$ via contradiction. Assume U is the universe of discourse.

Proof. *[State any upfront assumptions.]* For sake of a contradiction, assume that for all $x \in U$, $\neg P(x)$.

... *[Do something to derive a contradiction.]* ...

This is a contradiction. Therefore, there exists $x \in U$ such that $P(x)$. □

Note that if $Q(x)$ is a predicate for which $(\forall x)Q(x)$ is false, then a counterexample to this proposition amounts to showing $(\exists x)(\neg Q(x))$, which can be proved by following the structure of Skeleton Proof 2.77.

It is important to point out that sometimes we will have to combine various proof techniques in a single proof. For example, if you wanted to prove a proposition of the form $(\forall x)(P(x) \implies Q(x))$ by contradiction, we would start by assuming that there exists x in the universe of discourse such that $P(x)$ and $\neg Q(x)$.

Problem 2.79. For each of the following statements, determine its truth value. If the statement is false, provide a counterexample. Prove at least two of the true statements.

(a) For all $n \in \mathbb{N}$, $n^2 \geq 5$.

(b) There exists $n \in \mathbb{N}$ such that $n^2 - 1 = 0$.

(c) There exists $x \in \mathbb{N}$ such that for all $y \in \mathbb{N}$, $y \leq x$.

(d) For all $x \in \mathbb{Z}$, $x^3 \geq x$.

(e) For all $n \in \mathbb{Z}$, there exists $m \in \mathbb{Z}$ such that $n + m = 0$.

(f) There exists integers a and b such that $2a + 7b = 1$.

(g) There do not exist integers m and n such that $2m + 4n = 7$.

(h) For all integers a, b, c, if a divides bc, then either a divides b or a divides c.

To prove the next theorem, you might want to consider two different cases.

Theorem 2.80. For all integers, $3n^2 + n + 14$ is even.

Chapter 3

Set Theory and Topology

At its essence, all of mathematics is built on set theory. In this chapter, we will introduce some of the basics of sets and their properties.

3.1 Sets

Definition 3.1. A **set** is a collection of objects called **elements**. If A is a set and x is an element of A, we write $\boxed{x \in A}$. Otherwise, we write $\boxed{x \notin A}$. The set containing no elements is called the **empty set**, and is denoted by the symbol $\boxed{\emptyset}$. Any set that contains at least one element is referred to as a **nonempty set**.

If we think of a set as a box potentially containing some stuff, then the empty set is a box with nothing in it. One assumption we will make is that for any set A, $A \notin A$. The language associated to sets is specific. We will often define sets using the following notation, called **set-builder notation**:

$$\boxed{S = \{x \in A \mid x \text{ satisfies some condition}\}}$$

The first part "$x \in A$" denotes what type of x is being considered. The statements to the right of the vertical bar (not to be confused with "divides") are the conditions that x must satisfy in order to be members of the set. This notation is read as "The set of all x in A such that x satisfies some condition," where "some condition" is something specific about the restrictions on x relative to A.

There are a few sets that are commonly discussed in mathematics and have predefined symbols to denote them. We've already encountered the integers, natural numbers, and real numbers. Notice that our definition of the rational numbers uses set-builder notation.

- **Natural Numbers:** $\boxed{\mathbb{N} := \{1, 2, 3, \ldots\}}$. Some books will include zero in the set of natural numbers, but we do not.
- **Integers:** $\boxed{\mathbb{Z} := \{0, \pm 1, \pm 2, \pm 3, \ldots\}}$.
- **Rational Numbers:** $\boxed{\mathbb{Q} := \{a/b \mid a, b \in \mathbb{Z} \text{ and } b \neq 0\}}$.

- **Real Numbers:** $\boxed{\mathbb{R}}$ denotes the set of real numbers. We are taking for granted that you have some familiarity with this set.

Since the set of natural numbers consists of the positive integers, the natural numbers are sometimes denoted by $\mathbb{Z}^+$.

Problem 3.2. Unpack each of the following sets and see if you can find a simple description of the elements that each set contains.

(a) $A = \{x \in \mathbb{N} \mid x = 3k \text{ for some } k \in \mathbb{N}\}$

(b) $B = \{t \in \mathbb{R} \mid t^2 \leq 2\}$

(c) $C = \{t \in \mathbb{Z} \mid t^2 \leq 2\}$

(d) $D = \{m \in \mathbb{R} \mid m = 1 - \frac{1}{n}, \text{ where } n \in \mathbb{N}\}$

Problem 3.3. Write each of the following sentences using set-builder notation.

(a) The set of all real numbers less than $-\sqrt{2}$.

(b) The set of all real numbers greater than -12 and less than or equal to 42.

(c) The set of all even natural numbers.

Definition 3.4. If A and B are sets, then we say that A is a **subset** of B, written $\boxed{A \subseteq B}$, provided that every element of A is an element of B.

Observe that $A \subseteq B$ is equivalent to "For all x (in the universe of discourse), if $x \in A$, then $x \in B$." Since we know how to deal with "for all" statements and conditional propositions, we know how to go about proving $A \subseteq B$.

Problem 3.5. Suppose A and B are sets. Describe a skeleton proof for proving that $A \subseteq B$.

Every nonempty set always has two subsets.

Theorem 3.6. Let A be a set. Then

(a) $A \subseteq A$, and

(b) $\emptyset \subseteq A$.

Notice that if $A = \emptyset$, then parts (a) and (b) of the previous theorem say the same thing.

Problem 3.7. List all of the subsets of $A = \{1, 2, 3\}$.

Theorem 3.8 (Transitivity of subsets)**.** Suppose that A, B, and C are sets. If $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C$.

Definition 3.9. If $A \subseteq B$, then A is called a **proper subset** provided that $A \neq B$. In this case, we may write $\boxed{A \subset B}$ or $\boxed{A \subsetneq B}$.[1]

[1] *Warning:* Some books use $\subset$ to mean $\subseteq$.

Definition 3.10. Let A and B be sets in some universe of discourse U.

(a) The **union** of the sets A and B is $\boxed{A \cup B = \{x \in U \mid x \in A \text{ or } x \in B\}}$.

(b) The **intersection** of the sets A and B is $\boxed{A \cap B = \{x \in U \mid x \in A \text{ and } x \in B\}}$.

(c) The **set difference** of the sets A and B is $\boxed{A \setminus B = \{x \in U \mid x \in A \text{ and } x \notin B\}}$.

(d) The **complement of** A (relative to U) is the set $\boxed{A^c = U \setminus A = \{x \in U \mid x \notin A\}}$.

Definition 3.11. If two sets A and B have the property that $A \cap B = \emptyset$, then we say that A and B are **disjoint** sets.

Problem 3.12. Suppose that the universe of discourse is $U = \{1,2,3,4,5,6,7,8,9,10\}$. Let $A = \{1,2,3,4,5\}$, $B = \{1,3,5\}$, and $C = \{2,4,6,8\}$. Find each of the following.

(a) $A \cap C$

(b) $B \cap C$

(c) $A \cup B$

(d) $A \setminus B$

(e) $B \setminus A$

(f) $C \setminus B$

(g) B^c

(h) A^c

(i) $(A \cup B)^c$

(j) $A^c \cap B^c$

Problem 3.13. Suppose that the universe of discourse is $U = \mathbb{R}$. Let $A = [-3,-1)$, $B = (-2.5,2)$, and $C = (-2,0]$. Find each of the following.

(a) A^c

(b) $A \cap C$

(c) $A \cap B$

(d) $A \cup B$

(e) $(A \cap B)^c$

(f) $(A \cup B)^c$

(g) $A \setminus B$

(h) $A \setminus (B \cup C)$

(i) $B \setminus A$

Theorem 3.14. Let A and B be sets. If $A \subseteq B$, then $B^c \subseteq A^c$.

DEFINITION BELOW IS OUT OF PLACE SINCE PROPER SUBSET DEPENDS ON EQUALITY BEING DEFINED.

Definition 3.15. Two sets A and B are **equal**, denoted $\boxed{A = B}$, if and only if $A \subseteq B$ and $B \subseteq A$.

Given two sets A and B, if we want to prove $A = B$, then we have to do two separate mini-proofs: one for $A \subseteq B$ and one for $B \subseteq A$. It is common to label each mini-proof with "($\subseteq$)" and "($\supseteq$)", respectively.

INCLUDE SKELETON PROOF HERE...

Theorem 3.16. Let A and B be sets. Then $A \setminus B = A \cap B^c$.

For each of the next two theorems, you can choose to prove either part (a) or part (b). Of course, you are welcome to prove both parts, but you do not have to.

Theorem 3.17 (DeMorgan's Law)**.** Let A and B be sets. Then

(a) $(A \cup B)^c = A^c \cap B^c$, and

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

Theorem 3.18 (Distribution of Union and Intersection)**.** Let A, B, and C be sets. Then

(a) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$, and

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

The following definitions likely look familiar.

Definition 3.19 (Interval Notation)**.** For $a, b \in \mathbb{R}$ with $a < b$, we define the following.

(a) $(a, b) = \{x \in \mathbb{R} \mid a < x < b\}$

(b) $(a, \infty) = \{x \in \mathbb{R} \mid a < x\}$

(c) $(-\infty, b) = \{x \in \mathbb{R} \mid x < b\}$

(d) $[a, b] = \{x \in \mathbb{R} \mid a \leq x \leq b\}$

We analogously define $[a, b)$, $(a, b]$, $[a, \infty)$, and $(-\infty, b]$.

ADD SOME PROBLEMS INVOLVING INTERVALS...

3.2 Russell's Paradox

We now turn our attention to the issue of whether there is one mother of all universal sets. Before reading any further, consider this for a moment. That is, is there one largest set that all other sets are a subset of? Or, in other words, is there a set of all sets? To help wrap our heads around this issue, consider the following riddle, known as the **Barber of Seville Paradox**.

> In Seville, there is a barber who shaves all those men, and only those men, who do not shave themselves. Who shaves the barber?

Problem 3.20. In the Barber of Seville Paradox, does the barber shave himself or not?

Problem 3.20 is an example of a **paradox**. A paradox is a statement that can be shown, using a given set of axioms and definitions, to be both true and false. Recall that an axiom is a statement that is assumed to be true without proof. These are the basic building blocks from which all theorems are proved. Paradoxes are often used to show the inconsistencies in a flawed axiomatic theory. The term paradox is also used informally to describe a surprising or counterintuitive result that follows from a given set of rules. Now, suppose that there is a set of all sets and call it $\mathcal{U}$. That is, $\mathcal{U} := \{A \mid A \text{ is a set}\}$.

Problem 3.21. Given our definition of $\mathcal{U}$, explain why $\mathcal{U}$ is an element of itself.

If we continue with this line of reasoning, it must be the case that some sets are elements of themselves and some are not. Let X be the set of all sets that are elements of themselves and let Y be the set of all sets that are not elements of themselves.

Problem 3.22. Does Y belong to X or Y? Explain why this is a paradox.

The above paradox is one way of phrasing a paradox referred to as **Russell's Paradox**. How did we get into this mess in the first place?! By assuming the existence of a set of all sets, we can produce all sorts of paradoxes. The only way to avoid these types of paradoxes is to conclude that there is no set of all sets. That is, the collection of all sets cannot be a set itself.

According to naive set theory (i.e., approaching set theory using natural language as opposed to formal logic), any definable collection is a set. As Russell's Paradox illustrates, this leads to problems. It turns out that any proposition can be proved from a contradiction, and hence the presence of contradictions like Russell's Paradox would appear to be catastrophic for mathematics. Since set theory is often viewed as the basis for axiomatic development in mathematics, Russell's Paradox calls the foundations of mathematics into question. In response to this threat, a great deal of research went into developing consistent axioms (i.e., free of contradictions) for set theory in the early 20th century. In 1908, Ernst Zermelo proposed a collection of axioms for set theory that avoided the inconsistencies of naive set theory. In the 1920s, adjustments to Zermelo's axioms were made by Abraham Fraenkel, Thoralf Skolem, and Zermelo that resulted in a collection of nine axioms, called ZFC, where ZF stands for Zermelo and Fraenkel and C stands for the Axiom of Choice, which one of the nine axioms. Loosely speaking, the Axiom of Choice states that says that given any collection of sets, each containing at least one element, it is possible to make a selection of exactly one object from each set, even if the collection of sets is infinite. There was a period of time in mathematics when the Axiom of Choice was controversial, but nowadays it is generally accepted. There is a fascinating history concerning the Axiom of Choice, including its controversy, that I encourage you to read up on. The Wikipedia page for the Axiom of Choice is a good place to start. There are several competing axiomatic approaches to set theory, but ZFC is considered the canonical collection of axioms by most mathematicians.

Appendix C includes a few more examples of paradoxes. I suggest you spend some time thinking about a few of them.

3.3 Power Sets

We've already seen that using union, intersection, set difference, and complement we can create new sets (in the same universe) from existing sets. In this section, we will describe another way to generate new sets; however, the new sets will not "live" in the same universe this time.

Definition 3.23. If S is a set, then the **power set** of S is the set of subsets of S. The power set of S is denoted $\boxed{\mathcal{P}(S)}$.

It follows immediately from the definition that $A \subseteq S$ if and only if $A \in \mathcal{P}(S)$. For example, if $S = \{a, b\}$, then $\mathcal{P} = \{\emptyset, \{a\}, \{b\}, S\}$.

Problem 3.24. For each of the following sets, find the power set.

(a) $A = \{\circ, \triangle, \square\}$

(b) $B = \{a, \{a\}\}$

(c) $C = \emptyset$

(d) $D = \{\emptyset\}$

Problem 3.25. How many subsets do you think that a set with n elements has? What if $n = 0$? You do not need to prove your conjecture at this time. We will prove this later using mathematical induction.

It is important to realize that the concepts of *element* and *subset* need to be carefully delineated. For example, consider the set $A = \{x, y\}$. The object x is an element of A, but the object $\{x\}$ is both a subset of A and an element of $\mathcal{P}(A)$. This can get confusing rather quickly. Consider the set B from Problem 3.24. The set $\{a\}$ happens to be an element of B, a subset of B, and an element of $\mathcal{P}(B)$. The upshot is that it is important to pay close attention to whether "$\subseteq$" or "$\in$" is the proper symbol to use.

Theorem 3.26. Let S and T be sets. Then $S \subseteq T$ if and only if $\mathcal{P}(S) \subseteq \mathcal{P}(T)$.[2]

Theorem 3.27. Let S and T be sets. Then $\mathcal{P}(S) \cap \mathcal{P}(T) = \mathcal{P}(S \cap T)$.

Theorem 3.28. Let S and T be sets. Then $\mathcal{P}(S) \cup \mathcal{P}(T) \subseteq \mathcal{P}(S \cup T)$.

Problem 3.29. Provide a counterexample to show that it is not necessarily true that $\mathcal{P}(S) \cup \mathcal{P}(T) = \mathcal{P}(S \cup T)$. This verifies that the converse of Theorem 3.28 is not true in general. Is it ever true that $\mathcal{P}(S) \cup \mathcal{P}(T)$ and $\mathcal{P}(S \cup T)$ are equal?

3.4 Indexing Sets

Suppose we consider the following collection of open intervals:

$$(0,1), (0,1/2), (0,1/4), \ldots, (0,1/2^{n-1}), \ldots$$

This collection has a natural way for us to "index" the sets:

$$I_1 = (0,1), I_2 = (0,1/2), \ldots, I_n = (0,1/2^{n-1}), \ldots$$

In this case the sets are **indexed** by the set $\mathbb{N}$. The subscripts are taken from the **index set**. If we wanted to talk about an arbitrary set from this indexed collection, we could use the notation I_n.

Let's consider another example:

$$\{a\}, \{a,b\}, \{a,b,c\}, \ldots, \{a,b,c,\ldots,z\}$$

[2] To prove this theorem, you have to write two distinct subproofs: $A \implies B$ and $B \implies A$.

An obvious way to index these sets is as follows:

$$A_1 = \{a\}, A_2 = \{a,b\}, A_3 = \{a,b,c\}, \ldots, A_{26} = \{a,b,c,\ldots,z\}$$

In this case, the collection of sets is indexed by $\{1,2,\ldots,26\}$.

Using indexing sets in mathematics is an extremely useful notational tool, but it is important to keep straight the difference between the sets that are being indexed, the elements in each set being indexed, the indexing set, and the elements of the indexing set.

Any set (finite or infinite) can be used as an indexing set. Often capital Greek letters are used to denote arbitrary indexing sets and small Greek letters to represent elements of these sets. If the indexing set is a subset of $\mathbb{R}$, then it is common to use Roman letters as individual indices. Of course, these are merely conventions, not rules.

- If Δ is a set and we have a collection of sets indexed by Δ, then we may write $\{S_\alpha\}_{\alpha\in\Delta}$ to refer to this collection. We read this as "the set of S-alphas over alpha in Delta."
- If a collection of sets is indexed by $\mathbb{N}$, then we may write $\{U_n\}_{n\in\mathbb{N}}$ or $\{U_n\}_{n=1}^{\infty}$.
- Borrowing from this idea, a collection $\{A_1,\ldots,A_{26}\}$ may be written as $\{A_n\}_{n=1}^{26}$.

Definition 3.30. Suppose we have a collection $\{A_\alpha\}_{\alpha\in\Delta}$.

(a) The **union of the entire collection** is defined via

$$\boxed{\bigcup_{\alpha\in\Delta} A_\alpha = \{x \mid x \in A_\alpha \text{ for some } \alpha \in \Delta\}.}$$

(b) The **intersection of the entire collection** is defined via

$$\boxed{\bigcap_{\alpha\in\Delta} A_\alpha = \{x \mid x \in A_\alpha \text{ for all } \alpha \in \Delta\}.}$$

In the special case that $\Delta = \mathbb{N}$, we write

$$\bigcup_{n=1}^{\infty} A_n = \{x \mid x \in A_n \text{ for some } n \in \mathbb{N}\} = A_1 \cup A_2 \cup A_3 \cup \cdots$$

and

$$\bigcap_{n=1}^{\infty} A_n = \{x \mid x \in A_n \text{ for all } n \in \mathbb{N}\} = A_1 \cap A_2 \cap A_3 \cap \cdots$$

Similarly, if $\Delta = \{1,2,3,4\}$, then

$$\bigcup_{n=1}^{4} A_n = A_1 \cup A_2 \cup A_3 \cup A_4 \quad \text{and} \quad \bigcap_{n=1}^{4} A_n = A_1 \cap A_2 \cap A_3 \cap A_4.$$

Notice the difference between "$\bigcup$" and "$\cup$" (respectively, "$\bigcap$" and "$\cap$").

Problem 3.31. Let $\{I_n\}_{n\in\mathbb{N}}$ be the collection of open intervals from the beginning of the section. Find each of the following.

(a) $\bigcup_{n\in\mathbb{N}} I_n$

(b) $\bigcap_{n\in\mathbb{N}} I_n$

Problem 3.32. Let $\{A_n\}_{n=1}^{26}$ be the collection from earlier in the section. Find each of the following.

(a) $\bigcup_{n=1}^{26} A_n$

(b) $\bigcap_{n=1}^{26} A_n$

Problem 3.33. Let $S_n = \{x \in \mathbb{R} \mid n-1 < x < n\}$, where $n \in \mathbb{N}$. Find each of the following.

(a) $\bigcup_{n=1}^{\infty} S_n$

(b) $\bigcap_{n=1}^{\infty} S_n$

Problem 3.34. Let $T_n = \{x \in \mathbb{R} \mid -\frac{1}{n} < x < \frac{1}{n}\}$, where $n \in \mathbb{N}$. Find each of the following.

(a) $\bigcup_{n=1}^{\infty} T_n$

(b) $\bigcap_{n=1}^{\infty} T_n$

Problem 3.35. For each $r \in \mathbb{Q}$ (the rational numbers), let N_r be the set containing all real numbers *except* r. Find each of the following.

(a) $\bigcup_{r\in\mathbb{Q}} N_r$

(b) $\bigcap_{r\in\mathbb{Q}} N_r$

Definition 3.36. A collection of sets $\{A_\alpha\}_{\alpha\in\Delta}$ is **pairwise disjoint** if $A_\alpha \cap A_\beta = \emptyset$ for $\alpha \neq \beta$.

Problem 3.37. Draw a Venn diagram of a collection of 3 sets that are pairwise disjoint.

Problem 3.38. Provide an example of a collection of three sets, say $\{A_1, A_2, A_3\}$, such that the collection is *not* pairwise disjoint, but $\bigcap_{n=1}^{3} A_n = \emptyset$.

For each of the next two theorems, you can choose to prove either part (a) or part (b).

Theorem 3.39 (Generalized Distribution of Union and Intersection)**.** Let $\{A_\alpha\}_{\alpha\in\Delta}$ be a collection of sets and let B be any set. Then

(a) $B \cup \left(\bigcap_{\alpha\in\Delta} A_\alpha\right) = \bigcap_{\alpha\in\Delta} (B \cup A_\alpha)$, and

(b) $B \cap \left(\bigcup_{\alpha\in\Delta} A_\alpha\right) = \bigcup_{\alpha\in\Delta} (B \cap A_\alpha)$.

Theorem 3.40 (Generalized DeMorgan's Law)**.** Let $\{A_\alpha\}_{\alpha\in\Delta}$ be a collection of sets. Then

(a) $\left(\bigcup_{\alpha\in\Delta} A_\alpha\right)^C = \bigcap_{\alpha\in\Delta} A_\alpha^C$, and

(b) $\left(\bigcap_{\alpha\in\Delta} A_\alpha\right)^C = \bigcup_{\alpha\in\Delta} A_\alpha^C$.

At the end of Section 3.2, we mentioned the Axiom of Choice. Using the language of indexing sets, we can now state this axiom precisely.

Axiom 3.41 (Axiom of Choice)**.** For every indexed collection $\{A_\alpha\}_{\alpha\in\Delta}$ of nonempty sets, there exists an indexed collection $\{a_\alpha\}_{\alpha\in\Delta}$ of elements such that $a_\alpha \in A_\alpha$ for each $\alpha \in \Delta$.

3.5 Cartesian Products of Sets

ADD INTRO BLURB HERE...(move to Chapter 3 (after indexing sets, partly to shorten this chapter?)

Definition 3.42. For each $n \in \mathbb{N}$, we define an n**-tuple** to be an ordered list of n elements of the form $(a_1, a_2, \ldots, a_n)$. We refer to a_i as the ith **component** (or **coordinate**) of $(a_1, a_2, \ldots, a_n)$. Two n-tuples $(a_1, a_2, \ldots, a_n)$ and $(b_1, b_2, \ldots, b_n)$ are equal if and only if $a_i = b_i$ for all $1 \leq i \leq n$. A 2-tuple (a, b) is more commonly referred to as an **ordered pair** while a 3-tuple (a, b, c) is often called an **ordered triple**.

We can use the notion of n-tuples to construct new sets from existing sets.

Definition 3.43. If A and B are sets, the **Cartesian product** (or **direct product**) of A and B, denoted $A \times B$ (read as "A times B" or "A cross B"), is the set of all ordered pairs where the first component is from A and the second component is from B. In set-builder notation, we have

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

We similarly define the Cartesian product of n sets, say $A_1, \ldots, A_n$, by

$$\boxed{\prod_{i=1}^{n} A_i := A_1 \times \cdots \times A_n := \{(a_1, \ldots, a_n) \mid a_j \in A_j \text{ for all } 1 \leq j \leq n\}},$$

where A_i is referred to as the ith **factor** of the Cartesian product. As a special case, the set

$$\underbrace{A \times \cdots \times A}_{n \text{ factors}}$$

is often abbreviated as A^n.

Example 3.44. If $A = \{a, b, c\}$ and $B = \{☺, ☹\}$, then

$$A \times B = \{(a, ☺), (a, ☹), (b, ☺), (b, ☹), (c, ☺), (c, ☹)\}.$$

Example 3.45. The standard two-dimensional plane $\mathbb{R}^2$ and standard three space $\mathbb{R}^3$ are familiar examples of Cartesian products. In particular, we have

$$\mathbb{R}^2 = \mathbb{R} \times \mathbb{R} = \{(x, y) \mid x, y \in \mathbb{R}\}$$

and

$$\mathbb{R}^3 = \mathbb{R} \times \mathbb{R} \times \mathbb{R} = \{(x, y, z) \mid x, y, z \in \mathbb{R}\}.$$

Problem 3.46. Consider the sets A and B from Example 3.44.

(a) Find $B \times A$.

(b) Find $B \times B$.

Problem 3.47. If A and B are both finite sets, then how many elements will $A \times B$ have?

Problem 3.48. Let $A = \{1, 2, 3\}$, $B = \{1, 2\}$, and $C = \{1, 3\}$. Find $A \times B \times C$.

Problem 3.49. Let $X = [0, 1]$ and $Y = \{1\}$. Write each of the following using set-builder notation and then describe the set geometrically (e.g., draw a picture).

