An Introduction to Proof via Inquiry-Based Learning

Dana C. Ernst, PhD
Northern Arizona University

Version Fall 2020

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 **??** and provided an initial draft of Section **??**: 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 **??**: Elements of Style for Proofs. The current version in Appendix **??** is a result of modifications made by myself with some suggestions from David Richeson.

- Rebecca Jayne (Hampden–Sydney College). The current version of Section **??**: 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 **??**: Fancy Mathematical Terms and Appendix **??**: Definitions in Mathematics. In addition, the current version of Chapter **??**: 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 **??**: 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 exercises aimed at solidifying your understanding of the material. Most importantly, you will be asked to make conjectures, produce counterexamples, and prove theorems.

Most items in the notes are labelled with a number. The items labelled as **Definition** and **Example** are meant to be read and digested. However, the items labelled as **Exercise**, **Question**, **Theorem**, **Corollary**, and **Problem** require action on your part. In particular, items labelled as **Exercise** are typically computational in nature and are aimed at improving your understanding of a particular concept. There are very few items in the notes labelled as **Question**, but in each case it should be obvious what is required of you.

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 **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. The items labelled as **Problem** are sort of a mixed bag. In many circumstances, I ask you to provide a counterexample for a statement if it is false or to provide a proof if the statement is true. Usually, I have left it to you to determine the truth value. If the statement for a problem is true, one could relabel it as a theorem.

It is important to point out that there are very few examples in the notes. This is intentional. One of the goals of the items labelled as **Exercise** 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., □ or ■), 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 kick some butt!

> 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've read Chapter **??**, which sets the tone for the work we will begin doing here.

2.1 A Taste of Number Theory

In this section, we will work with the set of integers, $\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$. The purpose of this section is to get started with proving some theorems about numbers and study the properties of $\mathbb{Z}$. Because you are so familiar with properties of the integers, one of the issues that we will bump into knowing which facts about the integers 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. We will likely need to discuss this further as issues arise.

It is important to note that we are diving in head first here. There are going to be some subtle issues that you will bump into and our goal will be to see what those issues are, and then we will take a step back and start again. See what you can do!

Recall that we 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."

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

Definition 2.2. 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 2 while odd numbers do have a remainder." For the remainder of this section, you may assume that every integer is either even or odd but never both.

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

Theorem 2.4. If n is an even integer, then n^2 is an even integer.

Problem 2.5. Prove or provide a counterexample: The sum of an even integer and an odd integer is odd.

Question 2.6. Did Theorem **??** need to come before Problem **??**? Could we have used Problem **??** to prove Theorem **??**? If so, outline how this alternate proof would go. Perhaps your original proof utilized the approach I'm hinting at. If this is true, can you think of a proof that does not rely directly on Problem **??**? Is one approach better than the other?

Problem 2.7. Prove or provide a counterexample: The product of an odd integer and an even integer is odd.

Problem 2.8. Prove or provide a counterexample: The product of an odd integer and an odd integer is odd.

Problem 2.9. Prove or provide a counterexample: The product of two even integers is even.

Definition 2.10. An integer n **divides** the integer m, written $n|m$, if and only if there exists $k \in \mathbb{Z}$ such that $m = nk$. In the same context, we may also write that m **is divisible by** n.

Question 2.11. For integers n and m, how are the following mathematical expressions similar and how are they different?

(a) $m|n$

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

(c) m/n

In this section on number theory, we allow addition, subtraction, and multiplication of integers. In general, division is not allowed since an integer divided by an integer may result in a number that is not an integer. The upshot: don't write $\frac{m}{n}$. 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.

Problem 2.12. Let $n \in \mathbb{Z}$. Prove or provide a counterexample: If 6 divides n, then 3 divides n.

Problem 2.13. Let $n \in \mathbb{Z}$. Prove or provide a counterexample: If 6 divides n, then 4 divides n.

Theorem 2.14. Assume $n, m, a \in \mathbb{Z}$. If $a|n$, then $a|mn$.

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

Corollary 2.15. Assume $n, a \in \mathbb{Z}$. If a divides n, then a divides n^2.

Problem 2.16. Assume $n, a \in \mathbb{Z}$. Prove or provide a counterexample: If a divides n^2, then a divides n.

Theorem 2.17. Assume $n, a \in \mathbb{Z}$. If a divides n, then a divides $-n$.

Theorem 2.18. Assume $n, m, a \in \mathbb{Z}$. If a divides m and a divides n, then a divides $m + n$.

Problem 2.19. Is the converse[1] of Theorem **??** true? That is, is the following statement true?

> Assume $n, m, a \in \mathbb{Z}$. If a divides $m + n$, then a divides m and a divides n.

If the statement is true, prove it. If the statement is false, provide a counterexample.

Once we've 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's no point in reinventing the wheel if we don't have to. Try to use a couple of our previous results to prove the next theorem.

Theorem 2.20. Assume $n, m, a \in \mathbb{Z}$. If a divides m and a divides n, then a divides $m - n$.

Problem 2.21. Assume $a, b, m \in \mathbb{Z}$. Determine whether the following statement holds sometimes, always, or never.

> If ab divides m, then a divides m and b divides m.

Justify with a proof or counterexample.

Theorem 2.22. If $a, b, c \in \mathbb{Z}$ such that a divides b and b divides c, then a divides c.

The previous theorem is referred to as **transitivity of division of integers**.

Theorem 2.23. The sum of any three consecutive integers is always divisible by three.

2.2 Introduction to Logic

After diving in head first in the last section, we'll take a step back and do a more careful examination of what it is we are actually doing.