(a) $X \times Y$

(b) $Y \times X$

(c) $X \times X$

(d) $Y \times Y$

Problem 3.50. If A is a set, then what is $A \times \emptyset$ equal to?

Problem 3.51. Given sets A and B, when will $A \times B$ be equal to $B \times A$?

We now turn our attention to subsets of Cartesian products.

Problem 3.52. Write $\mathbb{N} \times \mathbb{R}$ using set-builder notation and then describe this set geometrically by interpreting it as a subset of $\mathbb{R}^2$.

Theorem 3.53. Let A, B, C, and D be sets. If $A \subseteq C$ and $B \subseteq D$, then $A \times B \subseteq C \times D$.

Problem 3.54. Is it true that if $A \times B \subseteq C \times D$, then $A \subseteq C$ and $B \subseteq D$? Don't forget to think about cases involving the empty set.

Problem 3.55. Is every subset of $C \times D$ of the form $A \times B$, where $A \subseteq C$ and $B \subseteq D$? If so, prove it. If not, find a counterexample.

Problem 3.56. If A, B, and C are nonempty sets, is $A \times B$ a subset of $A \times B \times C$?

Problem 3.57. Let $A = [2, 5]$, $B = [3, 7]$, $C = [1, 3]$, and $D = [2, 4]$. Compute each of the following.

(a) $(A \cap B) \times (C \cap D)$

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

(c) $(A \cup B) \times (C \cup D)$

(d) $(A \times C) \cup (B \times D)$

(e) $A \times (B \cap C)$

(f) $(A \times B) \cap (A \times C)$

(g) $A \times (B \cup C)$

(h) $(A \times B) \cup (A \times C)$

Problem 3.58. Let A, B, C, and D be sets. Determine whether each of the following statements is true or false. If a statement is true, prove it. Otherwise, provide a counterexample.

(a) $(A \cap B) \times (C \cap D) = (A \times C) \cap (B \times D)$

(b) $(A \cup B) \times (C \cup D) = (A \times C) \cup (B \times D)$

(c) $A \times (B \cap C) = (A \times B) \cap (A \times C)$

(d) $A \times (B \cup C) = (A \times B) \cup (A \times C)$

(e) $A \times (B \setminus C) = (A \times B) \setminus (A \times C)$

Problem 3.59. If A and B are sets, conjecture a way to rewrite $(A \times B)^C$ in a way that involves A^C and B^C and then prove your conjecture.

3.6 Topology of $\mathbb{R}$

For this entire section, our universe of discourse is the set of real numbers. You may assume all the usual basic algebraic properties of the real numbers (addition, subtraction, multiplication, division, commutative property, distribution, etc.).

Recall that an **axiom** is a statement that we *assume* to be true. Here are some useful axioms of the real numbers.

Axiom 3.60. If p and q are two different real numbers in $\mathbb{R}$, then there is a number between them.

Problem 3.61. Given real numbers p and q with $p < q$, construct a real number x such that $p < x < q$. We know such a point must exist by the previous axiom, but this problem is asking you to produce an actual candidate.

Axiom 3.62 (Linear ordering)**.** If a, b, and c are real numbers, then:

(a) If $a < b$ and $b < c$, then $a < c$;

(b) Exactly one of the following is true: (i) $a < b$, (ii) $a = b$, or (iii) $a > b$.

Axiom 3.63. If p is a real number, then there exists $q, r \in \mathbb{R}$ such that $q < p < r$.

Axiom 3.64 (Archimedean Property)**.** If x is a real number, then either (i) x is an integer or (ii) there exists an integer n, such that $n < x < n + 1$.

Definition 3.65. Suppose $a, b \in \mathbb{R}$ such that $a < b$. The intervals $(a, b), (-\infty, b), (a, \infty)$ are called **open intervals** while the interval $[a, b]$ is called a **closed interval**. An interval like $[a, b)$ is neither open nor closed.

We will always assume that any time we write $(a, b), [a, b], (a, b]$, or $[a, b)$ that $a < b$.

Problem 3.66. Give an example of each of the following.

(a) An open interval.

(b) A closed interval.

(c) An interval that is neither open nor closed.

(d) An infinite set that is not an interval.

Definition 3.67. A set U is called an **open set** if and only if for every $t \in U$, there exists an open interval containing t such that the open interval is a subset of U. We define the empty set to be open.

Problem 3.68. Prove that the set $I = (1, 2)$ is an open set.

Theorem 3.69. Every open interval is an open set.

Theorem 3.70. The set of real numbers forms an open set.

Problem 3.71. Provide an example of an open set that is not a single open interval.

Theorem 3.72. Every closed interval is not an open set.

Theorem 3.73. If $x \in \mathbb{R}$, then the set $\{x\}$ is not open.

Problem 3.74. Determine whether $\{4, 17, 42\}$ is an open set. Briefly justify your assertion.

Theorem 3.75. If A and B are open sets, then

(a) $A \cup B$ is an open set, and

(b) $A \cap B$ is an open set.

Theorem 3.76. If $\{U_\alpha\}_{\alpha \in \Delta}$ is a collection of open sets, then $\bigcup_{\alpha \in \Delta} U_\alpha$ is an open set.

Problem 3.77. Give an example of each of the following.

(a) A collection of open sets $\{B_\alpha\}_{\alpha \in \Delta}$ such that $\bigcap_{\alpha \in \Delta} B_\alpha$ is an open set.

(b) A collection of open sets $\{U_\alpha\}_{\alpha \in \Delta}$ such that $\bigcap_{\alpha \in \Delta} U_\alpha$ is not an open set.

Remark 3.78. Taken together, Theorems 3.75–3.76 and Problem 3.77 tell us that the union of any collection of open sets is open, but that the intersection of open sets may or may not be open. However, if we are taking the intersection of finitely many open sets, then the intersection will be open.

Problem 3.79. Determine whether each of the following sets is open or not open.

(a) $W = \bigcup_{n=2}^{\infty} \left(n - \frac{1}{2}, n\right)$

(b) $X = \bigcap_{n=1}^{\infty} \left(-\frac{1}{n}, \frac{1}{n}\right)$

Definition 3.80. A point p is a **limit point of the set** S if and only if for every open interval I containing p, there exists a point $q \in I$ such that $q \in S$ with $q \neq p$.

Problem 3.81. Consider the open interval $S = (1, 2)$. Prove each of the following.

(a) The points 1 and 2 are limit points of S.

(b) If $p \in S$, then p is a limit point of S.

(c) If $p < 1$ or $p > 2$, then p is not a limit point of S.

Theorem 3.82. A point p is a limit point of (a, b) if and only if $p \in [a, b]$.

Problem 3.83. Prove that the point $p = 0$ is a limit point of $S = \{\frac{1}{n} \mid n \in \mathbb{N}\}$. Are there any other limit points?

Problem 3.84. Provide an example of a set S such that 1 is a limit point of S, $1 \neq S$, and S contains no intervals.

Problem 3.85. Provide an example of a set T with exactly two limit points.

Theorem 3.86. If $p \in \mathbb{R}$, then p is a limit point of $\mathbb{Q}$.

Definition 3.87. A set is called **closed** if and only if it contains all of its limit points.

Problem 3.88. Provide an example of each of the following. You do not need to prove that your answers are correct.

(a) A closed set.

(b) A set that is not closed.

(c) A set that is open and closed.

(d) A set that neither open nor closed.

Theorem 3.89. The set $[a, b]$ is closed.

Theorem 3.90. The set U is open if and only if U^C is closed.

Theorem 3.91. Every finite set is closed.

Problem 3.92. Prove or provide a counterexample: If a set S is not open, then it is closed.

Theorem 3.93. The set of real numbers is both open and closed.

Theorem 3.94. The set of rational numbers is neither open nor closed.

Theorem 3.95. The empty set is both open and closed.

Theorem 3.96. If $\{A_\alpha\}_{\alpha\in\Delta}$ is a collection of closed sets, then $\bigcap_{\alpha\in\Delta} A_\alpha$ is a closed set.

Problem 3.97. Prove or provide a counterexample: If A and B are closed sets, then $A\cup B$ is also closed.

Problem 3.98. Provide an example of a collection of closed sets $\{A_\alpha\}_{\alpha\in\Delta}$ such that $\bigcup_{\alpha\in\Delta} A_\alpha$ is a *not* closed set.

You should take the time to compare what happened in Theorem 3.96 and Problem 3.98 to what we stated in Remark 3.78.

Chapter 4

Induction

In this chapter, we introduce mathematical induction, which is a proof technique that is useful for proving statements of the form $(\forall n \in \mathbb{N})P(n)$, or more generally $(\forall n \in \mathbb{Z})(n \geq a \implies P(n))$, where $P(n)$ is some predicate and $a \in \mathbb{Z}$.

4.1 Introduction to Induction

Consider the claims:

(a) For all $n \in \mathbb{N}$, $1 + 2 + 3 + \cdots + n = \dfrac{n(n+1)}{2}$.

(b) For all $n \in \mathbb{N}$, $n^2 + n + 41$ is prime.

Let's take a look at potential proofs.

"Proof" of (a). If $n = 1$, then $1 = \frac{1(1+1)}{2}$. If $n = 2$, then $1 + 2 = 3 = \frac{2(2+1)}{2}$. If $n = 3$, then $1 + 2 + 3 = 6 = \frac{3(3+1)}{2}$, and so on. □

"Proof" of (b). If $n = 1$, then $n^2 + n + 41 = 43$, which is prime. If $n = 2$, then $n^2 + n + 41 = 47$, which is prime. If $n = 3$, then $n^2 + n + 41 = 53$, which is prime, and so on. □

Are these actual proofs? No! In fact, the second claim isn't even true. If $n = 41$, then $n^2 + n + 41 = 41^2 + 41 + 41 = 41(41 + 1 + 1)$, which is not prime since it has 41 as a factor. It turns out that the first claim is true, but what we wrote cannot be a proof since the same type of reasoning when applied to the second claim seems to prove something that isn not actually true. We need a rigorous way of capturing "and so on" and a way to verify whether it really is "and so on."

Recall that an axiom is a basic mathematical assumption. The following axiom is one of the Peano Axioms, which is a collection of axioms for the natural numbers introduced in the 19th century by Italian mathematician Giuseppe Peano.

Axiom 4.1 (Axiom of Induction)**.** Let $S \subseteq \mathbb{N}$ such that both

(i) $1 \in S$, and

(ii) if $k \in S$, then $k+1 \in S$.

Then $S = \mathbb{N}$.

We can think of the set S as a ladder, where the first hypothesis as saying that we have a first rung of a ladder. The second hypothesis says that if we are on any arbitrary rung of the ladder, then we can always get to the next rung. Taken together, this says that we can get from the first rung to the second, from the second to the third, and in general, from any kth rung to the $(k+1)$st rung, so that our ladder is actually $\mathbb{N}$. I am hoping that you agree that the Axiom of Induction is a pretty reasonable assumption.

At the end of Section 3.2, we briefly discussed ZFC, which is the standard choice for axiomatic set theory. It turns out that one can prove the Axiom of Induction as a theorem in ZFC. However, that will not be the approach we take. Instead, we are assuming the Axiom of Induction is true. Using this axiom, we can prove the following theorem, known as the Principle of Mathematical Induction, or PMI for short.

Theorem 4.2 (Principle of Mathematical Induction)**.** Let $P(1), P(2), P(3), \ldots$ be a sequence of statements, one for each natural number.[1] Assume

(i) $P(1)$ is true, and

(ii) if $P(k)$ is true, then $P(k+1)$ is true.

Then $P(n)$ is true for all $n \in \mathbb{N}$.[2]

The Principle of Mathematical Induction (PMI) provides us with a process for proving statements of the form: "For all $n \in \mathbb{N}$, $P(n)$," where $P(n)$ is some predicate involving n. Hypothesis (i) above is called the **base step** (or **base case**) while (ii) is called the **inductive step**.

You should not confuse *mathematical induction* with *inductive reasoning* associated with the natural sciences. Inductive reasoning is a scientific method whereby one induces general principles from observations. On the other hand, mathematical induction is a deductive form of reasoning used to establish the validity of a proposition.

Skeleton Proof 4.3 (Proof of $(\forall n \in \mathbb{N})P(n)$ by Induction)**.** Here is the general structure for a proof by induction.

[1] Think of $P(n)$ as a predicate, where $P(1)$ is the statement that corresponds to substituting in the value 1 for n.

[2] *Hint:* Let $S = \{k \in \mathbb{N} \mid P(k) \text{ is true}\}$ and use the Axiom of Induction. The set S is sometimes called the **truth set**. Your job is to show that the truth set is all of $\mathbb{N}$.

Proof. We proceed by induction.

(i) Base step: *[Verify that $P(1)$ is true. This often, but not always, amounts to plugging $n = 1$ into two sides of some claimed equation and verifying that both sides are actually equal.]*

(ii) Inductive step: *[Your goal is to prove "For all $k \in \mathbb{N}$, if $P(k)$ is true, then $P(k+1)$ is true."]* Let $k \in \mathbb{N}$ and assume that $P(k)$ is true. *[Do something to derive that $P(k+1)$ is true.]* Therefore, $P(k+1)$ is true.

Thus, by induction, $P(n)$ is true for all $n \in \mathbb{N}$. □

Prove the next few theorems using induction. The first result may look familiar from calculus.

Theorem 4.4. For all $n \in \mathbb{N}$, $\displaystyle\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$.[3]

Theorem 4.5. For all $n \in \mathbb{N}$, 3 divides $4^n - 1$.

Theorem 4.6. For all $n \in \mathbb{N}$, 6 divides $n^3 - n$.

Theorem 4.7. Let $p_1, p_2, \ldots, p_n$ be n distinct points arranged on a circle. Then the number of line segments joining all pairs of points is $\frac{n^2-n}{2}$.

Problem 4.8. Consider a grid of squares that is 2^n squares wide by 2^n squares long, where $n \in \mathbb{N}$. One of the squares has been cut out, but you don't know which one! You have a bunch of L-shapes made up of 3 squares. Prove that you can perfectly cover this chessboard with the L-shapes (with no overlap) for any $n \in \mathbb{N}$. Figure 4.1 depicts one possible covering for the case involving $n = 2$.

4.2 More on Induction

In the previous section, we discussed proving statements of the form $(\forall n \in \mathbb{N})P(n)$. Mathematical induction can actually be used to prove a broader family of results; namely, those of the form

$$(\forall n \in \mathbb{Z})(n \geq a \implies P(n))$$

for any value $a \in \mathbb{Z}$. Theorem 4.2 handles the special case when $a = 1$. The ladder analogy from the previous section holds for this more general situation, too.

Theorem 4.9 (Principle of Mathematical Induction)**.** Let $P(a), P(a+1), P(a+2), \ldots$ be a sequence of statements, one for each integer greater than or equal to a. Assume that

[3] Recall that $\displaystyle\sum_{i=1}^{n} i = 1 + 2 + 3 + \cdots + n$, by definition.

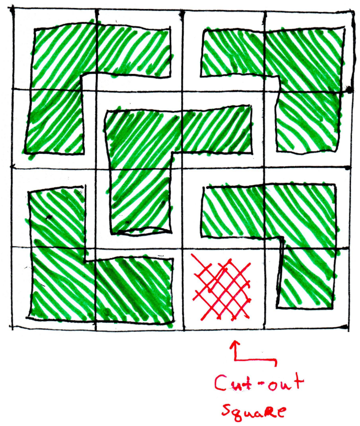

Figure 4.1: One possible covering for the case involving $n = 2$ for Problem 4.8.

(i) $P(a)$ is true, and

(ii) if $P(k)$ is true, then $P(k+1)$ is true.

Then $P(n)$ is true for all integers $n \geq a$.[4]

Theorem 4.9 gives a process for proving statements of the form: "For all integers $n \geq a$, $P(n)$." As before, hypothesis (i) is called the **base step**, and (ii) is called the **inductive step**.

Skeleton Proof 4.10 (Proof of $(\forall n \in \mathbb{Z})(n \geq a \implies P(n))$ by Induction)**.** Here is the general structure for a proof by induction when the base case does not necessarily involve $a = 1$.

Proof. We proceed by induction.

(i) Base step: *[Verify that $P(a)$ is true. This often, but not always, amounts to plugging $n = a$ into two sides of some claimed equation and verifying that both sides are actually equal.]*

(ii) Inductive step: *[Your goal is to prove "For all $k \in \mathbb{Z}$, if $P(k)$ is true, then $P(k+1)$ is true."]* Let $k \geq a$ be an integer and assume that $P(k)$ is true. *[Do something to derive that $P(k+1)$ is true.]* Therefore, $P(k+1)$ is true.

Thus, by induction, $P(n)$ is true for all integers $n \geq a$. $\square$

Theorem 4.11. Let A be a finite set with n elements. Then $\mathcal{P}(A)$ is a set with 2^n elements.[5]

Theorem 4.12. For all integers $n \geq 0$, 4 divides $9^n - 5$.

Theorem 4.13. For all integers $n \geq 0$, 4 divides $6 \cdot 7^n - 2 \cdot 3^n$.

[4] *Hint:* Mimic the proof of Theorem 4.2, but this time use the set $S = \{k \in \mathbb{N} \mid P(a+k-1) \text{ is true}\}$.

[5] We encountered this theorem back in Section 3.3 (see Conjecture 3.25), but we didn't prove it. If you prove this theorem using induction, at some point, you will need to argue that if you add one more element to a finite set, then you end up with twice as many subsets. Also, notice that A may have 0 elements.

Theorem 4.14. For all integers $n \geq 2$, $2^n > n+1$.

Theorem 4.15. For all integers $n \geq 0$, $1 + 2^1 + 2^2 + \cdots + 2^n = 2^{n+1} - 1$.

Theorem 4.16. Fix a real number $r \neq 1$. For all integers $n \geq 0$,

$$1 + r^1 + r^2 + \cdots + r^n = \frac{r^{n+1} - 1}{r - 1}.$$

Theorem 4.17. For all integers $n \geq 3$, $2 \cdot 3 + 3 \cdot 4 + \cdots + (n-1) \cdot n = \dfrac{(n-2)(n^2+2n+3)}{3}$.

Theorem 4.18. For all integers $n \geq 1$, $\dfrac{1}{1 \cdot 2} + \dfrac{1}{2 \cdot 3} + \cdots + \dfrac{1}{n(n+1)} = \dfrac{n}{n+1}$.

Theorem 4.19. For all integers $n \geq 1$, $\dfrac{1}{1 \cdot 3} + \dfrac{1}{3 \cdot 5} + \dfrac{1}{5 \cdot 7} + \cdots + \dfrac{1}{(2n-1)(2n+1)} = \dfrac{n}{2n+1}$.

Theorem 4.20. For all integers $n \geq 0$, $3^{2n} - 1$ is divisible by 8.

Theorem 4.21. For all integers $n \geq 2$, $2^n < (n+1)!$.

Theorem 4.22. For all integers $n \geq 2$, $2 \cdot 9^n - 10 \cdot 3^n$ is divisible by 4.

We now consider an induction problem of a different sort, where you have to begin with some experimentation.

DOUBLE CHECK THIS PROBLEM. MAYBE A CLOSED FORM IS MORE NATURAL.

Problem 4.23. For any $n \in \mathbb{N}$, say that n straight lines are "safely drawn in the plane" if no two of them are parallel and no three of them meet in a single point. Let $S(n)$ be the number of regions formed when n straight lines are safely drawn in the plane.

(a) Compute $S(1)$, $S(2)$, $S(3)$, and $S(4)$.

(b) Conjecture a recursive formula for $S(n)$. That is, find a formula for $S(n)$ that involves some of the previous terms $S(n-1), S(n-2)$, etc. If necessary, first compute a few more values of $S(n)$.

(c) Prove your conjecture.

4.3 Complete Induction

There is another formulation of induction, where the inductive step begins with a set of assumptions rather than one single assumption. This method is sometimes called **complete induction** or **strong induction**.

Theorem 4.24 (Principle of Complete Mathematical Induction)**.** Let $P(1), P(2), P(3), \ldots$ be a sequence of statements, one for each natural number. Assume that

(i) $P(1)$ is true, and

(ii) For all $k \in \mathbb{N}$, if $P(j)$ is true for all $j \in \mathbb{N}$ such that $j \leq k$, then $P(k+1)$ is true.

Then $P(n)$ is true for all $n \in \mathbb{N}$.

Note the difference between ordinary induction (Theorems 4.2 and 4.9) and complete induction. For the induction step of complete induction, we are not only assuming that $P(k)$ is true, but rather that $P(j)$ is true for all j from 1 to k. Despite the name, complete induction is not any stronger or more powerful than ordinary induction. It is worth pointing out that anytime ordinary induction is an appropriate proof technique, so is complete induction. So, when should we use complete induction?

In the inductive step, you need to reach $P(k+1)$, and you should ask yourself which of the previous cases you need to get there. If all you need, is the statement $P(k)$, then ordinary induction is the way to go. If two preceding cases, $P(k-1)$ and $P(k)$, are necessary to reach $P(k+1)$, then complete induction is appropriate. In the extreme, if one needs the full range of preceding cases (i.e., all statements $P(1), P(2), \ldots, P(k)$), then again complete induction should be utilized.

Note that in situations where complete induction is appropriate, it might be the case that you need to verify more than one case in the base step. The number of base cases to be checked depends on how one needs to "look back" in the induction step.

Skeleton Proof 4.25 (Proof of $(\forall n \in \mathbb{N})P(n)$ by Complete Induction)**.** Here is the general structure for a proof by complete induction.

> *Proof.* We proceed by induction.
>
> (i) Base step: *[Verify that $P(1)$ is true. Depending on the statement, you may also need to verify that $P(k)$ is true for other specific values of k.]*
>
> (ii) Inductive step: *[Your goal is to prove "For all $k \in \mathbb{N}$, if for each $k \in \mathbb{N}$, $P(j)$ is true for all $j \in \mathbb{N}$ such that $j \leq k$, then $P(k+1)$ is true."]* Let $k \in \mathbb{N}$. Suppose $P(j)$ is true for all $j \leq k$. *[Do something to derive that $P(k+1)$ is true.]* Therefore, $P(k+1)$ is true.
>
> Thus, by complete induction, $P(n)$ is true for all integers $n \geq a$. □

Recall that Theorem 4.9 generalized Theorem 4.2 and allowed us to handle situations where the base case was something other than $P(1)$. We can generalize complete induction in the same way, but we won't write this down as a formal theorem.

Theorem 4.26. Define a sequence of numbers by $a_1 = 1$, $a_2 = 3$, and $a_n = 3a_{n-1} - 2a_{n-2}$ for all natural numbers $n \geq 3$. Then $a_n = 2^n - 1$ for all $n \in \mathbb{N}$.

Theorem 4.27. Define a sequence of numbers by $a_1 = 3, a_2 = 5, a_3 = 9$ and $a_n = 2a_{n-1} + a_{n-2} - 2a_{n-3}$ for all natural numbers $n \geq 4$. Then $a_n = 2^n + 1$ for all $n \in \mathbb{N}$.

Theorem 4.28. Define a sequence of numbers by $a_1 = 1$, $a_2 = 3$, and $a_n = a_{n-1} + a_{n-2}$ for all natural numbers $n \geq 3$. Then $a_n < \left(\frac{7}{4}\right)^n$ for all $n \in \mathbb{N}$.

Theorem 4.29. Define a sequence of numbers by $a_1 = 1$, $a_2 = 2$, $a_3 = 3$ and $a_n = a_{n-1} + a_{n-2} + a_{n-3}$ for all natural numbers $n \geq 4$. Then $a_n < 2^n$ for all $n \in \mathbb{N}$.

Theorem 4.30. Define a sequence of numbers by $a_1 = 1$, $a_2 = 1$, and $a_n = a_{n-1} + a_{n-2}$ for all natural numbers $n \geq 3$. Then $a_n < \left(\frac{5}{3}\right)^n$ for all $n \in \mathbb{N}$.

Problem 4.31. Prove that every amount of postage that is at least 12 cents can be made from 4-cent and 5-cent stamps.

Problem 4.32. Prove that for any $n \geq 4$, one can obtain n dollars using only $2 bills and $5 bills.

Problem 4.33. Consider a grid of squares that is 2 squares wide and n squares long. Using n dominoes that are 1 square by 2 squares, there are many ways to perfectly cover this chessboard with no overlap. How many? Prove your answer.

The final theorem of this chapter is known as the Well-Ordering Principle (WOP). As you shall see, this seemingly obvious theorem requires a bit of work to prove. It is worth noting that in some axiomatic systems, the WOP is sometimes taken as an axiom. However, in our case, the result follows from complete induction.

Theorem 4.34 (Well-Ordering Principle)**.** Every nonempty subset of the natural numbers contains a least element.[6]

It turns out that the Well-Ordering Principle (Theorem 4.34) and the Axiom of Induction (Axiom 4.1) are equivalent. In other words, one can prove the Well-Ordering Principle from the Axiom of Induction, as we have done, but one can also prove the Axiom of Induction if the Well-Ordering Principle is assumed.

[6] *Hint:* Towards a contradiction, suppose S is a nonempty subset of $\mathbb{N}$ that does not have a least element. Define the proposition $P(n)$:="n is not an element of S". Use complete induction.

Chapter 5

Three Famous Theorems

As the title suggests, we tackle three famous theorems in this chapter.

5.1 The Fundamental Theorem of Arithmetic

The goal of this section is to prove The Fundamental Theorem of Arithmetic, which is a theorem that you have been intimately familiar with since grade school, but perhaps don't recognize by name. The Fundamental Theorem of Arithmetic (sometimes called the Unique Factorization Theorem) states that every natural number greater than 1 is either prime or is the product of prime numbers, where this product is unique up to the order of the factors. For example, the natural number 12 has prime factorization $2^2 \cdot 3$, where the order in which we write the prime factors (i.e., 2, 2, and 3) is irrelevant. That is, $2^2 \cdot 3$, $2 \cdot 3 \cdot 2$, and $3 \cdot 2^2$ are all the same prime factorization of 12. The requirement that the factors be prime is necessary since factorizations containing composite numbers may not be unique. For example, $12 = 2 \cdot 6$ and $12 = 3 \cdot 4$, but these factorizations into composite numbers are distinct. We've just thrown around a few fancy terms; we should make sure we understand their precise meaning.

Definition 5.1. Let $n \in \mathbb{Z}$.

(a) If $a \in \mathbb{Z}$ such that a divides n, then we say that a is a **factor** of n.

(b) If $n \in \mathbb{N}$ such that n has exactly two distinct positive factors (namely, 1 and n itself), then n is called **prime**.

(c) If $n > 1$ such that n is not prime, then n is called **composite**.

Problem 5.2. Is 1 a prime number or composite number? Explain your answer.

Problem 5.3. List the first 10 prime numbers.

The next theorem makes up half of the Fundamental Theorem of Arithmetic.

Lemma 5.4. Let n be a natural number greater than 1. Then n can be expressed as a product of primes. That is, we can write

$$n = p_1 p_2 \cdots p_k,$$

where each of $p_1, p_2, \ldots, p_k$ is a prime number (not necessarily distinct).[1]

Lemma 5.4 states that we can write every natural number greater than 1 as a product of primes, but it does not say that the primes and the number of times each prime appears are unique. To prove uniqueness, we will need Euclid's Lemma (Theorem 5.12). To prove Euclid's Lemma, we will utilize a special case of Bezout's Lemma (Lemma 5.10), the proof of which relies on the following result, known as the Division Algorithm. One can prove the Division Algorithm using the Well-Ordering Principle (Theorem 4.34) and we have the necessary tools to do this, but we will skip proving the Division Algorithm for now. If you are interested in the proof of the Division Algorithm, I encourage you to give it a try yourself or to look up the proof in a textbook or an online resource. It's worth pointing out that we are stating the Division Algorithm for natural numbers, but the theorem holds more generally for integers, but we must replace $0 \leq r < n$ with $0 \leq r < |n|$.

Theorem 5.5 (Division Algorithm)**.** If $m, n \in \mathbb{N}$, then there exists unique $q, r \in \mathbb{N} \cup \{0\}$ such that $m = nq + r$ with $0 \leq r < n$.

The numbers q and r from the Division Algorithm are referred to as **quotient** and **remainder**, respectively.

Problem 5.6. Suppose $m = 27$ and $n = 5$. Find the quotient and remainder that are guaranteed to exists by the Division Algorithm. That is, find the unique $q, r \in \mathbb{N}$ such that $0 \leq r < n$ and $m = nq + r$.

It's useful to have some additional terminology.

Definition 5.7. Let $m, n \in \mathbb{Z}$ such that at least one of m or n is nonzero. The **greatest common divisor** (gcd) of m and n, denoted $\boxed{\gcd(m,n)}$, is the largest positive integer that is a factor of both m and n. If $\gcd(m,n) = 1$, we say that m and n are **relatively prime**.

Problem 5.8. Find $\gcd(54, 72)$.

Problem 5.9. Provide an example of two natural numbers that are relatively prime.

The next result is a special case of a theorem known as Bézout's Lemma (or Bézout's Identity). Ultimately, we will need this theorem to prove Euclid's Lemma (Theorem 5.12), which we then use to prove uniqueness for the Fundamental Theorem of Arithmetic (Theorem 5.14).

[1] *Hint:* Use a proof by contradiction. Let S be the set of natural numbers for which the theorem fails. For sake of a contradiction, assume $S \neq \emptyset$. By the Well-Ordering Principle (Theorem 4.34), S contains a least element, say n. Then n cannot be prime since this would satisfy the theorem. So, it must be the case that n has a divisor other than 1 and itself. This implies that there exists natural numbers a and b greater than 1 such that $n = ab$. Since n was our smallest counterexample, what can you conclude about both a and b? Use this information to derive a counterexample for n.

Lemma 5.10 (Special Case of Bézout's Lemma)**.** If $p, a \in \mathbb{Z}$ such that p is prime and p and a are relatively prime, then there exists $s, t \in \mathbb{Z}$ such that $ps + at = 1$.[2]

Problem 5.11. Consider the natural numbers 2 and 7, which happen to be relatively prime. Find integers s and t guaranteed to exist according to Lemma 5.10. That is, find $s, t \in \mathbb{Z}$ such that $2s + 7t = 1$.

The following theorem is known as Euclid's Lemma. See if you can prove it using Lemma 5.10.

Theorem 5.12 (Euclid's Lemma)**.** Assume that p is prime. If p divides ab, where $a, b \in \mathbb{N}$, then either p divides a or p divides b.[3]

In Euclid's Lemma, it is crucial that p is prime as illustrated by the next problem.

Problem 5.13. Provide an example of integers a, b, d such that d divides ab yet d does not divide a and d does not divide b.

Alright, we are finally ready to tackle the proof of the Fundamental Theorem of Arithmetic.

Theorem 5.14 (Fundamental Theorem of Arithmetic)**.** Every natural number greater than 1 can be expressed uniquely (up to the order in which they appear) as the product of one or more primes.[4]

The Fundamental Theorem of Arithmetic is one of the many reasons why 1 is not considered a prime number. If 1 were prime, prime factorizations would not be unique.

5.2 The Irrationality of $\sqrt{2}$

In this section we will prove one of the oldest and most important theorems in mathematics: $\sqrt{2}$ is irrational (see Theorem 5.16). First, we need to know what this means.

[2] *Hint:* Consider the set $S := \{ps + at > 0 \mid s, t \in \mathbb{Z}\}$. First, observe that $p \in S$ (choose $s = 1$ and $t = 0$). It follows that S is nonempty. By the Well-Ordering Principle (Theorem 4.34), S contains a least element, say d. Then there exists $s_1, t_1 \in \mathbb{Z}$ such that $d = ps_1 + at_1$. Our goal is to show that $d = 1$. Now, choose $m \in S$. Then there exists $s_2, t_2 \in \mathbb{Z}$ such that $m = ps_2 + at_2$. By the definition of d, we know $d \leq m$. By the Division Algorithm, there exists unique $q, r \in \mathbb{N} \cup \{0\}$ such that $m = qd + r$ with $0 \leq r < d$. Now, solve for r and then replace m and d with $ps_1 + at_1$ and $ps_2 + at_2$, respectively. You should end up with an expression for r involving p, a, s_1, s_2, t_1, and t_2. Next, rearrange this expression to obtain something of the form $r = p(\text{junk}) + a(\text{stuff})$. What does the minimality of d imply about r? You should be able to conclude that m is a multiple of d. That is, every element of S is a multiple of d. However, recall that $p \in S$, p is prime, and p and a are relatively prime. What can you conclude about d?

[3] *Hint:* If p divides a, we are done. So, assume otherwise. That is, assume that p does not divide a, so that p and a are relatively prime. Apply Lemma 5.10 to p and a and then multiply the resulting equation by b. Try to conclude that p divides b.

[4] *Hint:* Let n be a natural number greater than 1. By Lemma 5.4, we know that n can be expressed as a product of primes. All that remains is to prove that this product is unique (up to the order in which they appear). For sake of a contradiction, suppose $p_1 p_2 \cdots p_k$ and $q_1 q_2 \cdots q_l$ are both prime factorizations of n. Your goal is to prove that $k = l$ and that each p_i is equal to some q_j. Make repeated use of Euclid's Lemma.

Definition 5.15. Let $r \in \mathbb{R}$.

(a) We say that r is **rational** if and only if $r = \frac{m}{n}$, where $m, n \in \mathbb{Z}$ and $n \neq 0$.

(b) In contrast, we say that r is **irrational** if and only if it is not rational.

The Pythagoreans were an ancient secret society that followed their spiritual leader: Pythagoras of Samos (c. 570–495 BCE). The Pythagoreans believed that the way to spiritual fulfillment and to an understanding of the universe was through the study of mathematics. They believed that all of mathematics, music, and astronomy could be described via whole numbers and their ratios. In modern mathematical terms they believed that all numbers are rational. Attributed to Pythagoras is the saying, "Beatitude is the knowledge of the perfection of the numbers of the soul." And their motto was "All is number."

Thus they were stunned when one of their own—Hippasus of Metapontum (c. 5th century BCE)—discovered that the side and the diagonal of a square are incommensurable. That is, the ratio of the length of the diagonal to the length of the side is irrational. Indeed, if the side of the square has length a, then the diagonal will have length $a\sqrt{2}$; the ratio is $\sqrt{2}$ (see Figure 5.1).

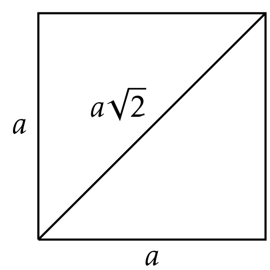

Figure 5.1: The side and diagonal of a square are incommensurable.

Theorem 5.16. The real number $\sqrt{2}$ is irrational.[5]

As one might expect, the Pythagoreans were unhappy with this discovery. Legend says that Hippasus was expelled from the Pythagoreans and was perhaps drowned at sea. Ironically, this result, which angered the Pythagoreans so much, is probably their greatest contribution to mathematics: the discovery of irrational numbers.

See if you can generalize the technique in the proof of Theorem 5.16 to prove the next two theorems.

Theorem 5.17. Let p be a prime number. Then $\sqrt{p}$ is irrational.

Theorem 5.18. Let p and q be distinct primes. Then $\sqrt{pq}$ is irrational.

Problem 5.19. State a generalization of Theorem 5.18 and briefly describe how its proof would go. Be as general as possible.

[5] *Hint:* Use a proof by contradiction. That is, suppose that there exist $m, n \in \mathbb{Z}$ such that $n \neq 0$ and $\sqrt{2} = \frac{m}{n}$. How many factors of 2 are on each side of this equation according to the Fundamental Theorem of Arithmetic? Don't actually try to find the exact number of 2's, but rather see if you can figure out if there is an odd or even number of 2's on each side.

It is important to point out that not every positive irrational number is equal to the square root of some natural number. For example, π is irrational, but is not equal to the square root of a natural number. It is also worth pointing out that our approach for proving that $\sqrt{2}$ was irrational was not the most efficient. However, our technique was easy to generalize to handle results like Theorem 5.17.

5.3 The Infinitude of Primes

The highlight of this section is Theorem 5.22, which states that there are infinitely many primes. The first known proof of this theorem is in Euclid's *Elements* (c. 300 BCE). Euclid stated it as follows:

> **Proposition IX.20.** Prime numbers are more than any assigned multitude of prime numbers.

There are a few interesting observations to make about Euclid's proposition and his proof. First, notice that the statement of the theorem does not contain the word "infinity." The Greek's were skittish about the idea of infinity. Thus, he proved that there were more primes than any given finite number. Today we'd say that they are infinite. In fact, Euclid proved that there are more than *three* primes and concluded that there were more than any finite number. While you would lose points for such a proof in this class, we can forgive Euclid for this less-than-rigorous proof; in fact, it is easy to turn his proof into the general one that you will give below. Lastly, Euclid's proof was geometric. He was viewing his numbers as line segments with integral length. The modern concept of number was not developed yet.

Prior to tackling a proof of Theorem 5.22, we need to prove a couple lemmas. The proof of the first lemma is provided for you.

Lemma 5.20. The only natural number that divides 1 is 1.

Proof. Let m be a natural number that divides 1. We know that $m \geq 1$ because 1 is the smallest positive integer. Since m divides 1, there exists $k \in \mathbb{N}$ such that $1 = mk$. Since $k \geq 1$, we see that $mk \geq m$. But $1 = mk$, and so $1 \geq m$. Thus, we have $1 \leq m \leq 1$, which implies that $m = 1$, as desired. □

Lemma 5.21. Let p be a prime number and let $n \in \mathbb{Z}$. If p divides n, then p does not divide $n+1$.[6]

We are now ready to prove the following important theorem.

Theorem 5.22. There are infinitely many prime numbers.[7]

[6] *Hint:* Use a proof by contradiction and utilize the previous lemma.

[7] *Hint:* Use a proof by contradiction. That is, assume that there are finitely many primes, say $p_1, p_2, \ldots, p_k$. Consider the product of all of them and then add 1.

Chapter 6

Relations and Partitions

6.1 Relations

While there is no agreed upon universal definition of mathematics, one could argue that mathematics focuses on the study of patterns and relationships. Certain types of relationships occur over and over in mathematics. One way of formalizing the abstract nature and structure of these relationships is with the notion of *relations*. In Chapter 7, we will see that a function is a special type of relation.

Recall from Section 3.5 that the Cartesian product of two sets A and B, written $A \times B$, is the set of all ordered pairs (a,b), where $a \in A$ and $b \in B$. That is, $A \times B = \{(a,b) \mid a \in A, b \in B\}$.

Definition 6.1. Let A and B be sets. A **relation** R **from** A **to** B is a subset of $A \times B$. If R is a relation from A to B and $(a,b) \in R$, then we say that a **is related to** b and we may write aRb in place of $(a,b) \in R$. If R is a relation from A to the same set A, then we say that R is a **relation on** A.

Example 6.2. The set $\mathbb{N} \times \mathbb{R}$ from Problem 3.52 is an example of a relation on $\mathbb{R}$ since $\mathbb{N} \times \mathbb{R}$ is a subset of $\mathbb{R} \times \mathbb{R}$.

It is important to notice that the order in which we write things for relations matters. In particular, if R is a relation from A to B and aRb, then it may or may not be the case that bRa.

Example 6.3. If $A = \{a,b,c,d,e\}$ and $B = \{1,2,3,4\}$, then the set of ordered pairs

$$R = \{(a,1),(a,2),(a,4),(c,2),(d,2),(e,2),(e,4)\}$$

is an example of a relation from A to B. In this case, we could write $(c,2) \in R$ or $cR2$. We could also say that a is related to 1, 2, and 4.

Example 6.4. As in the previous example, let $A = \{a,b,c,d,e\}$. One possible relation on A is given by

$$R = \{(a,a),(a,b),(a,c),(b,b),(b,a),(b,c),(c,d),(c,e),(d,d),(d,a),(d,c),(e,a)\}.$$

Example 6.5. Consider the set of accounts A on the social media platform Twitter. On Twitter, each account has a set of accounts that they follow. We can model this situation mathematically using a relation on A. Define T on A via xTy if and only if x follows y on Twitter. As a set

$$T = \{(x, y) \in A \times A \mid x \text{ follows } y \text{ on Twitter}\}.$$

Example 6.6. You are already familiar with many relations. For example, $=$, $\leq$, and $<$ are each examples of relations on the real numbers. We could say that $(3, \pi)$ is in the relation $\leq$ and the relation $<$ since $3 \leq \pi$ and $3 < \pi$. However, $(3, \pi)$ is not in the relation $=$ since $3 \neq \pi$. Also, notice that order matters for the relations $\leq$ and $<$ yet does not for $=$. For example, $(-\sqrt{2}, 4)$ is in the relation $\leq$ while $(4, -\sqrt{2})$ is not.

Example 6.7. Define the relation S from $\{-1, 1\}$ to $\mathbb{Z}$ via $1Sx$ if and only if x is even and $-1Sx$ if and only if x is odd. That is, 1 is related to all even integers and -1 is related to all odd integers.

Example 6.8. Let A be any set. Since $\emptyset \subseteq A \times A$, the empty set forms a relation on A. This relation is called the **empty relation** on A.

Relations can be represented using digraphs. A **digraph** (short for *directed graph*) is a discrete graph that consists of a set of vertices connected by edges, where the edges have a direction associated with them. If R is a relation from A to B, then the elements of A and B are the vertices of the digraph and there is a directed edge from $a \in A$ to $b \in B$ if and only if (a, b) is in the relation R (i.e., aRb). We can visually represent digraphs by using dots to represent the vertices and arrows to represent directed edges. We will not make a distinction between a digraph and its visual representation. Utilizing a digraph to represent a relation may be impractical if there is a large number of vertices or directed edges.

Example 6.9. Consider the relation given in Example 6.3. The corresponding digraph is depicted in Figure 6.1. Notice that we have placed the vertices corresponding to elements of A on the left and the elements of B on the right. This is standard practice, but what really matters is the edge connections not how the vertices are placed on the page.

Problem 6.10. Let $A = \{1, 2, 3, 4, 5, 6\}$ and $B = \{1, 2, 3, 4\}$ and define D from A to B via $(a, b) \in D$ if and only if $a - b$ is divisible by 2. List the ordered pairs in D and draw the corresponding digraph.

If R is a relation on A (i.e., a relation from A to A), then we can simplify the structure of the digraph by only utilizing one copy of A for the vertices. In this case, we may have directed edges that point from a vertex to itself. When drawing digraphs for a relation on a set, we will default to this simplified digraph (like the one depicted in Figure 6.2(b)).

Example 6.11. Figure 6.2(a) represents the relation of Example 6.4 as a digraph from A to A while the digraph in Figure 6.2(b) provides a streamlined representation of the same relation that uses the elements in A only once instead of twice.

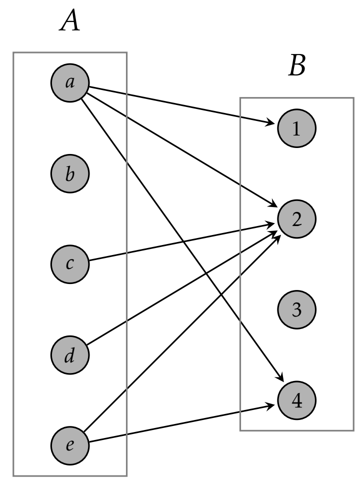

Figure 6.1: Digraph for a relation from $A = \{a, b, c, d, e\}$ to $B = \{1, 2, 3, 4\}$.

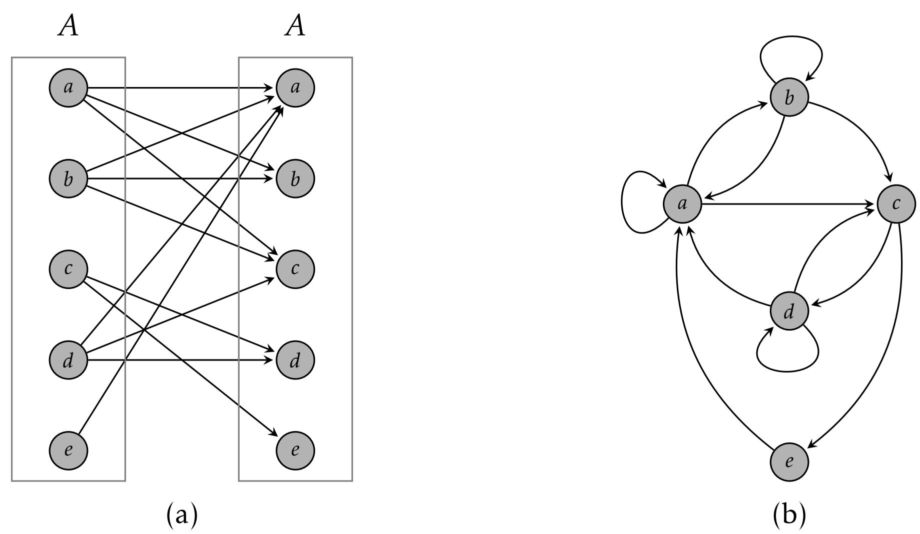

Figure 6.2: Two variations of digraphs for a relation on $A = \{a, b, c, d, e\}$.

Problem 6.12. Let $A = \{1, 2, 3, 4, 5, 6\}$ and define $|$ on A via $x|y$ if and only if x divides y. List the ordered pairs in $|$ and draw the corresponding digraph.

Problem 6.13. Let $A = \{a, b, c, d\}$ and define R on A via

$$R = \{(a, a), (a, b), (a, c), (b, b), (b, a), (b, c), (c, c), (c, a), (c, b), (d, d)\}.$$

(a) Draw the digraph for R.

(b) Draw the digraph for the empty relation on A.

We can also visually represent a relation by plotting the points in the relation. In particular, if R is a relation from A to B and aRb, we can plot all points (a, b) that satisfy aRb in two dimensions, where we interpret the set A to be the horizontal axis and B to be the vertical axis. We will refer to this visual representation of a relation as the **graph** of the relation.

Example 6.14. When we write $x^2 + y^2 = 1$, we are implicitly defining a relation. In particular, the relation is the set of ordered pairs (x, y) satisfying $x^2 + y^2 = 1$, namely $\{(x,y) \in \mathbb{R}^2 \mid x^2 + y^2 = 1\}$. The graph of this relation in $\mathbb{R}^2$ is the unit circle centered at the origin in the plane as shown in Figure 6.3.

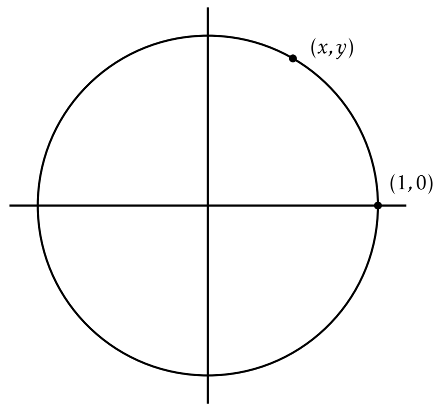

Figure 6.3: Graph of the relation determined by $x^2 + y^2 = 1$.

Problem 6.15. For each of the following, draw a portion of the graph that represents the relation as a subset of $\mathbb{R}^2$.

(a) $\{(x,y) \in \mathbb{R}^2 \mid y = x^2\}$

(b) $\{(x,y) \in \mathbb{Z}^2 \mid y = x^2\}$

(c) $\{(x,y) \in \mathbb{R}^2 \mid y^2 = x\}$

(d) $\{(x,y) \in \mathbb{N} \times \mathbb{R} \mid y^2 = x\}$

Problem 6.16. Draw a portion of the graph that represents the relation $\leq$ on $\mathbb{R}$.

For a relation on a set, it is natural to consider the collection of elements that a given element is related to. For example, a user's "Following List" on Twitter is the set of accounts on Twitter that the user is following.

Definition 6.17. Let R be a relation on a set A. For each $a \in A$, we define the **set of relatives of** a **with respect to** R via

$$\boxed{\operatorname{rel}(a, R) := \{b \in A \mid aRb\}}.$$

We also define the **collection of the sets of relatives with respect to** R by

$$\boxed{\operatorname{Rel}(R) := \{\operatorname{rel}(a) \mid a \in A\}}.$$

If R is clear from the context, we will usually write $\boxed{\mathrm{rel}(a)}$ in place of $\mathrm{rel}(a,R)$. In terms of digraphs, $\mathrm{rel}(a)$ is the collection of vertices that have a directed edge pointing towards them from the vertex labeled by a. In graph theory, this collection of vertices is called the **out neighborhood** of a and each such vertex is called an **out neighbor**. Notice that $\mathrm{Rel}(R)$ is a set of sets. In particular, an element in $\mathrm{Rel}(R)$ is a subset of A—equivalently, an element of $\mathcal{P}(A)$.

Example 6.18. Consider the relation given in Example 6.4. By inspecting the ordered pairs in R or by looking at the digraph in Figure 6.2(b), we see that

$$\mathrm{rel}(a)=\{a,b,c\},\ \mathrm{rel}(b)=\{a,b,c\},\ \mathrm{rel}(c)=\{d,e\},\ \mathrm{rel}(d)=\{a,c,d\},\ \mathrm{rel}(e)=\{a\},$$

so that $\mathrm{Rel}(R)=\{\{a,b,c\},\{d,e\},\{a,c,d\},\{a\}\}$.

Problem 6.19. Consider the relation given in Problem 6.13(a). Find $\mathrm{Rel}(R)$ by determining $\mathrm{rel}(x)$ for each $x\in A$.

Problem 6.20. Describe the collection of the sets of relatives with respect to the empty relation from Problem 6.13(b).

Problem 6.21. Let P denote the set of all people with accounts on Facebook and define the relation F on P via xFy if and only if x is friends with y. Describe rel(Maria), where Maria is the name of a specific Facebook user. What is $\mathrm{Rel}(F)$?

Problem 6.22. Define the relation $\equiv_5$ on $\mathbb{Z}$ via $a\equiv_5 b$ if and only if $a-b$ is divisible by 5. Find $\mathrm{rel}(1)$, $\mathrm{rel}(2)$, and $\mathrm{rel}(6)$. How many distinct sets are in $\mathrm{Rel}(\equiv_5)$? List the distinct sets in $\mathrm{Rel}(\equiv_5)$.

Problem 6.23. Consider the relation $\leq$ on $\mathbb{R}$. If $x\in\mathbb{R}$, what is $\mathrm{rel}(x)$?

Problem 6.24. Suppose R is a relation on $A=\{1,2,3,4,5\}$ such that $\mathrm{rel}(1)=\{1,3,4\}$, $\mathrm{rel}(2)=\{4\}$, $\mathrm{rel}(3)=\{3,4,5\}$, $\mathrm{rel}(4)=\{1,2\}$, and $\mathrm{rel}(5)=\emptyset$. List the ordered pairs in R and draw the corresponding digraph.

We will now examine three important properties that a relation on a set may or may not possess.

Definition 6.25. Let R be a relation on a set A.

(a) The relation R is **reflexive** if for all $a\in A$, aRa.

(b) The relation R is **symmetric** if for all $a,b\in A$, if aRb, then bRa.

(c) The relation R is **transitive** if for all $a,b,c\in A$, if aRb and bRc, then aRc.

Example 6.26. Here are a few examples that illustrate the concepts in the previous definition.

(a) The relation $=$ on $\mathbb{R}$ is reflexive, symmetric, and transitive.

(b) The relation $\leq$ is reflexive and transitive on $\mathbb{R}$, but not symmetric. However, notice that $<$ is transitive on $\mathbb{R}$, but neither symmetric nor reflexive.

(c) If S is a set, then $\subseteq$ on $\mathcal{P}(S)$ is reflexive and transitive, but not symmetric.

Problem 6.27. Determine whether the relations given in each of the following is reflexive, symmetric, or transitive.

(a) Example 6.4

(b) Problem 6.13

Problem 6.28. Suppose R is a relation on a set A.

(a) Explain what it means for R to *not* be reflexive.

(b) Explain what it means for R to *not* be symmetric.

(c) Explain what it means for R to *not* be transitive.

Problem 6.29. Let $A = \{a, b, c, d, e\}$.

(a) Define a relation R on A that is reflexive, but not symmetric or transitive.

(b) Define a relation S on A that is symmetric, but not reflexive or transitive.

(c) Define a relation T on A that is transitive, but not reflexive or symmetric.

Problem 6.30. Given a relation R on a finite set A, describe what each of reflexive, symmetric, and transitive look like in terms of a digraph. That is, draw pictureS that represent each of reflexive, symmetric, and transitive. One thing to keep in mind is that the elements used in the definitions of symmetric and transitive do not have to be distinct. So, you might need to consider multiple cases.

Below, we provide skeleton proofs for proving that a relation is reflexive, symmetric, or transitive. Notice that the skeleton proof for proving that a relation is reflexive is a special case of Skeleton Proof 2.74. Similarly, the skeleton proofs involving symmetric and transitive are both special cases of Skeleton Proof 2.75. It is important to point out that every relation on the empty set is vacuously reflexive, symmetric, and transitive. In the skeleton proofs below, we are implicitly assuming that the set in question is nonempty. In some circumstances, it may be necessary to mention the possibility of the empty set.

Skeleton Proof 6.31 (Proof that a relation is reflexive)**.** Here is the general structure for proving that a relation is reflexive.

Proof. Assume R is a relation on A defined by (or satisfying)... *[Use the given definition (or describe the given property) of R]*. Let $a \in A$.

... *[Use the definition (or property) of R to verify that aRa]* ...

Therefore, the relation R is reflexive on A. □

Skeleton Proof 6.32 (Proof that a relation is symmetric)**.** Here is the general structure for proving that a relation is symmetric.

> *Proof.* Assume R is a relation on A defined by (or satisfying)... *[Use the given definition (or describe the given property) of R].* Let $a, b \in A$ and suppose aRb.
>
> ... *[Use assumption that aRb with definition (or property) of R to verify that bRa]* ...
>
> Therefore, the relation R is symmetric on A. □

Skeleton Proof 6.33 (Proof that a relation is transitive)**.** Here is the general structure for proving that a relation is transitiv.

> *Proof.* Assume R is a relation on A defined by (or satisfying)... *[Use the given definition (or describe the given property) of R].* Let $a, b, c \in A$ and suppose aRb and bRc.
>
> ... *[Use assumption that aRb and bRc with definition (or property) of R to verify that aRc]* ...
>
> Therefore, the relation R is transitive on A. □

Problem 6.34. Determine whether each of the following relations is reflexive, symmetric, or transitive. In each case, you should either provide a specific counterexample or a proof.

(a) Consider the relation T described in Example 6.5.

(b) Consider the relation F described in Problem 6.21.

(c) Consider the relation $\equiv_5$ described in Problem 6.22.

(d) Let P be the set of all people and define H via xHy if and only if x and y have the same height.

(e) Let P be the set of all people and define T via xTy if and only if x is taller than y.

(f) Consider the relation "divides" on $\mathbb{N}$.

(g) Let L be the set of lines and define $\|$ via $l_1 \| l_2$ if and only if l_1 is parallel to l_2.

(h) Let $C[0,1]$ be the set of continuous functions on $[0,1]$. Define $f \sim g$ if and only if

$$\int_0^1 |f(x)|\,dx = \int_0^1 |g(x)|\,dx.$$

(i) Define R on $\mathbb{N}$ via nRm if and only if $n+m$ is even.

(j) Define D on $\mathbb{R}$ via $(x,y) \in D$ if and only if $x = 2y$.

(k) Define F on $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ via $(a,b)F(c,d)$ if and only $\frac{a}{b} = \frac{c}{d}$.

(l) Define $\sim$ on $\mathbb{R}^2$ via $(x_1, y_1) \sim (x_2, y_2)$ if and only if $x_1^2 + y_1^2 = x_2^2 + y_2^2$.

(m) Define S on $\mathbb{R}$ via xSy if and only if $\lfloor x \rfloor = \lfloor y \rfloor$, where $\lfloor x \rfloor$ is the greatest integer less than or equal to x (e.g., $\lfloor \pi \rfloor = 3$, $\lfloor -1.5 \rfloor = -2$, and $\lfloor 4 \rfloor = 4$).

(n) Define C on $\mathbb{R}$ via xCy if and only if $|x - y| < 1$.

6.2 Equivalence Relations

As we have seen in the previous section, the notions of reflexive, symmetric, and transitive are independent of each other. That is, a relation may have some combination of these properties, possibly none of them and possibly all of them. However, we have a special name for when a relation satisfies all three properties.

Definition 6.35. Let $\sim$ be a relation on a set A. Then $\sim$ is called an **equivalence relation** on A if and only if $\sim$ is reflexive, symmetric, and transitive.

The symbol "$\sim$" is usually pronounced as "twiddle" or "tilde" and the phrase "$a \sim b$" could be read as "a is related to b" or "a twiddles b".

Problem 6.36. Let $A = \{1, 2, 3, 4, 5, 6\}$ and define

$$R = \{(1,1), (1,6), (2,2), (2,3), (2,4), (3,3), (3,2), (3,4), (4,4), (4,2), (4,3), (5,5), (6,6), (6,1)\}.$$

Using R, complete each of the following.

(a) Draw the digraph for R.

(b) Determine whether R is an equivalence relation on A.

(c) Find $\mathrm{Rel}(R)$ by determining $\mathrm{rel}(x)$ for each $x \in A$.

Problem 6.37. Let $A = \{a, b, c, d, e\}$.

(a) Make up an equivalence relation $\sim$ on A by drawing a digraph such that a is not related to b and c is not related to b.

(b) Using your digraph, find $\mathrm{Rel}(\sim)$ by determining $\mathrm{rel}(x)$ for each $x \in A$.

Problem 6.38. Given a finite set A and an equivalence relation $\sim$ on A, describe what the corresponding digraph would have to look like.

Problem 6.39. Determine which relations given in Problem 6.34 are equivalence relations.

Problem 6.40. Let $\mathcal{T}$ be the set of all triangles and define $\sim$ on $\mathcal{T}$ via $T_1 \sim T_2$ if and only if T_1 is similar to T_2. Determine whether $\sim$ is an equivalence relation on $\mathcal{T}$.

Problem 6.41. If possible, construct an equivalence relation on the empty set. If this is not possible, explain why.

Theorem 6.42. Suppose $\sim$ is an equivalence relation on a set A and let $a, b \in A$. Then $\operatorname{rel}(a) = \operatorname{rel}(b)$ if and only if $a \sim b$.

Theorem 6.43. Suppose $\sim$ is an equivalence relation on a set A. Then

(a) $\displaystyle\bigcup_{a \in A} \operatorname{rel}(a) = A$, and

(b) For all $a, b \in A$, either $\operatorname{rel}(a) = \operatorname{rel}(b)$ or $\operatorname{rel}(a) \cap \operatorname{rel}(b) = \emptyset$.

In light of Theorem 6.43, we have the following definition.

Definition 6.44. If $\sim$ is an equivalence relation on a set A, then for each $a \in A$, we refer to $\operatorname{rel}(a)$ as the **equivalence class** of a.

When $\sim$ is an equivalence relation on a set A, it is common to write each equivalence class $\operatorname{rel}(a)$ as $\boxed{[a]}$ (or sometimes $\overline{a}$). The element a inside the square brackets is called the **representative of the equivalence class** $[a]$. Theorem 6.42 implies that an equivalence class can be represented by any element of the equivalence class. For example, in Problem 6.36, we have $[1] = [6]$ since 1 and 6 are in the same equivalence class. The collection of equivalence classes $\operatorname{Rel}(\sim)$ is often denoted by $\boxed{A/\sim}$, which is read as "A modulo $\sim$" or "A mod $\sim$". The collection $A/\sim$ is sometimes referred to as the **quotient of** A **by** $\sim$.

Example 6.45. Let P denote the residents of a particular town and define $\sim$ on P via $a \sim b$ if and only if a and b have the same last name. It is easily seen that this relation is reflexive, symmetric, and transitive, and hence $\sim$ is an equivalence relation on P. The equivalence classes correspond to collections of individuals with the same last name. For example, Maria Garcia, Anthony Garcia, and Ariana Garcia all belong to the same equivalence class. Any Garcia can be used as a representative for the corresponding equivalence class, so we can denote it as [Maria Garcia], for example. The collection $P/\sim$ consists of the various sets of people with the same last name. In particular, $[\text{Maria Garcia}] \in P/\sim$.

Example 6.46. The five distinct sets of relatives that you identified in Problem 6.22 are the equivalence classes for $\equiv_5$ on $\mathbb{Z}$. These equivalence classes are often called the **congruence classes modulo 5**.

The upshot of Theorem 6.43 is that given an equivalence relation, every element lives in exactly one equivalence class. In the next section, we will see that we can run this in reverse. That is, if we separate out the elements of a set so that every element is an element of exactly one subset, then this determines an equivalence relation.

Problem 6.47. If $\sim$ is an equivalence relation on a finite set A, describe $A/\sim$ in terms of the digraph corresponding to $\sim$.

Problem 6.48. For each of the equivalence relations you identified in Problem 6.39, succinctly describe the corresponding equivalence classes.

6.3 Partitions

Theorems 6.42 and 6.43 imply that if $\sim$ is an equivalence relation on a set A, then $\sim$ breaks A up into pairwise disjoint chunks, where each chunk is some $[a]$ for $a \in A$. As you have probably already noticed, equivalence relations are intimately related to the following concept.

Definition 6.49. A collection Ω of subsets of a set A is said to be a **partition** of A if the elements of Ω satisfy:

(a) Each $X \in \Omega$ is nonempty,

(b) For all $X, Y \in \Omega$, $X \cap Y = \emptyset$ when $X \neq Y$, and

(c) $\displaystyle\bigcup_{X \in \Omega} X = A$.

That is, the elements of Ω are pairwise disjoint nonempty sets and their union is all of A. Each $X \in \Omega$ is called a **block** of the partition.

Example 6.50. Consider the equivalence relation $\sim$ on the set P described in Example 6.45. Recall that the equivalence classes correspond to collections of individuals with the same last name. Since each equivalence class is nonempty and each resident of the town belongs to exactly one equivalence class, the collection of equivalence classes forms a partition of P. That is, $P/{\sim}$ is a partition of P, where the blocks of the partition correspond to sets of residents with the same last name.

Example 6.51. Each of the following is an example of a partition of the set given in parentheses.

(a) Democrat, Republican, Independent, Green Party, Libertarian, etc. (set of registered voters)

(b) Freshman, sophomore, junior, senior (set of high school students)

(c) Evens, odds (set of integers)

(d) Rationals, irrationals (set of real numbers)

Example 6.52. Let $A = \{a, b, c, d, e, f\}$ and $\Omega = \{\{a\}, \{b, c, d\}, \{e, f\}\}$. Since the elements of Ω are pairwise disjoint nonempty subsets of A such that their union is all of A, Ω is a partition of A consisting of three blocks.

Problem 6.53. Consider the set A from Example 6.52.

(a) Find a partition of A consisting of four blocks.

(b) Find a collection of subsets of A that does *not* form a partition. See how many ways you can prevent your collection from being a partition.

Problem 6.54. For each of the following, find a partition of $\mathbb{Z}$ with the given properties.

(a) A partition of $\mathbb{Z}$ that consists of finitely many blocks, where each of the blocks is infinite.

(b) A partition of $\mathbb{Z}$ that consists of infinitely many blocks, where each of the blocks is finite.

(c) A partition of $\mathbb{Z}$ that consists of infinitely many blocks, where each of the blocks is infinite.

Problem 6.55. For each relation in Problem 6.34, determine whether the corresponding collection of the sets of relatives forms a partition of the given set.

Problem 6.56. Can we partition the empty set? If so, describe a partition. If not, explain why.

The next theorem spells out half of the close connection between partitions and equivalence relations. Theorem 6.70 yields the other half.

Theorem 6.57. *If $\sim$ is an equivalence relation on a nonempty set A, then $A/\!\sim$ forms a partition of A.*

Problem 6.58. In the previous theorem, why did we require A to be nonempty?

Problem 6.59. Consider the equivalence relation

$$\sim = \{(1,1),(1,2),(2,1),(2,2),(3,3),(4,4),(4,5),(5,4),(5,5),(6,6),(5,6),(6,5),(4,6),(6,4)\}$$

on the set $A = \{1,2,3,4,5,6\}$. Find the partition determined by $\mathrm{Rel}(\sim)$.

It turns out that we can reverse the situation, as well. That is, given a partition, we can form an equivalence relation such that the equivalence classes correspond to the blocks of the partition. Before proving this, we need a definition.

Definition 6.60. Let A be a set and Ω any collection of subsets of A (not necessarily a partition). Define the relation $\boxed{R_\Omega}$ on A via $aR_\Omega b$ if and only if there exists $X \in \Omega$ that contains both a and b. This relation is called the **relation on A associated to Ω**.

In other words, two elements are related exactly when they are in the same subset.

Problem 6.61. Let $A = \{a,b,c,d,e,f\}$ and let $\Omega = \{\{a,c\},\{b,c\},\{d,f\}\}$. List the ordered pairs in R_Ω and draw the corresponding digraph.

Problem 6.62. Let A and Ω be as in Example 6.52. List the ordered pairs in R_Ω and draw the corresponding digraph.

Problem 6.63. Consider Problem 6.24. Find the relation on A associated to $\mathrm{Rel}(\sim)$ and compare with what you obtained for R in Problem 6.24.

Problem 6.64. Give an example of a set A and a collection Ω from $\mathcal{P}(A)$ such that the relation R_Ω is not reflexive.

Theorem 6.65. If Ω is a collection of subsets of a nonempty set A (not necessarily a partition) such that

$$\bigcup_{X\in\Omega} X = A,$$

then R_Ω is reflexive.

Problem 6.66. Is it necessary to require A to be nonempty in Theorem 6.65?

Theorem 6.67. If Ω is a collection of subsets of a set A (not necessarily a partition), then R_Ω is symmetric.

Theorem 6.68. If Ω is a collection of subsets of a set A (not necessarily a partition) such that the elements of Ω are pairwise disjoint, then R_Ω is transitive.

Problem 6.69. Why didn't we require A to be nonempty in Theorems 6.67 and 6.68?

Recall that Theorem 6.57 says that the equivalence classes for a relation on a nonempty set A determines a partition of A. The following theorem tells us that every partition of a set yields an equivalence relation where the equivalence classes correspond to the blocks of the partition. This result is a consequence of Theorems 6.65, 6.67, and 6.68.

Theorem 6.70. If Ω is a partition of a set A, then R_Ω is an equivalence relation.

Together, Theorems 6.57 and 6.70 tell us that equivalence relations and partitions are two different ways of viewing the same thing.

Corollary 6.71. If R is a relation on a nonempty set A such that the collection of the set of relatives with respect to R is a partition of A, then R is an equivalence relation.

Problem 6.72. Let $A = \{\circ, \triangle, \blacktriangle, \square, \blacksquare, \bigstar, ☺, ☹\}$. Make up a partition Ω on A and then draw the digraph corresponding to R_Ω.

6.4 Modular Arithmetic

In this section, we look at a particular family of equivalence relations on the integers and explore the way in which arithmetic interacts with them.

Definition 6.73. For each $n \in \mathbb{N}$, define $n\mathbb{Z}$ to be the set of all integers that are divisible by n. In set-builder notation, we have

$$\boxed{n\mathbb{Z} := \{m \in \mathbb{Z} \mid m = nk \text{ for some } k \in \mathbb{Z}\}}.$$

For example, $5\mathbb{Z} = \{\ldots, -10, -5, 0, 5, 10, \ldots\}$ and $2\mathbb{Z}$ is the set of even integers.

Problem 6.74. Consider the sets $3\mathbb{Z}$, $5\mathbb{Z}$, $15\mathbb{Z}$, and $20\mathbb{Z}$.

(a) List at least five elements in each of the above sets.

(b) Notice that $3\mathbb{Z} \cap 5\mathbb{Z} = n\mathbb{Z}$ for some $n \in \mathbb{N}$. What is n? Describe $15\mathbb{Z} \cap 20\mathbb{Z}$ in a similar way.

(c) Draw a Venn diagram illustrating how the sets $3\mathbb{Z}$, $5\mathbb{Z}$, and $15\mathbb{Z}$ intersect.

(d) Draw a Venn diagram illustrating how the sets $5\mathbb{Z}$, $15\mathbb{Z}$, and $20\mathbb{Z}$ intersect.

Theorem 6.75. Let $n \in \mathbb{N}$. If $a, b \in n\mathbb{Z}$, then $-a$, $a+b$, and ab are also in $n\mathbb{Z}$.

Definition 6.76. For each $n \in \mathbb{N}$, define the relation $\boxed{\equiv_n}$ on $\mathbb{Z}$ via $a \equiv_n b$ if and only if $a - b \in n\mathbb{Z}$. We read $a \equiv_n b$ as "a is congruent to b modulo n."

Note that $a - b \in n\mathbb{Z}$ if and only if n divides $a - b$, which implies that $a \equiv_n b$ if and only if n divides $a - b$.

Example 6.77. We encountered $\equiv_5$ in Problem 6.22 and discovered that there were five distinct sets of relatives. In particular, we have

$$\begin{aligned}
\text{rel}(0) &= \{\ldots, -10, -5, 0, 5, 10, \ldots\} \\
\text{rel}(1) &= \{\ldots, -9, -4, 1, 6, 11, \ldots\} \\
\text{rel}(2) &= \{\ldots, -8, -3, 2, 7, 12, \ldots\} \\
\text{rel}(3) &= \{\ldots, -7, -2, 3, 8, 13, \ldots\} \\
\text{rel}(4) &= \{\ldots, -6, -1, 4, 9, 14, \ldots\}.
\end{aligned}$$

Notice that this collection forms a partition of $\mathbb{Z}$. By Corollary 6.71, the relation $\equiv_5$ must be an equivalence relation.

The previous example generalizes as expected. You can prove the following theorem by either proving that $\equiv_n$ is reflexive, symmetric, and transitive or by utilizing Corollary 6.71.

Theorem 6.78. For $n \in \mathbb{N}$, the relation $\equiv_n$ is an equivalence relation on $\mathbb{Z}$.

We have have special notation and terminology for the equivalence classes that correspond to $\equiv_n$.

Definition 6.79. For $n \in \mathbb{N}$, let $\boxed{[a]_n}$ denote the equivalence class of a with respect to $\equiv_n$ (see Definitions 6.17 and 6.44). The equivalence class $[a]_n$ is called the **congruence** (or **residue**) **class of** a **modulo** n. The collection of all equivalence classes determined by $\equiv_n$ is denoted $\boxed{\mathbb{Z}/n\mathbb{Z}}$, which is read "$\mathbb{Z}$ modulo $n\mathbb{Z}$".

Example 6.80. Let's compute $[2]_7$. Tracing back through the definitions, we see that

$$\begin{aligned}
m \in [2]_7 &\iff m \equiv_7 2 \\
&\iff m - 2 \in 7\mathbb{Z} \\
&\iff m - 2 = 7k \text{ for some } k \in \mathbb{Z} \\
&\iff m = 7k + 2 \text{ for some } k \in \mathbb{Z}.
\end{aligned}$$

Since the multiples of 7 are $7\mathbb{Z} = \{\ldots, -14, -7, 0, 7, 14, \ldots\}$, we can find $[2]_7$ by adding 2 to each element of $7\mathbb{Z}$ to get $[2]_7 = \{\ldots, -12, -5, 2, 9, 16, \ldots\}$.

Problem 6.81. For each of the following congruence classes, find five elements in the set such that at least one is greater than 70 and one is less than 70.

(a) $[4]_7$

(b) $[-3]_7$

(c) $[7]_7$

Problem 6.82. Describe $[0]_3$, $[1]_3$, $[2]_3$, $[4]_3$, and $[-2]_3$ as lists of elements as in Example 6.80. How many distinct congruence classes are in $\mathbb{Z}/3\mathbb{Z}$? Theorem 6.43 might be helpful.

Consider using Theorem 6.42 to prove the next theorem.

Theorem 6.83. For $n \in \mathbb{N}$ and $a, b \in \mathbb{Z}$, $[a]_n = [b]_n$ if and only if n divides $a - b$.

Corollary 6.84. For $n \in \mathbb{N}$ and $a \in \mathbb{Z}$, $[a]_n = [0]_n$ if and only if n divides a.

The next result provides a useful characterization for when two congruence classes are equal. The Division Algorithm will be useful when proving this theorem.

Theorem 6.85. For $n \in \mathbb{N}$ and $a, b \in \mathbb{Z}$, $[a]_n = [b]_n$ if and only if a and b have the same remainder when divided by n.

Theorem 6.86. Let $n \in \mathbb{N}$ and let $a_1, a_2, b_1, b_2 \in \mathbb{Z}$. If $[a_1]_n = [a_2]_n$ and $[b_1]_n = [b_2]_n$, then

(a) $[a_1 + b_1]_n = [a_2 + b_2]_n$, and

(b) $[a_1 \cdot b_1]_n = [a_2 \cdot b_2]_n$.[1]

The previous theorem allows us to define addition and multiplication in $\mathbb{Z}/n\mathbb{Z}$.

Definition 6.87. Let $n \in \mathbb{N}$. We define the sum and product of congruence classes in $\mathbb{Z}/n\mathbb{Z}$ via

$$[a]_n + [b]_n := [a + b]_n \quad \text{and} \quad [a]_n \cdot [b]_n := [a \cdot b]_n.$$

Example 6.88. By Definition 6.87, $[2]_7 + [6]_7 = [2+6]_7 = [8]_7$. By Theorem 6.83, $[8]_7 = [1]_7$, and so $[2]_7 + [6]_7 = [1]_7$. Similarly, $[2]_7 \cdot [6]_7 = [2 \cdot 6]_7 = [12]_7 = [5]_7$.

Addition and multiplication for $\mathbb{Z}/n\mathbb{Z}$ has many familiar—and some not so familiar—properties. For example, addition and multiplication of congruence classes are both associative and commutative. However, it is possible for $[a]_n \cdot [b]_n = [0]_n$ even when $[a]_n \neq [0]_n$ and $[b]_n \neq [0]_n$.

Theorem 6.89. If $n \in \mathbb{N}$, then addition in $\mathbb{Z}/n\mathbb{Z}$ is commutative and associative. That is, for all $[a]_n, [b]_n, [c]_n \in \mathbb{Z}/n\mathbb{Z}$, we have

(a) $[a]_n + [b]_n = [b]_n + [a]_n$, and

[1] *Hint:* For part (a), make use of Theorem 6.83. For part (b), note that $a_1 b_1 - a_2 b_2 = a_1 b_1 - a_2 b_1 + a_2 b_1 - a_2 b_2$.

(b) $([a]_n + [b]_n) + [c]_n = [a]_n + ([b]_n + [c]_n)$.

Theorem 6.90. If $n \in \mathbb{N}$, then multiplication in $\mathbb{Z}/n\mathbb{Z}$ is commutative and associative. That is, for all $[a]_n, [b]_n, [c]_n \in \mathbb{Z}/n\mathbb{Z}$, we have

(a) $[a]_n \cdot [b]_n = [b]_n \cdot [a]_n$, and

(b) $([a]_n \cdot [b]_n) \cdot [c]_n = [a]_n \cdot ([b]_n \cdot [c]_n)$.

One consequence of Theorems 6.89(b) and 6.90(b) is that parentheses are not needed when adding or multiplying congruence classes. The next theorem follows from Definition 6.87 together with Theorems 6.89(b) and 6.90(b) and induction on k.

Theorem 6.91. Let $n \in \mathbb{N}$. For all $k \in \mathbb{N}$, if $[a_1]_n, [a_2]_n, \ldots, [a_k]_n \in \mathbb{Z}/n\mathbb{Z}$, then

(a) $[a_1]_n + [a_2]_n + \cdots + [a_k]_n = [a_1 + a_2 + \cdots + a_k]_n$, and

(b) $[a_1]_n[a_2]_n \cdots [a_k]_n = [a_1 a_2 \cdots a_k]_n$.

The next result is a special case of Theorem 6.91(b).

Corollary 6.92. Let $n \in \mathbb{N}$. If $a \in \mathbb{Z}$ and $k \in \mathbb{N}$, then $([a]_n)^k = [a^k]_n$

Example 6.93. Let's compute $[8^{179}]_7$. We see that

$$\begin{aligned}
[8^{179}]_7 &= ([8]_7)^{179} && \text{(Corollary 6.92)}\\
&= ([1]_7)^{179} && \text{(Theorem 6.83)}\\
&= [1^{179}]_7 && \text{(Corollary 6.92)}\\
&= [1]_7.
\end{aligned}$$

Problem 6.94. For each of the following, find a number a with $0 \leq a \leq 6$ such that the given quantity is equal to $[a]_7$.[2]

(a) $[6^{179}]_7$

(b) $[2^{300}]_7$

(c) $[2^{301} + 5]_7$

Problem 6.95. Find a and b such that $[a]_6 \cdot [b]_6 = [0]_6$ but $[a]_6 \neq [0]_6$ and $[b]_6 \neq [0]_6$.

Theorem 6.96. If $n \in \mathbb{N}$ such that n is not prime, then there exists $[a]_n, [b]_n \in \mathbb{Z}/n\mathbb{Z}$ such that $[a]_n \cdot [b]_n = [0]_n$ while $[a]_n \neq [0]_n$ and $[b]_n \neq [0]_n$.

Problem 6.97. Notice that $2x = 1$ has no solution in $\mathbb{Z}$. Show that $[2]_7[x]_7 = [1]_7$ does have a solution with x in $\mathbb{Z}$. What about $[14]_7[x]_7 = [1]_7$?

Make use of Theorem 6.91, Corollary 6.92, and Theorem 6.83 to prove the following theorem.

[2] *Hint:* For part (a), use the fact that $[6]_7 = [-1]_7$. For part (b), use the fact that $[2^3]_7 = [1]_7$.

Theorem 6.98. If $m \in \mathbb{N}$ such that

$$m = a_k 10^k + a_{k-1} 10^{k-1} + \cdots + a_1 10 + a_0,$$

where $a_k, a_{k-1}, \ldots, a_1, a_0 \in \{0, 1, \ldots, 9\}$ (i.e., $a_k, a_{k-1}, \ldots, a_1, a_0$ are the digits of m), then

$$[m]_3 = [a_k + a_{k-1} + \cdots + a_1 + a_0]_3.$$

You likely recognize the next result. Its proof follows quickly from Corollary 6.84 together with the previous theorem.

Theorem 6.99. An integer is divisible by 3 if and only if the sum of its digits is divisible by 3.

For the final problem of this chapter, let's revisit Theorem 4.20, which we originally proved by induction.

Problem 6.100. Use Corollary 6.84 to prove that for all integers $n \geq 0$, $3^{2n} - 1$ is divisible by 8. You will need to handle the case involving $n = 0$ separately.

Chapter 7

Functions

7.1 Introduction to Functions

In this section, we will introduce the concept of function as a special type of relation. Our definition should agree with any previous definition of function that you may have learned.

Up until this point, you may have only encountered functions as an algebraic rule, e.g., $f(x) = x^2 - 1$, for transforming one real number into another. However, we can study functions in a much broader context. The basic building blocks of a function are a first set and a second set, say X and Y, and a "correspondence" that assigns *every* element of X to *exactly one* element of Y. Let's take a look at the actual definition.

Definition 7.1. Let X and Y be two nonempty sets. A **function** f **from** X **to** Y is a relation from X to Y such that for every $x \in X$, there exists a unique $y \in Y$ such that $(x, y) \in f$. The set X is called the **domain** of f and is denoted by $\boxed{\mathrm{Dom}(f)}$. The set Y is called the **codomain** of f and is denoted by $\boxed{\mathrm{Codom}(f)}$ while the subset of the codomain defined via

$$\boxed{\mathrm{Rng}(f) := \{y \in Y \mid \text{there exists } x \text{ such that } (x, y) \in f\}}$$

is called the **range** of f or the **image of** X under f.

There is a variety of notation and terminology associated to functions. We will write $\boxed{f : X \to Y}$ to indicate that f is a function from X to Y. We will make use of statements such as "Let $f : X \to Y$ be the function defined via..." or "Define $f : X \to Y$ via...", where f is understood to be a function in the second statement. Sometimes the word **mapping** (or **map**) is used in place of the word function. If $(a, b) \in f$ for a function f, we often write $\boxed{f(a) = b}$ and say that "f maps a to b" or "f of a equals b". In this case, a may be called an **input** of f and is the **preimage** of b under f while b is called an **output** of f and is the **image** of a under f. Note that the domain of a function is the set of inputs while the range is the set of outputs for the function.

According to our definition, if $f : X \to Y$ is a function, then every element of the domain is utilized exactly once. However, there are no restrictions on whether an element of the codomain ever appears in the second coordinate of an ordered pair in the relation.

Yet if an element of Y is in the range of f, it may appear in more than one ordered pair in the relation.

It follows immediately from the definition of function that two functions are equal if and only if they have the same domain, same codomain, and the same set of ordered pairs in the relation. That is, functions f and g are equal if and only if $\mathrm{Dom}(f) = \mathrm{Dom}(g)$, $\mathrm{Codom}(f) = \mathrm{Codom}(g)$, and $f(x) = g(x)$ for all $x \in X$.

Since functions are special types of relations, we can represent them using digraphs and graphs when practical. Digraphs for functions are often called **function** (or **mapping**) **diagrams**. When drawing function diagrams, it is standard practice to put the vertices for the domain on the left and the vertices for the codomain on the right, so that all directed edges point from left to right. We may also draw an additional arrow labeled by the name of the function from the domain to the codomain.

Example 7.2. Let $X = \{a,b,c,d\}$ to $Y = \{1,2,3,4\}$ and define the relation f from X to Y via

$$f = \{(a,2),(b,4),(c,4),(d,1)\}.$$

Since each element X appears exactly once as a first coordinate, f is a function with domain X and codomain Y (i.e., $f : X \to Y$). In this case, we see that $\mathrm{Rng}(f) = \{1,2,4\}$. Moreover, we can write things like $f(a) = 2$ and $c \mapsto 4$, and say things like "f maps b to 4" and "the image of d is 1." The function diagram for f is depicted in Figure 7.1.

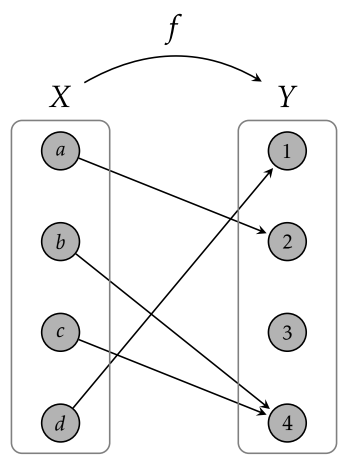

Figure 7.1: Function diagram for a function from $X = \{a,b,c,d,\}$ to $Y = \{1,2,3,4\}$.

Problem 7.3. Determine whether each of the relations defined in the following examples and problems is a function.

(a) Example 6.3 (see Figure 6.1)

(b) Example 6.14 (see Figure 6.3)

(c) Problem 6.15

(d) Problem 6.21

Problem 7.4. Let $X = \{\circ, \Box, \triangle, ☺\}$ and $Y = \{a, b, c, d, e\}$. For each of the following relations, draw the corresponding digraph and determine whether the relation represents a function from X to Y, Y to X, X to X, or does not represent a function. If the relation is a function, determine the domain, codomain, and range.

(a) $f = \{(\circ, a), (\Box, b), (\triangle, c), (☺, d)\}$

(b) $g = \{(\circ, a), (\Box, b), (\triangle, c), (☺, c)\}$

(c) $h = \{(\circ, a), (\Box, b), (\triangle, c), (\circ, d)\}$

(d) $k = \{(\circ, a), (\Box, b), (\triangle, c), (☺, d), (\Box, e)\}$

(e) $l = \{(\circ, e), (\Box, e), (\triangle, e), (☺, e)\}$

(f) $m = \{(\circ, a), (\triangle, b), (☺, c)\}$

(g) $i = \{(\circ, \circ), (\Box, \Box), (\triangle, \triangle), (☺, ☺)\}$

(h) Define the relation happy from Y to X via $(y, ☺) \in \text{happy}$ for all $y \in Y$.

(i) $\text{nugget} = \{(\circ, \circ), (\Box, \Box), (\triangle, \triangle), (☺, \Box)\}$

The last two parts of the previous problem make it clear that functions may have names consisting of more than one letter. The function names sin, cos, log, and ln are instances of this that you have likely encountered in your previous experience in mathematics. One thing that you may have never noticed is the type of font that we use for function names. It is common to italicize generic function names like f but not common function names like sin. However, we always italicize the variables used to represent the input and output for a function. For example, consider the font types used in the expressions $\sin(x)$ and $\ln(a)$.

Problem 7.5. What properties does the digraph for a relation from X to Y need to have in order for it to represent a function?

Problem 7.6. In high school I am sure that you were told that a graph represents a function if it passes the **vertical line test**. Carefully state what the vertical line test says and then explain why it works.

Sometimes we can define a function using a formula. For example, we can write $f(x) = x^2 - 1$ to mean that each x in the domain of f maps to $x^2 - 1$ in the codomain. However, notice that providing only a formula is ambiguous! A function is determined by its domain, codomain, and the correspondence between these two sets. If we only provide a description for the correspondence, it is not clear what the domain and codomain are. Two functions that are defined by the same formula, but have different domains or codomains are *not* equal.

Example 7.7. The function $f:\mathbb{R}\to\mathbb{R}$ defined via $f(x)=x^2-1$ is not equal to the function $g:\mathbb{N}\to\mathbb{R}$ defined by $g(x)=x^2-1$ since the two functions do not have the same domain.

Sometimes we rely on context to interpret the domain and codomain. For example, in a calculus class, when we describe a function in terms of a formula, we are implicitly assuming that the domain is the largest allowable subset of $\mathbb{R}$—sometimes called the **default domain**—that makes sense for the given formula while the codomain is $\mathbb{R}$.

Example 7.8. If we write $f(x)=x^2-1$, $g(x)=\sqrt{x}$, and $h(x)=\frac{1}{x}$ without mentioning the domains, we would typically interpret these as the functions $f:\mathbb{R}\to\mathbb{R}$, $g:[0,\infty)\to\mathbb{R}$, and $h:\mathbb{R}\setminus\{0\}\to\mathbb{R}$ that are determined by their respective formulas.

Problem 7.9. Provide an example of each of the following. You may draw a function diagram, write down a list of ordered pairs, or a write a formula as long as the domain and codomain are clear.

(a) A function f from a set with 4 elements to a set with 3 elements such that $\mathrm{Rng}(f)=\mathrm{Codom}(f)$.

(b) A function g from a set with 4 elements to a set with 3 elements such that $\mathrm{Rng}(g)$ is strictly smaller than $\mathrm{Codom}(g)$.

Problem 7.10. Let $f:X\to Y$ be a function and suppose that X and Y are finite sets with n and m elements, respectively, such that $n<m$. Is it possible for $\mathrm{Rng}(f)=\mathrm{Codom}(f)$? If so, provide an example. If this is not possible, explain why.

There are a few special functions that we should know the names of.

Definition 7.11. If X and Y are nonempty sets such that $X\subseteq Y$, then the function $\iota:X\to Y$ defined via $\iota(x)=x$ is called the **inclusion map from X into Y**.

Note that "ι" is the Greek letter "iota".

Problem 7.12. Let $X=\{a,b,c\}$ and $Y=\{a,b,c,d\}$. Draw the function diagram of the inclusion map from X into Y.

If the domain and codomain are equal, the inclusion map has a special name.

Definition 7.13. If X is a nonempty set, then the function $i_X:X\to X$ defined via $i_X(x)=x$ is called the **identity map** (or **identity function**) **on** X.

Example 7.14. The relation defined in Problem 7.4(g) is the identity map on $X=\{\circ,\square,\triangle,☺\}$.

Problem 7.15. Draw a portion of the graph of the identity map on $\mathbb{R}$ as a subset of $\mathbb{R}^2$.

Definition 7.16. Any function $f:X\to Y$ defined via $f(x)=c$ for a fixed $c\in Y$ is called a **constant function**.

Example 7.17. The function defined in Problem 7.4(h) is an example of a constant function. Notice that we can succinctly describe this function using the formula $\mathrm{happy}(y)=☺$.

Definition 7.18. A **piecewise-defined function** (or **piecewise function**) is a function defined by specifying its output on a partition of the domain.

Note that "piecewise" is a way of expressing the function, rather than a property of the function itself.

Example 7.19. We can express the function in Problem 7.4(i) as a piecewise function using the formula

$$\text{nugget}(x) = \begin{cases} x, & \text{if } x \text{ is a geometric shape,} \\ \square, & \text{otherwise.} \end{cases}$$

Example 7.20. The function $f : \mathbb{R} \to \mathbb{R}$ defined via

$$f(x) = \begin{cases} x^2 - 1, & \text{if } x \geq 0, \\ 17, & \text{if } -2 \leq x < 0, \\ -x, & \text{if } x < -2 \end{cases}$$

is an example of a piecewise-defined function.

Problem 7.21. Define $f : \mathbb{R} \setminus \{0\} \to \mathbb{R}$ via $f(x) = \frac{|x|}{x}$. Express f as a piecewise function.

It is important to point out that not every function can be described using a formula! Despite your prior experience, functions that can be represented succinctly using a formula are rare.

The next problem illustrates that some care must be taken when attempting to define a function.

Problem 7.22. For each of the following, explain why the given description does not define a function.

(a) Define $f : \{1,2,3\} \to \{1,2,3\}$ via $f(a) = a - 1$.

(b) Define $g : \mathbb{N} \to \mathbb{Q}$ via $g(n) = \frac{n}{n-1}$.

(c) Let $A_1 = \{1,2,3\}$ and $A_2 = \{3,4,5\}$. Define $h : A_1 \cup A_2 \to \{1,2\}$ via

$$h(x) = \begin{cases} 1, & \text{if } x \in A_1 \\ 2, & \text{if } x \in A_2. \end{cases}$$

(d) Define $s : \mathbb{Q} \to \mathbb{Z}$ via $s(a/b) = a + b$.

In mathematics, we say that an expression is **well defined** (or **unambiguous**) if its definition yields a unique interpretation. Otherwise, we say that the expression is not well defined (or is **ambiguous**). For example, if $a, b, c \in \mathbb{R}$, then the expression abc is well defined since it does not matter if we interpret this as $(ab)c$ or $a(bc)$ since the real numbers are associative under multiplication. This issue was lurking behind the scenes in the statement of Theorem 6.91. In particular, the expressions

$$[a_1]_n + [a_2]_n + \cdots + [a_k]_n$$

and
$$[a_1]_n[a_2]_n\cdots[a_k]_n$$
are well defined in $\mathbb{Z}/n\mathbb{Z}$ in light of Theorems 6.89(b) and 6.90(b).

When we attempt to define a function, it may not be clear without doing some work that our definition really does yield a function. If there is some potential ambiguity in the definition of a function that ends up not causing any issues, we say that the function is well defined. However, this phrase is a bit of misnomer since all functions are well defined. The issue of whether a description for a proposed function is well defined often arises when defining things in terms of representatives of equivalence classes, or more generally in terms of how an element of the domain is written. For example, the descriptions given in parts (c) and (d) of Problem 7.22 are not well defined. To show that a potentially ambiguous description for a function $f : X \to Y$ is well defined prove that if a and b are two representations for the same element in X, then $f(a) = f(b)$.

Problem 7.23. For each of the following, determine whether the description determines a well-defined function.

(a) Define $f : \mathbb{Z}/5\mathbb{Z} \to \mathbb{N}$ via
$$f([a]_5) = \begin{cases} 0, & \text{if } a \text{ is even} \\ 1, & \text{if } a \text{ is odd.} \end{cases}$$

(b) Define $g : \mathbb{Z}/6\mathbb{Z} \to \mathbb{N}$ via
$$g([a]_6) = \begin{cases} 0, & \text{if } a \text{ is even} \\ 1, & \text{if } a \text{ is odd.} \end{cases}$$

(c) Define $m : \mathbb{Z}/8\mathbb{Z} \to \mathbb{Z}/10\mathbb{Z}$ via $m([x]_8) = [6x]_{10}$.

(d) Define $h : \mathbb{Z}/10\mathbb{Z} \to \mathbb{Z}/10\mathbb{Z}$ via $h([x]_{10}) = [6x]_{10}$.

(e) Define $k : \mathbb{Z}/43\mathbb{Z} \to \mathbb{Z}/43\mathbb{Z}$ via $k([x]_{43}) = [11x - 5]_{43}$.

(f) Define $\ell : \mathbb{Z}/15\mathbb{Z} \to \mathbb{Z}/15\mathbb{Z}$ via $\ell([x]_{15}) = [5x - 11]_{15}$.

Problem 7.24. Let $k, n \in \mathbb{N}$ and $m \in \mathbb{Z}$. Under what conditions will $f_m : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/k\mathbb{Z}$ given by $f_m([x]_n) = [mx]_k$ be a well-defined function? Prove your claim.

7.2 Injective and Surjective Functions

We now turn our attention to some important properties that a function may or may not possess. Recall that if f is a function, then every element in its domain is mapped to a unique element in the range. However, there are no restrictions on whether more than one element of the domain is mapped to the same element in the range. If each element in the range has a unique element in the domain mapping to it, then we say that the function is injective. Moreover, the range of a function is not required to be all of the codomain. If every element of the codomain has at least one element in the domain that maps to it, then we say that the function is surjective. Let's make these definitions a bit more precise.

Definition 7.25. Let $f : X \to Y$ be a function.

(a) The function f is said to be **injective** (or **one-to-one**) if for all $y \in \mathrm{Rng}(f)$, there is a unique $x \in X$ such that $y = f(x)$.

(b) The function f is said to be **surjective** (or **onto**) if for all $y \in Y$, there exists $x \in X$ such that $y = f(x)$.

(c) If f is both injective and surjective, we say that f is **bijective**.

Problem 7.26. Compare and contrast the following statements. Do they mean the same thing?

(a) For all $x \in X$, there exists a unique $y \in Y$ such that $f(x) = y$.

(b) For all $y \in \mathrm{Rng}(f)$, there is a unique $x \in X$ such that $y = f(x)$.

Problem 7.27. Assume that X and Y are finite sets. Provide an example of each of the following. You may draw a function diagram, write down a list of ordered pairs, or a write a formula as long as the domain and codomain are clear.

(a) A function $f : X \to Y$ that is injective but not surjective.

(b) A function $f : X \to Y$ that is surjective but not injective.

(c) A function $f : X \to Y$ that is a bijection.

(d) A function $f : X \to Y$ that is neither injective nor surjective.

Problem 7.28. Provide an example of each of the following. You may either draw a graph or write down a formula. Make sure you have the correct domain.

(a) A function $f : \mathbb{R} \to \mathbb{R}$ that is injective but not surjective.

(b) A function $f : \mathbb{R} \to \mathbb{R}$ that is surjective but not injective.

(c) A function $f : \mathbb{R} \to \mathbb{R}$ that is a bijection.

(d) A function $f : \mathbb{R} \to \mathbb{R}$ that is neither injective nor surjective.

(e) A function $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ that is injective.

Problem 7.29. Suppose $X \subseteq \mathbb{R}$ and $f : X \to \mathbb{R}$ is a function. Fill in the blank with the appropriate word.

> The function $f : X \to \mathbb{R}$ is _________ if and only if every horizontal line hits the graph of f *at most once*.

This statement is often called the **horizontal line test**. Explain why the horizontal line test is true.

Problem 7.30. Suppose $X \subseteq \mathbb{R}$ and $f : X \to \mathbb{R}$ is a function. Fill in the blank with the appropriate word.

> The function $f : X \to \mathbb{R}$ is _________ if and only if every horizontal line hits the graph of f *at least once*.

Explain why this statement is true.

Problem 7.31. Suppose $X \subseteq \mathbb{R}$ and $f : X \to \mathbb{R}$ is a function. Fill in the blank with the appropriate word.

> The function $f : X \to \mathbb{R}$ is _________ if and only if every horizontal line hits the graph of f *exactly once*.

Explain why this statement is true.

How do we prove that a function f is injective? We would need to show that every element in the range has a unique element from the domain that maps to it. First, notice that each element in the range can be written as $f(x)$ for at least one x in the domain. To argue that each such element in domain is unique, we can suppose $f(x_1) = f(x_2)$ for arbitrary x_1 and x_2 in the domain and then work to show that $x_1 = x_2$. It is important to point out that when we suppose $f(x_1) = f(x_2)$ for some x_1 and x_2, we are not assuming that x_1 and x_2 are different. In general, when we write "Let $x_1, x_2 \in X \ldots$", we are leaving open the possibility that x_1 and x_2 are actually the same element. One could approach proving that a function is injective by utilizing a proof by contradiction, but this is not usually necessary.

Skeleton Proof 7.32 (Proof that a function is injective)**.** Here is the general structure for proving that a function is injective.

> *Proof.* Assume $f : X \to Y$ is a function defined by (or satisfying)... *[Use the given definition (or describe the given property) of f].* Let $x_1, x_2 \in X$ and suppose $f(x_1) = f(x_2)$.
>
> ... *[Use the definition (or property) of f to verify that $x_1 = x_2$]* ...
>
> Therefore, the function f is injective. □

How do we prove that a function f is surjective? We would need to argue that every element in the codomain is also in the range. Sometimes, the proof that a particular function is surjective is extremely short, so don't second guess yourself if you find yourself in this situation.

Skeleton Proof 7.33 (Proof that a function is surjective)**.** Here is the general structure for proving that a function is surjective.

> *Proof.* Assume $f : X \to Y$ is a function defined by (or satisfying)...*[Use the given definition (or describe the given property) of f]*. Let $y \in Y$.
>
> ... *[Use the definition (or property) of f to find some $x \in X$ such that $f(x) = y$]* ...
>
> Therefore, the function f is surjective. □

Problem 7.34. Determine whether each of the following functions is injective, surjective, both, or neither. In each case, you should provide a proof or a counterexample as appropriate.

(a) Define $f : \mathbb{R} \to \mathbb{R}$ via $f(x) = x^2$

(b) Define $g : \mathbb{R} \to [0, \infty)$ via $g(x) = x^2$

(c) Define $h : \mathbb{R} \to \mathbb{R}$ via $h(x) = x^3$

(d) Define $k : \mathbb{R} \to \mathbb{R}$ via $k(x) = x^3 - x$

(e) Define $c : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ via $c(x, y) = x^2 + y^2$

(f) Define $f : \mathbb{N} \to \mathbb{N} \times \mathbb{N}$ via $f(n) = (n, n)$

(g) Define $g : \mathbb{Z} \to \mathbb{Z}$ via

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

(h) Define $\ell : \mathbb{Z} \to \mathbb{N}$ via

$$\ell(n) = \begin{cases} 2n + 1, & \text{if } n \geq 0 \\ -2n, & \text{if } n < 0 \end{cases}$$

(i) The function h defined in Problem 7.23(d).

(j) The function k defined in Problem 7.23(e).

(k) The function ℓ defined in Problem 7.23(f).

Problem 7.35. Suppose X and Y are nonempty sets with m and n elements, respectively, where $m \leq n$. How many injections are there from X to Y?

Problem 7.36. Compare and contrast the definition of "function" with the definition of "injective function". Consider the vertical line test and horizontal line test in your discussion. Moreover, attempt to capture what it means for a relation to not be a function and for a function to not be an injection by drawing portions of a digraph.

The next two theorems should not come as as surprise.

Theorem 7.37. The inclusion map $\iota : X \to Y$ for $X \subseteq Y$ is an injection.

Theorem 7.38. The identity function $i_X : X \to X$ is a bijection.

Problem 7.39. Let A and B be nonempty sets and let S be a nonempty subset of $A \times B$. Define $\pi_1 : S \to A$ and $\pi_2 : S \to B$ via $\pi_1(a,b) = a$ and $\pi_2(a,b) = b$. We call π_1 and π_2 the **projections** of S onto A and B, respectively.

(a) Provide examples to show that π_1 does not need to be injective nor surjective.

(b) Suppose that S is also a function. Is π_1 injective? Is π_1 surjective? How about π_2?

The next theorem says that if we have an equivalence relation on a nonempty set, the mapping that assigns each element to its respective equivalence class is a surjective function.

Theorem 7.40. If $\sim$ is an equivalence relation on a nonempty set A, then the function $f : A \to A/\!\sim$ defined via $f(x) = [x]$ is a surjection.

The function from the previous theorem is sometimes called the **canonical projection map** induced by $\sim$.

Problem 7.41. Under what circumstances would the function from the previous theorem also be injective?

Let's explore whether we can weaken the hypotheses of Theorem 7.40.

Problem 7.42. Let R be a relation on a nonempty set A.

(a) What conditions on R must hold in order for $f : A \to \mathrm{Rel}(R)$ defined via $f(a) = \mathrm{rel}(a)$ to be a function?

(b) What additional conditions, if any, must hold on R in order for f to be a surjective function?

Problem 7.43. Let A be a nonempty set.

(a) Suppose R is an equivalence relation on A. Under what conditions is R a function from A to A?

(b) Suppose $f : A \to A$ is a function. Under what conditions is f an equivalence relation on A?

Given any function, we can define an equivalence relation on its domain, where the equivalence classes correspond to the elements that map to the same element of the range.

Theorem 7.44. Let $f : X \to Y$ be a function and define $\sim$ on X via $a \sim b$ if and only if $f(a) = f(b)$. Then $\sim$ is an equivalence relation on X.

It follows immediately from Theorem 6.57 that the equivalence classes induced by the equivalence relation in Theorem 7.44 partition the domain of a function.

Problem 7.45. For each of the following, identify the equivalence classes induced by the relation from Theorem 7.44 for the given function.

(a) The function f defined in Example 7.2.

(b) The function c defined in Problem 7.34(e).

If f is a function, the equivalence relation in Theorem 7.44 allows us to construct a bijective function whose domain is the set of equivalence classes and whose codomain coincides with the range of f. This is an important idea that manifests itself in many areas of mathematics. One such instance is the First Isomorphism Theorem for Groups, which is a fundamental theorem in a branch of mathematics called group theory. When proving the following theorem, the first thing you should do is verify that the description for $\overline{f}$ is well defined.

Theorem 7.46. Let $f : X \to Y$ be a function and define $\sim$ on X as in Theorem 7.44. Then the function $\overline{f} : X/{\sim} \to \operatorname{Rng}(f)$ defined via $\overline{f}([a]) = f(a)$ is a bijection.

Here is an analogy for helping understand the content of Theorem 7.46. Suppose we have a collection airplanes filled with passengers and a collection of potential destination cities such that at most one airplane may land at each city. The function f indicates which city each passenger lands at while the function $\overline{f}$ indicates which city each airplane lands at. Moreover, the codomain for the function $\overline{f}$ consists only of the cities that an airplane lands at.

Example 7.47. Let $X = \{a, b, c, d, e, f\}$ and $Y = \{1, 2, 3, 4, 5\}$ and define $\varphi : X \to Y$ via

$$\varphi = \{(a,1),(b,1),(c,2),(d,4),(e,4),(f,4)\}.$$

The function diagram for φ is given in Figure 7.2(a), where we have highlighted the elements of the domain that map to the same element in the range by enclosing them in additional boxes. We see that $\operatorname{Rng}(\varphi) = \{1, 2, 4\}$. The function diagram for the induced map $\overline{\varphi}$ that is depicted in Figure 7.2(b) makes it clear that $\overline{\varphi}$ is a bijection. Note that since $\varphi(a) = \varphi(b)$ and $\varphi(d) = \varphi(e) = \varphi(f)$, it must be the case that $[a] = [b]$ and $[d] = [e] = [f]$ according to Theorem 6.42. Thus, the vertices labeled as $[a]$ and $[d]$ in Figure 7.2(b) could have also been labeled as $[b]$ and $[c]$ or $[d]$, respectively. In terms of our passengers and airplanes analogy, $X = \{a, b, c, d, e, f\}$ is the set of passengers, $Y = \{1, 2, 3, 4, 5\}$ is the set of potential destination cities, $X/{\sim} = \{[a], [c], [d]\}$ is the set of airplanes, and $\operatorname{Rng}(\varphi) = \{1, 2, 4\}$ is the set of cities that airplanes land at. The equivalence class $[a]$ is the airplane containing the passenger a, and since a and b are on the same plane, $[b]$ is also the plane containing the passenger a.

Problem 7.48. Consider the equivalence classes you identified in parts (a) and (b) of Problem 7.45.

(a) Draw the function diagram for the function $\overline{f}$ as defined in Theorem 7.46, where f is the function defined in Example 7.2.

(b) Describe the function $\overline{c}$ as defined in Theorem 7.46, where c is the function defined in Problem 7.34(e).

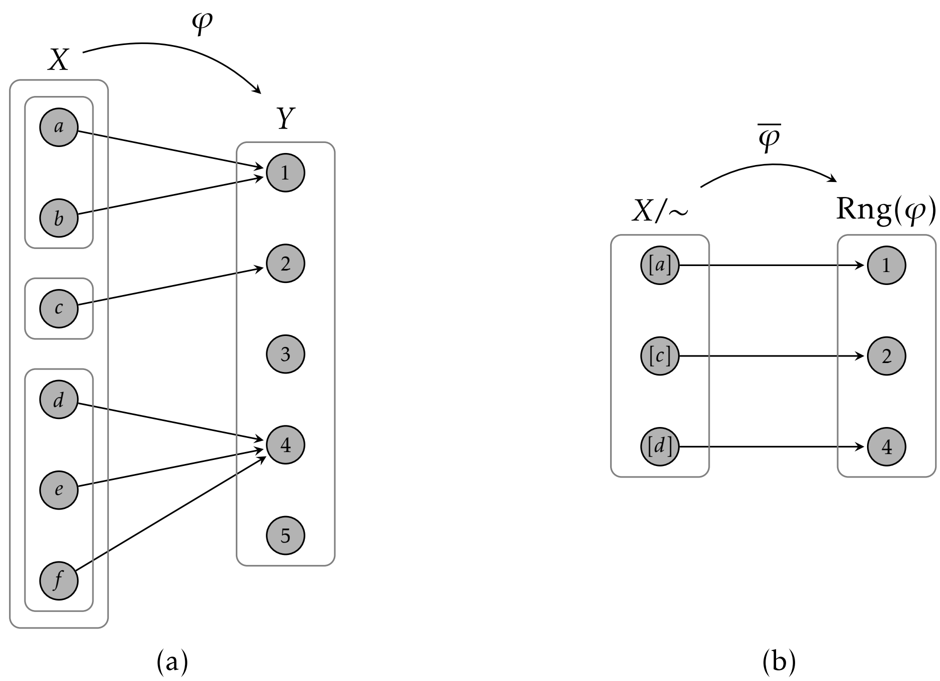

Figure 7.2: Example of a visual representation of Theorem 7.46.

While perhaps not surprising, Problem 7.48(b) tells us that there is a one-to-one correspondence between circles centered at the origin and real numbers.

Problem 7.49. Let $Y = \{0, 1, 2, 3\}$ and define the function $f : \mathbb{Z} \to Y$ such that $f(n)$ equals the unique remainder obtained after dividing n by 4. For example, $f(11) = 3$ since $11 = 4 \cdot 2 + 3$ according to the Division Algorithm (Theorem 5.5). This function is sometimes written as $f(n) = n \pmod 4$, where it is understood that we restrict the output to $\{0, 1, 2, 3\}$. It is clear that f is surjective since 0, 1, 2, and 3 are mapped to 0, 1, 2, and 3, respectively. Figure 7.3 depicts a portion of the function diagram for f, where we have drawn the diagram from the top down instead of left to right.

(a) Describe the equivalence classes induced by the relation given in Theorem 7.44.

(b) What familiar set is $\mathbb{Z}/\sim$ equal to?

(c) Draw the function diagram for the function $\overline{f}$ as defined in Theorem 7.46.

(d) The function diagram in Figure 7.3 is a bit hard to interpret due to the ordering of the elements in the domain. Can you find a better way to lay out the vertices in the domain that makes the function f easier to interpret?

Problem 7.50. Consider the function h defined in Problem 7.23(d).

(a) Draw the function diagram for h.

(b) Identify the equivalence classes induced by the relation given in Theorem 7.44.

(c) Draw the function diagram for the function $\overline{h}$ as defined in Theorem 7.46.

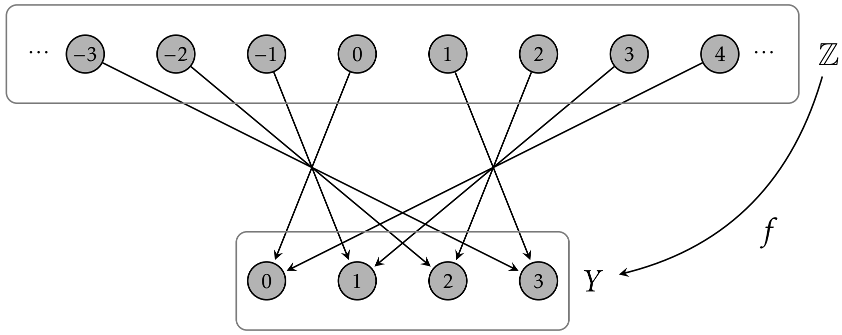

Figure 7.3: Function diagram for the function described in Problem 7.49.

7.3 Compositions and Inverse Functions

We begin this section with a method for combining two functions together that have compatible domains and codomains.

Definition 7.51. If $f : X \to Y$ and $g : Y \to Z$ are functions, we define $g \circ f : X \to Z$ via $\boxed{(g \circ f)(x) = g(f(x))}$. The function $g \circ f$ is called the **composition of** f **and** g.

It is important to notice that the function on the right is the one that "goes first." Moreover, we cannot compose any two random functions since the codomain of the first function must agree with the domain of the second function. In particular, $f \circ g$ may not be a sensible function even when $g \circ f$ exists. Figure 7.4 provides a visual representation of function composition in terms of function diagrams.

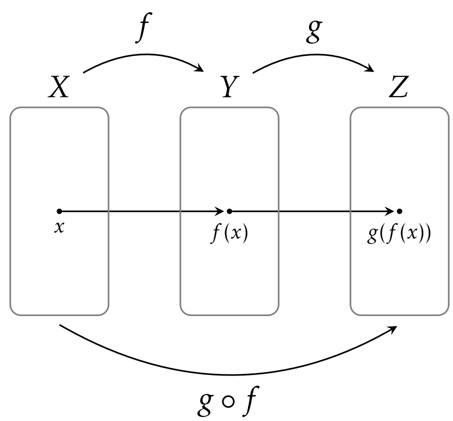

Figure 7.4: Visual representation of function composition.

Problem 7.52. Let $X = \{1,2,3,4\}$ and define $f : X \to X$ and $g : X \to X$ via

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

and

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

For each of the following functions, draw the corresponding function diagram in the spirit of Figure 7.4 and identify the range.

(a) $g \circ f$

(b) $f \circ g$

Example 7.53. Consider the inclusion map $\iota : X \to Y$ such that X is a proper subset of Y and suppose $f : Y \to Z$ is a function. Then the composite function $f \circ \iota : X \to Z$ is given by

$$f \circ \iota(x) = f(\iota(x)) = f(x)$$

for all $x \in X$. Notice that $f \circ \iota$ is simply the function f but with a smaller domain. In this case, we say that $f \circ \iota$ is the **restriction of** f **to** X, which is often denoted by $\boxed{f|_X}$.

The next problem illustrates that $f \circ g$ and $g \circ f$ need not be equal even when both composite functions exist.

Problem 7.54. Define $f : \mathbb{R} \to \mathbb{R}$ and $g : \mathbb{R} \to \mathbb{R}$ via $f(x) = x^2$ and $g(x) = 3x-5$, respectively. Determine formulas for the composite functions $f \circ g$ and $g \circ f$.

Problem 7.55. Define $f : \mathbb{R} \to \mathbb{R}$ and $g : \mathbb{R} \to \mathbb{R}$ via

$$f(x) = \begin{cases} 5x+7, & \text{if } x < 0 \\ 2x+1, & \text{if } x \geq 0 \end{cases}$$

and $g(x) = 7x - 11$, respectively. Find a formula for the composite function $g \circ f$.

Problem 7.56. Define $f : \mathbb{Z}/15\mathbb{Z} \to \mathbb{Z}/23\mathbb{Z}$ and $g : \mathbb{Z}/23\mathbb{Z} \to \mathbb{Z}/32\mathbb{Z}$ via $f([x]_{15}) = [3x+5]_{23}$ and $g([x]_{23}) = [2x+1]_{32}$, respectively. Find a formula for the composite function $g \circ f$.

The following result provides some insight into where the identity map got its name.

Theorem 7.57. If $f : X \to Y$ is a function, then $f \circ i_x = f = i_Y \circ f$, where i_X and i_Y are the identity maps on X and Y, respectively.

The next theorem tells us that function composition is associative.

Theorem 7.58. If $f : X \to Y$, $g : Y \to Z$, and $h : Z \to W$ are functions, then $(h \circ g) \circ f = h \circ (g \circ f)$.

Problem 7.59. In each case, give examples of finite sets X, Y, and Z, and functions $f : X \to Y$ and $g : Y \to Z$ that satisfy the given conditions. Drawing a function diagram is sufficient.

(a) f is surjective, but $g \circ f$ is not surjective.

(b) g is surjective, but $g \circ f$ is not surjective.

(c) f is injective, but $g \circ f$ is not injective.

(d) g is injective, but $g \circ f$ is not injective.

Theorem 7.60. If $f : X \to Y$ and $g : Y \to Z$ are both surjective functions, then $g \circ f$ is also surjective.

Theorem 7.61. If $f : X \to Y$ and $g : Y \to Z$ are both injective functions, then $g \circ f$ is also injective.

Corollary 7.62. If $f : X \to Y$ and $g : Y \to Z$ are both bijections, then $g \circ f$ is also a bijection.

Problem 7.63. Assume that $f : X \to Y$ and $g : Y \to Z$ are both functions. Determine whether each of the following statements is true or false. If a statement is true, prove it. Otherwise, provide a counterexample.

(a) If $g \circ f$ is injective, then f is injective.

(b) If $g \circ f$ is injective, then g is injective.

(c) If $g \circ f$ is surjective, then f is surjective.

(d) If $g \circ f$ is surjective, then g is surjective.

Theorem 7.64. Let $f : X \to Y$ be a function. Then f is injective if and only if there exists a function $g : Y \to X$ such that $g \circ f = i_X$, where i_X is the identity map on X.

The function g in the previous theorem is often called a **left inverse** of f.

Theorem 7.65. Let $f : X \to Y$ be a function. Then f is surjective if and only if there exists a function $g : Y \to X$ such that $f \circ g = i_Y$, where i_Y is the identity map on Y.

The function g in the previous theorem is often called a **right inverse** of f.

Problem 7.66. Provide an example of a function that has a left inverse but does not have a right inverse. Find the left inverse of your proposed function.

Problem 7.67. Provide an example of a function that has a right inverse but does not have a left inverse. Find the right inverse of your proposed function.

Corollary 7.68. If $f : X \to Y$ and $g : Y \to X$ are functions satisfying $g \circ f = i_X$ and $f \circ g = i_Y$, then f is a bijection.

In the previous result, the functions f and g "cancel" each other out. In this case, we say that g is a **two-sided inverse** of f.

Definition 7.69. Let $f : X \to Y$ be a function. The relation f^{-1} from Y to X, called$f$ **inverse**, is defined via

$$\boxed{f^{-1} = \{(f(x), x) \in Y \times X \mid x \in X\}}.$$

Notice that we called f^{-1} a relation and not a function. In some circumstances f^{-1} will be a function and sometimes it will not be. Given a function f, the inverse relation is simply the set of ordered pairs that results from reversing the ordered pairs in f. It is worth pointing out that we have only defined inverse relations for functions. However, one can easily adapt our definition to handle arbitrary relations.

Problem 7.70. Consider the function f given in Example 7.2 (see Figure 7.1). List the ordered pairs in the relation f^{-1} and draw the corresponding digraph. Is f^{-1} a function?

Problem 7.71. Provide an example of a function $f : X \to Y$ such that f^{-1} is a function. Drawing a function diagram is sufficient.

Problem 7.72. Suppose $X \subseteq \mathbb{R}$ and $f : X \to \mathbb{R}$ is a function. What is the relationship between the graph of the function f and the graph of the inverse relation f^{-1}?

Theorem 7.73. Let $f : X \to Y$ be a function. Then $f^{-1} : Y \to X$ is a function if and only if f is a bijection.

Problem 7.74. Suppose $X \subseteq \mathbb{R}$ and $f : X \to \mathbb{R}$ is a function. Fill in the blank with the appropriate phrase.

> The relation f^{-1} is a function if and only if every horizontal line hits the graph of f ________________.

Explain why this statement is true.

Theorem 7.75. If $f : X \to Y$ is a bijection, then

(a) $f^{-1} \circ f = i_X$, and

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

Theorem 7.76. If $f : X \to Y$ is a bijection, then $f^{-1} : Y \to X$ is also a bijection.

Theorem 7.77. If $f : X \to Y$ and $g : Y \to X$ are functions such that $g \circ f = i_X$ and $f \circ g = i_Y$, then f^{-1} is a function and $g = f^{-1}$.

The upshot of Theorems 7.75 and 7.77 is that if f^{-1} is a function, then it is the only one satisfying the two-sided inverse property exhibited in Corollary 7.68 and Theorem 7.75. That is, inverse functions are unique when they exist. When the relation f^{-1} is a function, we call it the **inverse function** of f.

Theorem 7.78. If $f : X \to Y$ is a bijection, then $(f^{-1})^{-1} = f$.

In the previous theorem, we restricted our attention to bijections so that f^{-1} would be a function, thus making $(f^{-1})^{-1}$ a sensible inverse relation in light of Definition 7.69. If we had defined inverses for arbitrary relations, then we would not have needed to require the function in Theorem 7.78 to be a bijection. In fact, we do not even need to require the relation to be a function. That is, if R is a relation from X to Y, then $(R^{-1})^{-1} = R$, as expected. Similarly, the next result generalizes to arbitrary relations.

Theorem 7.79. If $f : X \to Y$ and $g : Y \to Z$ are both bijections, then $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

The previous theorem is sometimes referred to as the "socks and shoes theorem". Do you see how it got this name?

7.4 Images and Preimages of Functions

There are two important types of sets related to functions.

Definition 7.80. Let $f : X \to Y$ be a function.

(a) If $S \subseteq X$, the **image** of S under f is defined via

$$\boxed{f(S) := \{f(x) \mid x \in S\}}.$$

(b) If $T \subseteq Y$, the **preimage** (or **inverse image**) of T under f is defined via

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

The image of a subset S of the domain is simply the subset of the codomain we obtain by mapping the elements of S. It is important to emphasize that the function f maps *elements* of X to *elements* of Y, but we can apply f to a *subset* of X to yield a *subset* of Y. That is, if $S \subseteq X$, then $f(S) \subseteq Y$. Note that the image of the domain is the same as the range of the function. That is, $f(X) = \mathrm{Rng}(f)$.

When it comes to preimages, there is a real opportunity for confusion. In Section 7.3, we introduced the inverse relation f^{-1} of a function f (see Defintion 7.69) and proved that this relation is a function exactly when f is a bijection (see Theorem 7.73). If $f^{-1} : Y \to X$ is a function, then it is sensible to write $f^{-1}(y)$ for $y \in Y$. Notice that we defined the preimage of a subset of the codomain regardless of whether f^{-1} is a function or not. In particular, for $T \subseteq Y$, $f^{-1}(T)$ is the set of elements in the domain that map to elements in T. As a special case, $f^{-1}(\{y\})$ is the set of elements in the domain that map to $y \in Y$. If $y \notin \mathrm{Rng}(f)$, then $f^{-1}(\{y\}) = \emptyset$. Notice that if $y \in Y$, $f^{-1}(\{y\})$ is always a sensible thing to write while $f^{-1}(y)$ only makes sense if f^{-1} is a function. Also, note that the preimage of the codomain is the domain. That is, $f^{-1}(Y) = X$.

Problem 7.81. Define $f : \mathbb{Z} \to \mathbb{Z}$ via $f(x) = x^2$. List elements in each of the following sets.

(a) $f(\{0, 1, 2\})$

(b) $f^{-1}(\{0, 1, 4\})$

Problem 7.82. Define $f : \mathbb{R} \to \mathbb{R}$ via $f(x) = 3x^2 - 4$. Find each of the following sets.

(a) $f(\{-1, 1\})$

(b) $f([-2, 4])$

(c) $f((-2, 4))$

(d) $f^{-1}([-10, 1])$

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

(f) $f(\emptyset)$

(g) $f(\mathbb{R})$

(h) $f^{-1}(\{-1\})$

(i) $f^{-1}(\emptyset)$

(j) $f^{-1}(\mathbb{R})$

Problem 7.83. Define $f : \mathbb{R} \to \mathbb{R}$ via $f(x) = x^2$.

(a) Find two nonempty subsets A and B of $\mathbb{R}$ such that $A \cap B = \emptyset$ but $f^{-1}(A) = f^{-1}(B)$.

(b) Find two nonempty subsets A and B of $\mathbb{R}$ such that $A \cap B = \emptyset$ but $f(A) = f(B)$.

Problem 7.84. Let $f : X \to Y$ and consider the relation defined in Theorem 7.44. For $x \in X$, what is the relationship between $f^{-1}(\{f(x)\})$ and the equivalence class containing x? Justify your answer.

Problem 7.85. Suppose $f : X \to Y$ is an injection and A and B are disjoint subsets of X. Are $f(A)$ and $f(B)$ necessarily disjoint subsets of Y? If so, prove it. Otherwise, provide a counterexample.

Problem 7.86. Find examples of functions f and g together with sets S and T such that $f(f^{-1}(T)) \neq T$ and $g^{-1}(g(S)) \neq S$.

Problem 7.87. Let $f : X \to Y$ be a function and suppose $A, B \subseteq X$ and $C, D \subseteq Y$. Determine whether each of the following statements is true or false. If a statement is true, prove it. Otherwise, provide a counterexample.

(a) If $A \subseteq B$, then $f(A) \subseteq f(B)$.

(b) If $C \subseteq D$, then $f^{-1}(C) \subseteq f^{-1}(D)$.

(c) $f(A \cup B) \subseteq f(A) \cup f(B)$.

(d) $f(A \cup B) \supseteq f(A) \cup f(B)$.

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

(f) $f(A \cap B) \supseteq f(A) \cap f(B)$.

(g) $f^{-1}(C \cup D) \subseteq f^{-1}(C) \cup f^{-1}(D)$.

(h) $f^{-1}(C \cup D) \supseteq f^{-1}(C) \cup f^{-1}(D)$.

(i) $f^{-1}(C \cap D) \subseteq f^{-1}(C) \cap f^{-1}(D)$.

(j) $f^{-1}(C \cap D) \supseteq f^{-1}(C) \cap f^{-1}(D)$.

(k) $A \subseteq f^{-1}(f(A))$.

(l) $A \supseteq f^{-1}(f(A))$.

(m) $f(f^{-1}(C)) \subseteq C$.

(n) $f(f^{-1}(C)) \supseteq C$.

Problem 7.88. For each of the statements in the previous problem that were false, determine conditions, if any, on the corresponding sets that would make the statement true.

Chapter 8

Cardinality

In this chapter, we will explore the notion of cardinality, which formalizes what it means for two sets to be the same "size".

8.1 Introduction to Cardinality

What does it mean for two sets to have the same "size"? If the sets are finite, this is easy: just count how many elements are in each set. Another approach would be to pair up the elements in each set and see if there are any left over. In other words, check to see if there is a one-to-one correspondence (i.e., bijection) between the two sets.

But what if the sets are infinite? For example, consider the set of natural numbers $\mathbb{N}$ and the set of even natural numbers $2\mathbb{N} := \{2n \mid n \in \mathbb{N}\}$. Clearly, $2\mathbb{N}$ is a proper subset of $\mathbb{N}$. Moreover, both sets are infinite. In this case, you might be thinking that $\mathbb{N}$ is "larger than" $2\mathbb{N}$. However, it turns out that there is a one-to-one correspondence between these two sets. In particular, consider the function $f : \mathbb{N} \to 2\mathbb{N}$ defined via $f(n) = 2n$. It is easily verified that f is both injective and surjective. In this case, mathematics has determined that the right viewpoint is that $\mathbb{N}$ and $2\mathbb{N}$ do have the same "size". However, it is clear that "size" is a bit too imprecise when it comes to infinite sets. We need something more rigorous.

Definition 8.1. Let A and B be sets. We say that A and B have the same **cardinality** if and only if there exists a bijection between A and B. In this case, we write $\boxed{\mathrm{card}(A) = \mathrm{card}(B)}$.

Note that we have not defined $\mathrm{card}(A)$ by itself. Doing so would not be too difficult for finite sets, but making such a notation precise in general is tricky business. When we write $\mathrm{card}(A) = \mathrm{card}(B)$ (and later $\mathrm{card}(A) \leq \mathrm{card}(B)$ and $\mathrm{card}(A) < \mathrm{card}(B)$), we are asserting the existence of a certain type of function from A to B.

If f is a bijection from A to B, then by Theorem 7.76, f^{-1} is a bijection from B to A. Either one of these functions can be utilized to prove that $\mathrm{card}(A) = \mathrm{card}(B)$. This idea is worth keeping in mind as you tackled problems in this chapter. In particular, you might have an easier time creating a bijection between two sets in one direction over the other. This is often a limitation of the human mind as to opposed to some fundamental mathematical difficulty.

Example 8.2. Let $A = \{1,2,3,4,5\}$ and $B = \{\text{apple}, \text{banana}, \text{cherry}, \text{dragon fruit}, \text{elderberry}\}$. The function $f : A \to B$ given by

$$f = \{(1, \text{apple}), (2, \text{banana}), (3, \text{cherry}), (4, \text{dragon fruit}), (5, \text{elderberry})\}$$

is a bijection from A to B, and hence $\text{card}(A) = \text{card}(B)$. Note that this is not the only bijection from A to B. In fact, there are $5! = 120$ bijections from A to B, one of which is the function f we defined above. The inverse of each bijection from A to B is a bijection from B to A. We could also use any of of these bijections to verify that $\text{card}(A) = \text{card}(B)$.

Example 8.3. Define $f : \mathbb{Z} \to 6\mathbb{Z}$ via $f(n) = 6n$. It is easily verified that f is both injective and surjective, and hence $\text{card}(\mathbb{Z}) = \text{card}(6\mathbb{Z})$. We could also utilize the inverse function $f^{-1} : 6\mathbb{Z} \to \mathbb{Z}$ given by $f^{-1}(n) = \frac{1}{6}n$ to show that $\mathbb{Z}$ and $6\mathbb{Z}$ have the same cardinality.

Example 8.4. Let $\mathbb{R}^+$ denote the set of positive real numbers and define $f : \mathbb{R} \to \mathbb{R}^+$ via $f(x) = e^x$. As you are likely familiar with, this exponential function is a bijection, and so $\text{card}(\mathbb{R}) = \text{card}(\mathbb{R}^+)$. Similar to the previous example, we could also use the inverse function $f^{-1} : \mathbb{R}^+ \to \mathbb{R}$ given by $f(x) = \ln(x)$ to show that these two sets have the same cardinality.

The previous two examples illustrate an important distinction between finite sets and infinite sets, namely infinite sets can be in bijection with proper subsets of themselves! Theorems 8.23 and 8.31 will make this idea explicit.

Example 8.5. Let $m, n \in \mathbb{N} \cup \{0\}$. A North-East lattice path from $(0,0)$ to (m,n) is path in the plane from $(0,0)$ to (m,n) consisting only steps either one unit North or one unit East. Note that every lattice path from $(0,0)$ to (m,n) consists of a total of $m+n$ steps. Figure 8.1 shows a North-East lattice path from $(0,0)$ to $(4,3)$. Let $\mathcal{L}_{m,n}$ denote the set of North-East paths from $(0,0)$ to (m,n). For example, the North-East lattice path given in Figure 8.1 is an element of $\mathcal{L}_{4,3}$. A binary string of length k is an ordered list of consisting of k entries where each entry is either 0 or 1. For example, 0101100 and 0101001 are two different binary strings of length 7. Let $\mathcal{S}_k$ denote the set of binary strings of length k. For example, $\mathcal{S}_3 = \{000, 100, 010, 001, 110, 101, 011, 111\}$. We claim that there is a bijection between $\mathcal{L}_{m,n}$ and $\mathcal{S}_{m+n}$. One such bijection is given by mapping a lattice path to the string that results by assigning each East step to 0 and each North step to 1 as we travel the path from $(0,0)$ to (m,n). Using this construction, the lattice path in Figure 8.1 would get mapped to the binary string 0101100. Since no two lattice paths will map to the same string, our mapping is injective. Given a string in $\mathcal{S}_{m+n}$, it is easy to find the lattice path in $\mathcal{L}_{m,n}$ that maps to it, and so our function is also surjective. Thus, our mapping is a bijection between $\mathcal{L}_{m,n}$ and $\mathcal{S}_{m+n}$. We have shown that $\text{card}(\mathcal{L}_{m,n}) = \text{card}(\mathcal{S}_{m+n})$.

Problem 8.6. Prove each of the following. In each case, you should create a bijection between the two sets. Briefly justify that your functions are in fact bijections.

(a) $\text{card}(\{a,b,c\}) = \text{card}(\{x,y,z\})$

(b) $\text{card}(\mathbb{N}) = \text{card}(\{2n+1 \mid n \in \mathbb{N}\})$

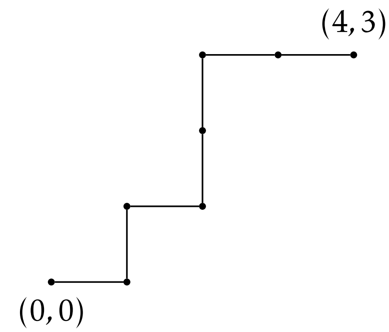

Figure 8.1: A North-East lattice path from $(0,0)$ to $(4,3)$.

(c) $\text{card}(\mathbb{N}) = \text{card}(\mathbb{Z})$

(d) $\text{card}((a,b)) = \text{card}((c,d))$ (where (a,b) and (c,d) are intervals)[1]

(e) $\text{card}(\mathbb{N}) = \text{card}(\{\frac{1}{2^n} \mid n \in \mathbb{N}\})$

Problem 8.7. If A is a set, do A and $A \times \{x\}$ have the same cardinality? Justify your answer.

Problem 8.8. Let $\mathcal{D}_n$ denote the collection of North-East lattice paths from $(0,0)$ to (n,n) that never drop below the line $y = x$. These types of lattice paths are often called Dyck paths after the German mathematician Walther Franz Anton von Dyck (1856–1934). A sequence of parentheses is balanced if it can be parsed syntactically. In other words, there should be the same number of open parentheses "(" and closed parentheses ")", and when reading from left to right there should never be more closed parentheses than open. For example, ()()() and ()(()) are balanced parenthesizations consisting of three pairs of parentheses while ())(() and ()(()(are not balanced. Let $\mathcal{B}_n$ denote the collection of balanced parenthesizations consisting of n pairs of parentheses. For example, $\mathcal{B}_3 = \{()()(), ()(()), (()()), (())(), ((()))\}$.

(a) Find all Dyck paths in $\mathcal{D}_3$.

(b) Prove that $\text{card}(\mathcal{D}_n) = \text{card}(\mathcal{B}_n)$.

Problem 8.9. Let $\mathcal{F}$ denote the set of functions from $\mathbb{N}$ to $\{0,1\}$.

(a) Describe at least three functions in $\mathcal{F}$.

(b) Prove that $\mathcal{F}$ and $\mathcal{P}(\mathbb{N})$ have the same cardinality.[2]

Our first theorem concerning cardinality will likely not come as a surprise.

Theorem 8.10. Let A, B, and C be sets.

(a) $\text{card}(A) = \text{card}(A)$.

[1] *Hint:* Try creating a linear function $f : (a,b) \to (c,d)$. Drawing a picture should help.
[2] *Hint:* Define $\varphi : \mathcal{F} \to \mathcal{P}(\mathbb{N})$ so that $\varphi(f)$ outputs a subset of $\mathbb{N}$ determined by when f outputs a 1.

(b) If $\text{card}(A) = \text{card}(B)$, then $\text{card}(B) = \text{card}(A)$.

(c) If $\text{card}(A) = \text{card}(B)$ and $\text{card}(B) = \text{card}(C)$, then $\text{card}(A) = \text{card}(C)$.

In light of the previous theorem, the next result should not be surprising.

Corollary 8.11. If X is a set, then "has the same cardinality as" is an equivalence relation on $\mathcal{P}(X)$.

Theorem 8.12. Let A, B, C, and D be sets such that $\text{card}(A) = \text{card}(C)$ and $\text{card}(B) = \text{card}(D)$.

(a) If A and B are disjoint and C and D are disjoint, then $\text{card}(A \cup B) = \text{card}(C \cup D)$.

(b) $\text{card}(A \times B) = \text{card}(C \times D)$.

Given two finite sets, it makes sense to say that one set is "larger than" another provided one set contains more elements than the other. We would like to generalize this idea to handle both finite and infinite sets.

Definition 8.13. Let A and B be sets. If there is a injective function from A to B, then we say that the **cardinality of A is less than or equal to the cardinality of** B. In this case, we write $\boxed{\text{card}(A) \leq \text{card}(B)}$.

Theorem 8.14. Let A, B, and C be sets.

(a) If $A \subseteq B$, then $\text{card}(A) \leq \text{card}(B)$.

(b) If $\text{card}(A) \leq \text{card}(B)$ and $\text{card}(B) \leq \text{card}(C)$, then $\text{card}(A) \leq \text{card}(C)$.

(c) If $C \subseteq A$ while $\text{card}(B) = \text{card}(C)$, then $\text{card}(B) \leq \text{card}(A)$.

It might be tempting to think that the existence of injective function from a set A to a set B that is *not* surjective would verify that $\text{card}(A) \leq \text{card}(B)$ and $\text{card}(A) \neq \text{card}(B)$. While this is true for finite sets, it is not true for infinite sets as the next problem asks you to verify.

Problem 8.15. Provide an example of sets A and B such that $\text{card}(A) = \text{card}(B)$ despite the fact that there exists an injective function from A to B that is not surjective.

Definition 8.16. Let A and B be sets. We write $\boxed{\text{card}(A) < \text{card}(B)}$ if and only if $\text{card}(A) \leq \text{card}(B)$ and $\text{card}(A) \neq \text{card}(B)$.

As a reminder, the statements $\text{card}(A) = \text{card}(B)$ and $\text{card}(A) \leq \text{card}(B)$ are symbolic ways of asserting the existence of certain types of functions from A to B. When we write $\text{card}(A) < \text{card}(B)$, we are saying something much stronger than "There exists a function $f : A \to B$ that is injective but not surjective." The statement $\text{card}(A) < \text{card}(B)$ is asserting that *every* injective function from A to B is not surjective. In general, it is difficult to prove statements like $\text{card}(A) \neq \text{card}(B)$ or $\text{card}(A) < \text{card}(B)$.

8.2 Finite Sets

In the previous section, we used the phrase "finite set" without formally defining it. Let's be a bit more precise. The following shorthand comes in handy.

Definition 8.17. For each $n \in \mathbb{N}$, define $\boxed{[n] := \{1, 2, \ldots, n\}}$.

For example, $[5] = \{1, 2, 3, 4, 5\}$. Notice that our notation looks just like the notation we used for equivalence classes. However, despite the similar notation, these concepts are unrelated. We will have to rely on context to keep them straight.

The next definition should coincide with your intuition about what it means for a set to be finite.

Definition 8.18. A set A is **finite** if and only if $A = \emptyset$ or $\text{card}(A) = \text{card}([n])$ for some $n \in \mathbb{N}$. If $A = \emptyset$, then we say that A has **cardinality** 0 and if $\text{card}(A) = \text{card}([n])$, then we say that A has **cardinality** n.

Let's prove a few results about finite sets. When proving the following theorems, do not forget to consider the empty set.

Theorem 8.19. If A is finite and $\text{card}(A) = \text{card}(B)$, then B is finite.

Theorem 8.20. If A has cardinality $n \in \mathbb{N} \cup \{0\}$ and $x \notin A$, then $A \cup \{x\}$ is finite and has cardinality $n + 1$.

Consider using induction when proving the next theorem.

Theorem 8.21. For every $n \in \mathbb{N}$, every subset of $[n]$ is finite.

Theorem 8.20 shows that adding a single element to a finite set increases the cardinality by 1. As you would expect, removing one element from a finite set decreases the cardinality by 1.

Theorem 8.22. If A has cardinality $n \in \mathbb{N}$, then for all $x \in A$, $A \setminus \{x\}$ is finite and has cardinality $n - 1$.

The next result tells us that the cardinality of a proper subset of a finite set is never the same as the cardinality of the original set. It turns out that this theorem does not hold for infinite sets.

Theorem 8.23. Every subset of a finite set is finite. In particular, if A is a finite set, then $\text{card}(B) < \text{card}(A)$ for all proper subsets B of A.

Induction is a sensible approach to proving the next two theorems.

Theorem 8.24. If $A_1, A_2, \ldots, A_k$ is a finite collection of finite sets, then $\displaystyle\bigcup_{i=1}^{k} A_i$ is finite.

The next theorem, called the Pigeonhole Principle, is surprisingly useful. It puts restrictions on when we may have an injective function. The name of the theorem is inspired by the following idea: If n pigeons wish to roost in a house with k pigeonholes and $n > k$, then it must be the case that at least one hole contains more than one pigeon. Note that 2 is the smallest value of n that makes sense in the hypothesis below.

Theorem 8.25 (Pigeonhole Principle)**.** If $n, k \in \mathbb{N}$ and $f : [n] \to [k]$ with $n > k$, then f is not injective.

8.3 Infinite Sets

In the previous section, we explored finite sets. Now, let's tinker with infinite sets.

Definition 8.26. A set A is **infinite** if and only if A is not finite.

Let's see if we can utilize this definition to prove that the set of natural numbers is infinite.

Theorem 8.27. The set $\mathbb{N}$ of natural numbers is infinite.[3]

The next theorem is analogous to Theorem 8.19, but for infinite sets. As we shall see later, the converse of this theorem is not true in general.

Theorem 8.28. If A is infinite and $\operatorname{card}(A) = \operatorname{card}(B)$, then B is infinite.[4]

Problem 8.29. Quickly verify that the following sets are infinite by appealing to Theorem 8.27, Theorem 8.28, or Problem 8.6.

(a) The set of odd natural numbers

(b) The set of even natural numbers

(c) $\mathbb{Z}$

(d) $R = \{\frac{1}{2^n} \mid n \in \mathbb{N}\}$

(e) $\mathbb{N} \times \{a\}$

Notice that Definition 8.26 tells us what infinite sets are not, but it doesn't really tell us what they are. In light of Theorem 8.27, one way of thinking about infinite sets is as follows. Suppose A is some nonempty set. Let's select a random element from A and set it aside. We will call this element the "first" element. Then we select one of the remaining elements and set is aside, as well. This is the "second" element. Imagine we continue

[3]*Hint:* For sake of a contradiction, assume otherwise. Then there exists $n \in \mathbb{N}$ such that $\operatorname{card}([n]) = \operatorname{card}(\mathbb{N})$, which implies that there exists a bijection $f : [n] \to \mathbb{N}$. What can you say about the number $m := \max(f(1), f(2), \ldots, f(n)) + 1$?

[4]*Hint:* Try a proof by contradiction. You should end up composing two bijections, say $f : A \to B$ and $g : B \to [n]$ for some $n \in \mathbb{N}$.

this way, choosing a "third" element, and "fourth" element, etc. If the set is infinite, we should never run out of elements to select. Otherwise, we would create a bijection with $[n]$ for some $n \in \mathbb{N}$.

The next problem, sometimes refered to as the Hilbert Hotel[5], illustrates another way of thinking about infinite sets.

Problem 8.30. The Infinite Hotel has rooms numbered $1, 2, 3, 4, \ldots$. Every room in the Infinite Hotel is currently occupied.

(i) Is it possible to make room for one more guest (assuming they want a room all to themselves)?

(ii) An infinite number of new guests, say $g_1, g_2, g_3, \ldots$, show up in the lobby and each demands a room. Is it possible to make room for all the new guests even if the hotel is already full?

The previous problem verifies that a proper subset of the natural numbers is in bijection with the natural numbers themselves. We also witnessed this in parts (a) and (b) of Problem 8.29. Notice that Theorem 8.23 forbids this type of behavior for finite sets. It turns out that this phenomenon is true for all infinite sets. The next theorem verifies that that the two viewpoints of infinite sets discussed above are valid.

Theorem 8.31. The following statements are equivalent.[6]

(i) The set A is infinite.

(ii) There exists an injective function $f : \mathbb{N} \to A$.

(iii) The set A can be put in bijection with a proper subset of A (i.e., there exists a proper subset B of A such that $\operatorname{card}(B) = \operatorname{card}(A)$).

It is worth mentioning that for the previous theorem, (iii) implies (i) follows immediately from the contrapositive of Theorem 8.23.

Corollary 8.32. A set is infinite if and only if it has an infinite subset.

Corollary 8.33. If A is an infinite set, then $\operatorname{card}(\mathbb{N}) \leq \operatorname{card}(A)$.

Problem 8.34. Find a new proof of Theorem 8.27 that uses (iii) implies (i) from Theorem 8.31.

Problem 8.35. Quickly verify that the following sets are infinite by appealing to either Theorem 8.31 (use (ii) implies (i)) or Corollary 8.32.

[5]The Hilbert Hotel is named after mathematician David Hilbert (1862–1942).

[6]*Hint:* Prove (i) if and only if (ii) and (ii) if and only if (iii). For (i) implies (ii), construct f recursively. For (ii) implies (i), try a proof by contradiction. For (ii) implies (iii), let $B = A \setminus \{f(1), f(2), \ldots\}$ and show that A can be put in bijection with $B \cup \{f(2), f(3), \ldots\}$. Lastly, for (iii) implies (ii), suppose $g : A \to C$ is a bijection for some proper subset C of A. Let $a \in A \setminus C$. Define $f : \mathbb{N} \to A$ via $f(n) = g^n(a)$, where g^n means compose g with itself n times.

(a) Set of odd natural numbers

(b) Set of even natural numbers

(c) $\mathbb{Z}$

(d) $\mathbb{N} \times \mathbb{N}$

(e) $\mathbb{Q}$

(f) $\mathbb{R}$

(g) Set of perfect squares in $\mathbb{N}$

(h) $(0, 1)$

(i) $\mathbb{C} := \{a + bi \mid a, b \in \mathbb{R}\}$

8.4 Countable Sets

Recall that if $A = \emptyset$, then we say that A has cardinality 0. Also, if $\text{card}(A) = \text{card}([n])$ for $n \in \mathbb{N}$, then we say that A has cardinality n. We have a special way of describing sets that are in bijection with the natural numbers.

Definition 8.36. If A is a set such that $\text{card}(A) = \text{card}(\mathbb{N})$, then we say that A is **denumerable** and has **cardinality $\aleph_0$** (read "aleph naught").

Notice if a set A has cardinality $1, 2, \ldots$, or $\aleph_0$, we can label the elements in A as "first", "second", and so on. That is, we can "count" the elements in these situations. Certainly, if a set has cardinality 0, counting is not an issue. This idea leads to the following definition.

Definition 8.37. A set A is called **countable** if and only if A is finite or denumerable. A set is called **uncountable** if and only if it is not countable.

Problem 8.38. Quickly justify that each of the following sets is countable. Feel free to appeal to previous problems.

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

(b) Set of odd natural numbers

(c) Set of even natural numbers

(d) $R := \{\frac{1}{2^n} \mid n \in \mathbb{N}\}$

(e) Set of perfect squares in $\mathbb{N}$

(f) $\mathbb{Z}$

(g) $\mathbb{N} \times \{a\}$

Theorem 8.39. Let A and B be sets such that A is countable. If $f : A \to B$ is a bijection, then B is countable.

Theorem 8.40. Every subset of a countable set is countable.[7]

Theorem 8.41. A set is countable if and only if it has the same cardinality of some subset of the natural numbers.

Theorem 8.42. If $f : \mathbb{N} \to A$ is a surjective function, then A is countable.

Loosely speaking, the next theorem tells us that we can arrange all of the rational numbers then count them "first", "second", "third", etc. Given the fact that between any two distinct rational numbers on the number line, there are an infinite number of other rational numbers (justified by taking repeated midpoints), this may seem counterintuitive.

Theorem 8.43. The set of rational numbers $\mathbb{Q}$ is countable.[8]

Theorem 8.44. If A and B are countable sets, then $A \cup B$ is countable.

We would like to prove a stronger result than the previous theorem. To do so, we need a lemma.

Lemma 8.45. Let $\{A_n\}_{n=1}^{\infty}$ be a collection of sets. Define $B_1 := A_1$ and for each natural number $n > 1$, define

$$B_n := A_n \setminus \bigcup_{i=1}^{n-1} A_i.$$

Then we we have the following:

(a) The collection $\{B_n\}_{n=1}^{\infty}$ is pairwise disjoint.

(b) $\displaystyle\bigcup_{n=1}^{\infty} A_n = \bigcup_{n=1}^{\infty} B_n$.

The next theorem states that the union of a countable collection of countable sets is countable. To prove this, consider two cases: To prove the next theorem, consider two cases:

1. The collection of sets is finite.
2. The collection of sets is infinite.

[7] *Hint:* Let A be a countable set. Consider the cases when A is finite versus infinite. The contrapositive of Corollary 8.32 should be useful for the case when A is finite.

[8] *Hint:* Make a table with column headings $0, 1, -1, 2, -2, \ldots$ and row headings $1, 2, 3, 4, 5, \ldots$. If a column has heading m and a row has heading n, then the corresponding entry in the table is given by the fraction m/n. Find a way to zig-zag through the table making sure to hit every entry in the table (not including column and row headings) exactly once. This justifies that there is a bijection between $\mathbb{N}$ and the entries in the table. Do you see why? Now, we aren't done yet because every rational number appears an infinite number of times in the table. Appeal to Theorem 8.40.

To handle the first case, use induction together with Theorem 8.44. The second case is substantially more challenging. First, use Lemma 8.45 to construct a collection $\{B_n\}$ of pairwise disjoint sets whose union is equal to the union of the original collection. Since each B_n is a subset of one of the sets in the original collection and each of these sets is countable, each B_n is also countable by Theorem 8.40. This implies that for each n, we can write $B_n = \{b_{n,1}, b_{n,2}, b_{n,3}, \ldots\}$, where the set may be finite or infinite. From here, we outline two different approaches for continuing. One approach is to construct a bijection from $\mathbb{N}$ to $\bigcup_{n=1}^{\infty} B_n$ using Figure 8.2 as inspiration. One thing you will need to address is what to do when a set in the collection $\{B_n\}$ is finite. For the second approach, define $f : \bigcup_{n=1}^{\infty} B_n \to \mathbb{N}$ via $f(b_{n,m}) = 2^n 3^m$, verify that this function is injective, and then appeal to Theorem 8.40. Try using both of these approaches when tackling the proof of the following theorem.

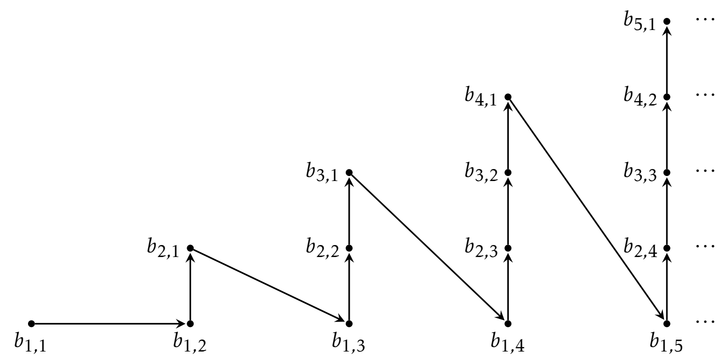

Figure 8.2: Inspiration for one possible approach to proving Theorem 8.46.

Theorem 8.46. Let Δ be equal to either $\mathbb{N}$ or $[k]$ for some $k \in \mathbb{N}$. If $\{A_n\}_{n\in\Delta}$ is a countable collection of sets such that each A_n is countable, then $\bigcup_{n\in\Delta} A_n$ is countable.

Theorem 8.47. If A and B are countable sets, then $A \times B$ is countable.

Theorem 8.48. The set of all finite sequences of 0's and 1's (e.g., 0110010 is a finite sequence consisting of 0's and 1') is countable.

Theorem 8.49. The collection of all finite subsets of a countable set is countable.

8.5 Uncountable Sets

Recall from Definition 8.37 that a set A is **uncountable** if and only if A is not countable. Since all finite sets are countable, the only way a set could be uncountable is if it is infinite. It follows that a set A is uncountable if and only if there is never a bijection between $\mathbb{N}$ and A. It's not clear that uncountable sets even exist! It turns out that uncountable sets do exist and in this section, we will discover a few of them.

Our first task is to prove that the interval $(0,1)$ is uncountable. By Problem 8.35(h), we know that $(0,1)$ is an infinite set, so it is at least plausible that $(0,1)$ is uncountable. The following problem outlines the proof of Theorem 8.51. Our approach is often referred to as **Cantor's Diagonalization Argument**.

Before we get started, recall that every number in $(0,1)$ can be written in decimal form. However, there may be more than one way to write a given number in decimal form. For example, 0.2 equals $0.1\overline{99}$. A number $0.a_1a_2a_3\ldots$ in $(0,1)$ is said to be in **standard decimal form** if and only if there is no k such that for all $i>k$, $a_i=9$. That is, a number is in standard decimal form if and only if its decimal expansion does not end with a repeating sequence of 9's. For example, 0.2 is in standard decimal form while $0.1\overline{99}$ is not, even though both represent the same number. It turns out that every real number can be expressed uniquely in standard decimal form. We will take this fact for granted.

Problem 8.50. For sake of a contradiction, assume the interval $(0,1)$ is countable. Then there exists a bijection $f:\mathbb{N}\to(0,1)$. For each $n\in\mathbb{N}$, its image under f is some number in $(0,1)$. Write $f(n)=0.a_{1n}a_{2n}a_{3n}\ldots$, where a_{1n} is the first digit in the standard decimal form for the image of n, a_{2n} is the second digit, and so on. If $f(n)$ terminates after k digits, then our convention will be to continue the decimal expansion with 0's. Now, define $b=0.b_1b_2b_3\ldots$, where

$$b_i=\begin{cases}2, & \text{if } a_{ii}\neq 2\\ 3, & \text{if } a_{ii}=2.\end{cases}$$

(a) Prove that the decimal expansion that defines b above is in standard decimal form.

(b) Prove that for all $n\in\mathbb{N}$, $f(n)\neq b$.

(c) Explain why f is cannot be surjective and why this is a contradiction.

You just proved that the interval $(0,1)$ cannot be countable!

The previous problem proves following theorem.

Theorem 8.51. The open interval $(0,1)$ is uncountable.

Loosely speaking, what Theorem 8.51 says is that the open interval $(0,1)$ is "bigger" in terms of the number of elements it contains than the natural numbers and even the rational numbers. This shows that there are infinite sets of different sizes! We now know there is at least one uncountable set, namely the interval $(0,1)$. The next three results are useful for finding other uncountable sets.

Theorem 8.52. If A and B are sets such that $A\subseteq B$ and A is uncountable, then B is uncountable.[9]

Corollary 8.53. If A and B are sets such that A is uncountable and B is countable, then $A\setminus B$ is uncountable.

Theorem 8.54. If $f:A\to B$ is an injective function and A is uncountable, then B is uncountable.

[9] *Hint:* Try a proof by contradiction. Take a look at Theorem 8.40.

Theorem 8.55. The set of real numbers is uncountable. Moreover, $\text{card}((0,1)) = \text{card}(\mathbb{R})$.[10]

Theorem 8.56. If $a, b \in \mathbb{R}$ with $a < b$, then (a,b), $[a,b]$, $(a,b]$, and $[a,b)$ are all uncountable.

Theorem 8.57. The set of irrational numbers is uncountable.

Theorem 8.58. The set $\mathbb{C}$ of complex numbers is uncountable.

Problem 8.59. Determine whether each of the following statements is true or false. If a statement is true, prove it. Otherwise, provide a counterexample.

(a) If A and B are sets such that A is uncountable, then $A \cup B$ is uncountable.

(b) If A and B are sets such that A is uncountable, then $A \cap B$ is uncountable.

(c) If A and B are sets such that A is uncountable, then $A \times B$ is uncountable.

(d) If A and B are sets such that A is uncountable, then $A \setminus B$ is uncountable.

Problem 8.60. Let S be the set of infinite sequences of 0's and 1's. Determine whether S is countable or uncountable and prove that your answer is correct.

It turns out that the two uncountable sets may or may not have the same cardinality. Perhaps surprisingly, there are sets that are even "bigger" than the set of real numbers. Given any set, we can always increase the cardinality by considering its power set.

Theorem 8.61. If A is a set, then $\text{card}(A) < \text{card}(\mathcal{P}(A))$.[11]

Recall that cardinality provides a way for talking about "how big" a set is. The fact that the natural numbers and the real numbers have different cardinality (one countable, the other uncountable), tells us that there are at least two different "sizes of infinity". Theorem 8.61 tells us that there are infinitely many "sizes of infinity."

Theorem 8.62. If S is the set from Problem 8.60, then $\text{card}(\mathcal{P}(\mathbb{N})) = \text{card}(S)$.

[10] *Hint:* To show that $\mathbb{R}$ is uncountable, appeal to Theorem 8.52. To show that $\text{card}((0,1)) = \text{card}(\mathbb{R})$, consider the function $f : (0,1) \to \mathbb{R}$ defined via $f(x) = \tan(\pi x - \frac{\pi}{2})$. It is worth pointing out that proving $\text{card}((0,1)) = \text{card}(\mathbb{R})$ automatically proves that $\mathbb{R}$ is uncountable.

[11] *Hint:* Mimic Cantor's Diagonalization Argument for showing that the interval $(0,1)$ is uncountable.

Appendix A

Elements of Style for Proofs

Years of elementary school math taught us incorrectly that the answer to a math problem is just a single number, "the right answer." It is time to unlearn those lessons; those days are over. From here on out, mathematics is about discovering proofs and writing them clearly and compellingly.

The following rules apply whenever you write a proof. Keep these rules handy so that you may refer to them as you write your proofs.

1. **The burden of communication lies on you, not on your reader.** It is your job to explain your thoughts; it is not your reader's job to guess them from a few hints. You are trying to convince a skeptical reader who doesn't believe you, so you need to argue with airtight logic in crystal clear language; otherwise the reader will continue to doubt. If you didn't write something on the paper, then (a) you didn't communicate it, (b) the reader didn't learn it, and (c) the grader has to assume you didn't know it in the first place.

2. **Tell the reader what you're proving.** The reader doesn't necessarily know or remember what "Theorem 2.13" is. Even a professor grading a stack of papers might lose track from time to time. Therefore, the statement you are proving should be on the same page as the beginning of your proof. For an exam this won't be a problem, of course, but on your homework, recopy the claim you are proving. This has the additional advantage that when you study for exams by reviewing your homework, you won't have to flip back in the notes/textbook to know what you were proving.

3. **Use English words.** Although there will usually be equations or mathematical statements in your proofs, use English sentences to connect them and display their logical relationships. If you look in your notes/textbook, you'll see that each proof consists mostly of English words.

4. **Use complete sentences.** If you wrote a history essay in sentence fragments, the reader would not understand what you meant; likewise in mathematics you must use complete sentences, with verbs, to convey your logical train of thought.

   Some complete sentences can be written purely in mathematical symbols, such as equations (e.g., $a^3 = b^{-1}$), inequalities (e.g., $x < 5$), and other relations (like $5 \mid 10$ or

$7 \in \mathbb{Z}$). These statements usually express a relationship between two mathematical *objects*, like numbers or sets. However, it is considered bad style to begin a sentence with symbols. A common phrase to use to avoid starting a sentence with mathematical symbols is "We see that..."

5. **Show the logical connections among your sentences.** Use phrases like "Therefore" or "because" or "if…, then…" or "if and only if" to connect your sentences.

6. **Know the difference between statements and objects.** A mathematical object is a *thing*, a noun, such as a group, an element, a vector space, a number, an ordered pair, etc. Objects either exist or don't exist. Statements, on the other hand, are mathematical *sentences*: they can be true or false.

   When you see or write a cluster of math symbols, be sure you know whether it's an object (e.g., "x^2+3") or a statement (e.g., "$x^2+3<7$"). One way to tell is that every mathematical statement includes a verb, such as $=$, $\leq$, "divides", etc.

7. **The symbol "=" means "equals".** Don't write $A = B$ unless you mean that A actually equals B. This rule seems obvious, but there is a great temptation to be sloppy. In calculus, for example, some people might write $f(x) = x^2 = 2x$ (which is false), when they really mean that "if $f(x) = x^2$, then $f'(x) = 2x$."

8. **Don't interchange $=$ and $\implies$.** The equals sign connects two *objects*, as in "$x^2 = b$"; the symbol "$\implies$" is an abbreviation for "implies" and connects two *statements*, as in "$a+b=a \implies b=0$." You should avoid using $\implies$ in your formal write-ups.

9. **Avoid logical symbols in your proofs.** Similar to $\implies$, you should avoid using the logical symbols $\forall, \exists, \vee, \wedge$, and $\iff$ in your formal write-ups. These symbols are useful for abbreviating in your scratch work.

10. **Say exactly what you mean.** Just as $=$ is sometimes abused, so too people sometimes write $A \in B$ when they mean $A \subseteq B$, or write $a_{ij} \in A$ when they mean that a_{ij} is an entry in matrix A. Mathematics is a very precise language, and there is a way to say exactly what you mean; find it and use it.

11. **Don't write anything unproven.** Every statement on your paper should be something you *know* to be true. The reader expects your proof to be a series of statements, each proven by the statements that came before it. If you ever need to write something you don't yet know is true, you *must* preface it with words like "assume," "suppose," or "if" (if you are temporarily assuming it), or with words like "we need to show that" or "we claim that" (if it is your goal). Otherwise the reader will think they have missed part of your proof.

12. **Write strings of equalities (or inequalities) in the proper order.** When your reader sees something like
$$A = B \leq C = D,$$
    he/she expects to understand easily why $A = B$, why $B \leq C$, and why $C = D$, and he/she expects the *point* of the entire line to be the more complicated fact that $A \leq$

D. For example, if you were computing the distance d of the point $(12,5)$ from the origin, you could write

$$d = \sqrt{12^2 + 5^2} = 13.$$

In this string of equalities, the first equals sign is true by the Pythagorean theorem, the second is just arithmetic, and the *point* is that the first item equals the last item: $d = 13$.

A common error is to write strings of equations in the wrong order. For example, if you were to write "$\sqrt{12^2+5^2} = 13 = d$", your reader would understand the first equals sign, would be baffled as to how we know $d = 13$, and would be utterly perplexed as to why you wanted or needed to go through 13 to prove that $\sqrt{12^2+5^2} = d$.

13. **Avoid circularity.** Be sure that no step in your proof makes use of the conclusion!

14. **Don't write the proof backwards.** Beginning students often attempt to write "proofs" like the following, which attempts to prove that $\tan^2(x) = \sec^2(x) - 1$:

$$\begin{aligned}
\tan^2(x) &= \sec^2(x) - 1 \\
\left(\frac{\sin(x)}{\cos(x)}\right)^2 &= \frac{1}{\cos^2(x)} - 1 \\
\frac{\sin^2(x)}{\cos^2(x)} &= \frac{1-\cos^2(x)}{\cos^2(x)} \\
\sin^2(x) &= 1 - \cos^2(x) \\
\sin^2(x) + \cos^2(x) &= 1 \\
1 &= 1
\end{aligned}$$

Notice what has happened here: the student *started* with the conclusion, and deduced the true statement "$1 = 1$." In other words, he/she has proved "If $\tan^2(x) = \sec^2(x) - 1$, then $1 = 1$," which is true but highly uninteresting.

Now this isn't a bad way of *finding* a proof. Working backwards from your goal often is a good strategy *on your scratch paper*, but when it's time to *write* your proof, you have to start with the hypotheses and work to the conclusion.

Here is an example of a suitable proof for the desired result, where each expression follows from the one immediately proceeding it:

$$\begin{aligned}
\sec^2(x) - 1 &= \frac{1}{\cos^2(x)} - 1 \\
&= \frac{1 - \cos^2(x)}{\cos^2(x)} \\
&= \frac{\sin^2(x)}{\cos^2(x)} \\
&= \left(\frac{\sin(x)}{\cos(x)}\right)^2 \\
&= (\tan(x))^2 \\
&= \tan^2(x).
\end{aligned}$$

15. **Be concise.** Most students err by writing their proofs too short, so that the reader can't understand their logic. It is nevertheless quite possible to be too wordy, and if you find yourself writing a full-page essay, it's probably because you don't really have a proof, but just an intuition. When you find a way to turn that intuition into a formal proof, it will be much shorter.

16. **Introduce every symbol you use.** If you use the letter "k," the reader should know exactly what k is. Good phrases for introducing symbols include "Let $n \in \mathbb{N}$," "Let k be the least integer such that...," "For every real number a...," and "Suppose that X is a counterexample."

17. **Use appropriate quantifiers (once).** When you introduce a variable $x \in S$, it must be clear to your reader whether you mean "for all $x \in S$" or just "for some $x \in S$." If you just say something like "$y = x^2$ where $x \in S$," the word "where" doesn't indicate whether you mean "for all" or "some".

    Phrases indicating the quantifier "for all" include "Let $x \in S$"; "for all $x \in S$"; "for every $x \in S$"; "for each $x \in S$"; etc. Phrases indicating the quantifier "some" (or "there exists") include "for some $x \in S$"; "there exists an $x \in S$"; "for a suitable choice of $x \in S$"; etc.

    On the other hand, don't introduce a variable more than once! Once you have said "Let $x \in S$," the letter x has its meaning defined. You don't *need* to say "for all $x \in S$" again, and you definitely should *not* say "let $x \in S$" again.

18. **Use a symbol to mean only one thing.** Once you use the letter x once, its meaning is fixed for the duration of your proof. You cannot use x to mean anything else.

19. **Don't "prove by example."** Most problems ask you to prove that something is true "for all"—You *cannot* prove this by giving a single example, or even a hundred. Your answer will need to be a logical argument that holds for *every example there possibly could be*.

On the other hand, if the claim that you are trying to prove involves the existence of a mathematical object with a particular property, then providing a specific example is sufficient.

20. **Write "Let $x = \dots$," not "Let $\cdots = x$."** When you have an existing expression, say a^2, and you want to give it a new, simpler name like b, you should write "Let $b = a^2$," which means, "Let the new symbol b mean a^2." This convention makes it clear to the reader that b is the brand-new symbol and a^2 is the old expression he/she already understands.

    If you were to write it backwards, saying "Let $a^2 = b$," then your startled reader would ask, "What if $a^2 \neq b$?"

21. **Make your counterexamples concrete and specific.** Proofs need to be entirely general, but counterexamples should be absolutely concrete. When you provide an example or counterexample, make it as specific as possible. For a set, for example, you must name its elements, and for a function you must give its rule. Do not say things like "θ could be one-to-one but not onto"; instead, provide an actual function θ that *is* one-to-one but not onto.

22. **Don't include examples in proofs.** Including an example very rarely adds anything to your proof. If your logic is sound, then it doesn't need an example to back it up. If your logic is bad, a dozen examples won't help it (see rule 19). There are only two valid reasons to include an example in a proof: if it is a *counterexample* disproving something, or if you are performing complicated manipulations in a general setting and the example is just to help the reader understand what you are saying.

23. **Use scratch paper.** Finding your proof will be a long, potentially messy process, full of false starts and dead ends. Do all that on scratch paper until you find a real proof, and only then break out your clean paper to write your final proof carefully.

    Only sentences that actually contribute to your proof should be part of the proof. Do not just perform a "brain dump," throwing everything you know onto the paper before showing the logical steps that prove the conclusion. *That is what scratch paper is for.*

Appendix B

Fancy Mathematical Terms

Here are some important mathematical terms that you will encounter in this course and throughout your mathematical career.

1. **Definition**—a precise and unambiguous description of the meaning of a mathematical term. It characterizes the meaning of a word by giving all the properties and only those properties that must be true.

2. **Theorem**—a mathematical statement that is proved using rigorous mathematical reasoning. In a mathematical paper, the term theorem is often reserved for the most important results.

3. **Lemma**—a minor result whose sole purpose is to help in proving a theorem. It is a stepping stone on the path to proving a theorem. Very occasionally lemmas can take on a life of their own (Zorn's Lemma, Urysohn's Lemma, Burnside's Lemma, Sperner's Lemma).

4. **Corollary**—a result in which the (usually short) proof relies heavily on a given theorem (we often say that "this is a corollary of Theorem A").

5. **Proposition**—a proved and often interesting result, but generally less important than a theorem.

6. **Conjecture**—a statement that is unproved, but is believed to be true (Collatz Conjecture, Goldbach Conjecture, Twin prime Conjecture).

7. **Claim**—an assertion that is then proved. It is often used like an informal lemma.

8. **Axiom/Postulate**—a statement that is assumed to be true without proof. These are the basic building blocks from which all theorems are proved (Euclid's five postulates, axioms of ZFC, Peano axioms).

9. **Identity**—a mathematical expression giving the equality of two (often variable) quantities (trigonometric identities, Euler's identity).

10. **Paradox**—a statement that can be shown, using a given set of axioms and definitions, to be both true and false. Paradoxes are often used to show the inconsistencies in a flawed axiomatic theory (e.g., Russell's Paradox). The term paradox is also used informally to describe a surprising or counterintuitive result that follows from a given set of rules (Banach-Tarski Paradox, Alabama Paradox, Gabriel's Horn).

Appendix C

Paradoxes

A **paradox** is a statement that can be shown, using a given set of axioms and definitions, to be both true and false. Recall that an axiom is a statement that is assumed to be true without proof. These are the basic building blocks from which all theorems are proved. Paradoxes are often used to show the inconsistencies in a flawed axiomatic theory. The term paradox is also used informally to describe a surprising or counterintuitive result that follows from a given set of rules. In Section 3.2, we encountered two paradoxes:

- The Barber of Seville (Problem 3.20)
- Russell's Paradox (Problem 3.22)

Below are several additional paradoxes that are worth exploring.

1. **Librarian's Paradox.** A librarian is given the unenviable task of creating two new books for the library. Book A contains the names of all books in the library that reference themselves and Book B contains the names of all books in the library that do not reference themselves. But the librarian just created two new books for the library, so their titles must be in either Book A or Book B. Clearly Book A can be listed in Book B, but where should the librarian list Book B?

2. **Liar's Paradox.** Consider the statement: this sentence is false. Is it true or false?

3. **Berry Paradox.** Consider the claim: every natural number can be unambiguously described in fourteen words or less. It seems clear that this statement is false, but if that is so, then there is some smallest natural number which cannot be unambiguously described in fourteen words or less. Let's call it n. But now n is "the smallest natural number that cannot be unambiguously described in fourteen words or less." This is a complete and unambiguous description of n in fourteen words, contradicting the fact that n was supposed not to have such a description. Therefore, all natural numbers can be unambiguously described in fourteen words or less!

4. **The Naming Numbers Paradox.** Consider the claim: every natural number can be unambiguously described using no more than 50 characters (where a character is a–z, 0–9, and a "space"). For example, we can describe 9 as "9" or "nine" or "the square

of the second prime number.” There are only 37 characters, so we can describe at most 37^{50} numbers, which is very large, but not infinite. So the statement is false. However, here is a “proof” that it is true. Let S be the set of natural numbers that can be unambiguously described using no more than 50 characters. For the sake of contradiction, suppose it is not all of $\mathbb{N}$. Then there is a smallest number $t \in \mathbb{N} \setminus S$. We can describe t as: the smallest natural number not in S. Thus t can be described using no more than 50 characters. So $t \in S$, a contradiction.

5. **Euathlus and Protagoras.** Euathlus wanted to become a lawyer but could not pay Protagoras. Protagoras agreed to teach him under the condition that if Euathlus won his first case, he would pay Protagoras, otherwise not. Euathlus finished his course of study and did nothing. Protagoras sued for his fee. He argued:

   If Euathlus loses this case, then he must pay (by the judgment of the court).
   If Euathlus wins this case, then he must pay (by the terms of the contract).
   He must either win or lose this case.
   Therefore Euathlus must pay me.

   But Euathlus had learned well the art of rhetoric. He responded:

   If I win this case, I do not have to pay (by the judgment of the court).
   If I lose this case, I do not have to pay (by the contract).
   I must either win or lose the case.
   Therefore, I do not have to pay Protagoras.

Appendix D

Definitions in Mathematics

It is difficult to overstate the importance of definitions in mathematics. Definitions play a different role in mathematics than they do in everyday life.

Suppose you give your friend a piece of paper containing the definition of the rarely-used word **rodomontade**. According to the Oxford English Dictionary[1] (OED) it is:

> A vainglorious brag or boast; an extravagantly boastful, arrogant, or bombastic speech or piece of writing; an arrogant act.

Give your friend some time to study the definition. Then take away the paper. Ten minutes later ask her to define rodomontade. Most likely she will be able to give a reasonably accurate definition. Maybe she'd say something like, "It is a speech or act or piece of writing created by a pompous or egotistical person who wants to show off how great they are." It is unlikely that she will have quoted the OED word-for-word. In everyday English that is fine—you would probably agree that your friend knows the meaning of the rodomontade. This is because most definitions are *descriptive*. They describe the common usage of a word.

Let us take a mathematical example. The OED[2] gives this definition of *continuous*.

> Characterized by continuity; extending in space without interruption of substance; having no interstices or breaks; having its parts in immediate connection; connected, unbroken.

Likewise, we often hear calculus students speak of a continuous function as one whose graph can be drawn "without picking up the pencil." This definition is descriptive. However, as we learned in calculus, the picking-up-the-pencil description is not a perfect description of continuous functions. This is not a mathematical definition.

Mathematical definitions are *prescriptive*. The definition must prescribe the exact and correct meaning of a word. Contrast the OED's descriptive definition of continuous with the definition of continuous found in a real analysis textbook.

> A function $f : A \to \mathbb{R}$ is **continuous at a point** $c \in A$ if, for all $\varepsilon > 0$, there exists $\delta > 0$ such that whenever $|x-c| < \delta$ (and $x \in A$) it follows that $|f(x)-f(c)| < \varepsilon$. If f

[1] http://www.oed.com/view/Entry/166837
[2] http://www.oed.com/view/Entry/40280

is continuous at every point in the domain A, then we say that f is **continuous on** A.[3]

In mathematics there is very little freedom in definitions. Mathematics is a deductive theory; it is impossible to state and prove theorems without clear definitions of the mathematical terms. The definition of a term must completely, accurately, and unambiguously describe the term. Each word is chosen very carefully and the order of the words is critical. In the definition of continuity changing "there exists" to "for all," changing the orders of quantifiers, changing $<$ to $\leq$ or $>$, or changing $\mathbb{R}$ to $\mathbb{Z}$ would completely change the meaning of the definition.

What does this mean for you, the student? Our recommendation is that at this stage you memorize the definitions word-for-word. It is the safest way to guarantee that you have it correct. As you gain confidence and familiarity with the subject you may be ready to modify the wording. You may want to change "for all" to "given any" or you may want to change $|x-c|<\delta$ to $-\delta < x-c < \delta$ or to "the distance between x and c is less than δ."

Of course, memorization is not enough; you must have a conceptual understanding of the term, you must see how the formal definition matches up with your conceptual understanding, and you must know how to work with the definition. It is perhaps with the first of these that descriptive definitions are useful. They are useful for building intuition and for painting the "big picture." Only after days (weeks, months, years?) of experience does one get an intuitive feel for the ε,δ-definition of continuity; most mathematicians have the "picking-up-the-pencil" definitions in their head. This is fine as long as we know that it is imperfect, and that when we prove theorems about continuous functions in mathematics we use the mathematical definition.

We end this discussion with an amusing real-life example in which a descriptive definition was not sufficient. In 2003 the German version of the game show *Who wants to be a millionaire?* contained the following question: "Every rectangle is: (a) a rhombus, (b) a trapezoid, (c) a square, (d) a parallelogram."

The confused contestant decided to skip the question and left with €4000. Afterward the show received letters from irate viewers. Why were the contestant and the viewers upset with this problem? Clearly a rectangle is a parallelogram, so (d) is the answer. But what about (b)? Is a rectangle a trapezoid? We would describe a trapezoid as a quadrilateral with a pair of parallel sides. But this leaves open the question: can a trapezoid have *two* pairs of parallel sides or must there only be *one* pair? The viewers said two pairs is allowed, the producers of the television show said it is not. This is a case in which a clear, precise, mathematical definition is required.

[3]This definition is taken from page 109 of Stephen Abbott's *Understanding Analysis*, but the definition would be essentially the same in any modern real analysis textbook.