Definition 2.24. A **proposition** (or **statement**) is a sentence that is either 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.

Exercise 2.25. Determine whether the following are propositions or not. Explain.

[1] See Definition **??** for the formal definition of converse.

(a) All cars are red.

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

(c) $x^2 = 4$.

(d) There exists an 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 2.26. Let A and B be propositions.

(a) The proposition "**not** A" is true if and only if[2] A is false; expressed symbolically as $\boxed{\neg A}$ and called the **negation** of A.

(b) The proposition "A **and** B" is true if and only 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 and only 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 and only if both A and B are true, or A is false; expressed symbolically as $\boxed{A \implies B}$ and called an **implication** or **conditional statement**. Note that $A \implies B$ may also be read as "A implies B" or "A only if B".

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

Exercise 2.27. Reword Theorem **??** so that it explicitly reads as a conditional statement.

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

Skeleton Proof 2.28 (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.

[2]Throughout mathematics, the phrase "if and only if" is common enough that it is sometimes abbreviated "iff." Roughly speaking, this phrase/word means "exactly when."

Proof. Assume A.

... [Use definitions and known results to derive B] ...

Therefore, B. □

Exercise 2.29. Describe the meaning of $\neg(A \wedge B)$ and $\neg(A \vee B)$.

Exercise 2.30. Let A represent "6 is an even number" and B represent "6 is a multiple of 4." Express each of the following in ordinary English sentences and state whether the statement is true or false.

(a) $A \wedge B$

(b) $A \vee B$

(c) $\neg A$

(d) $\neg B$

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

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

(g) $A \implies B$

Definition 2.31. A **truth table** is a table that illustrates all possible truth values for a proposition.

Example 2.32. Let A and B be propositions. Then the truth table for the conjunction $A \wedge B$ is given by the following.

A	B	$A \wedge B$
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 for A and B. The third column gives us the truth value of $A \wedge B$ given the possible truth values for A and B.

Note that each proposition has two possible truth values: true or false. Thus, if a compound proposition P is built from n propositions, then the truth table for P will require 2^n rows.

Exercise 2.33. Create a truth table for each of $A \vee B$, $\neg A$, $\neg(A \wedge B)$, and $\neg A \wedge \neg B$. Feel free to add additional columns to your tables to assist you with intermediate steps.

Problem 2.34. A coach promises, "If we win tonight, then I will buy you pizza tomorrow." Determine the case(s) in which the players can rightly claim to have been lied to. Use this to help create a truth table for $A \implies B$.

Definition 2.35. Two statements P and Q are (**logically**) **equivalent**, expressed symbolically as $\boxed{P \iff Q}$ and read "P if and only if Q", if and only if they have the same truth table.

Each of the next three facts can be justified using truth tables.

Theorem 2.36. If A is a proposition, then $\neg(\neg A)$ is equivalent to A.

Theorem 2.37 (DeMorgan's Law)**.** If A and B are propositions, then $\neg(A \wedge B) \iff \neg A \vee \neg B$.

Problem 2.38. Let A and B be propositions. Conjecture a statement similar to Theorem **??** for the proposition $\neg(A \vee B)$ and then prove it. This is also called DeMorgan's Law.

Definition 2.39. The **converse** of $A \implies B$ is $B \implies A$.

Exercise 2.40. Provide an example of a true conditional proposition whose converse is false.

Definition 2.41. The **inverse** of $A \implies B$ is $\neg A \implies \neg B$.

Exercise 2.42. Provide an example of a true conditional proposition whose inverse is false.

Definition 2.43. The **contrapositive** of $A \implies B$ is $\neg B \implies \neg A$.

Exercise 2.44. Let A and B represent the statements from Exercise **??**. Express the following in ordinary English sentences.

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

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

Exercise 2.45. Find the converse and the contrapositive of the following statement: "If a person lives in Flagstaff, then that person lives in Arizona."

Use a truth table to prove the following theorem.

Theorem 2.46. The implication $A \implies B$ is equivalent to its contrapositive.

The upshot of Theorem **??** is that if you want to prove a conditional proposition, you can prove its contrapositive instead, called **proof by contraposition**.

Skeleton Proof 2.47 (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. We will prove that if A, then B by proving its contrapositive. Assume $\neg B$.

... [Use definitions and known results to derive $\neg A$] ...

This proves that if $\neg B$, then $\neg A$. Therefore, if A, then B. □

Problem 2.48. Consider the following statement:

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

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. Thus, we 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. Since the contrapositive is equivalent to the original statement and we have proved the contrapositive, the original statement is true.
8. By the definition of even integer, x^2 is an even integer.
9. The contrapositive is "If x is an even integer, then x^2 is an even integer."
10. Notice that $x^2 = 2(2k^2)$.

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

Theorem 2.49. Assume $x \in \mathbb{Z}$. If x^2 is even, then x is even.

Theorem 2.50. Assume $x, y \in \mathbb{Z}$. If xy is odd, then both x and y are odd.

Theorem 2.51. 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 $A \implies B$. To begin, try proving the following result with a truth table.

Theorem 2.52. The implication $A \implies B$ is equivalent to the disjunction $\neg A \vee B$.

The next result follows quickly from Theorem **??** together with DeMorgan's Law.

Corollary 2.53. The proposition $\neg(A \implies B)$ is equivalent to $A \wedge \neg B$.

Exercise 2.54. Let A and B be the propositions "Darth Vader is a hippie" and "Sarah Palin is a liberal," 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."

Exercise 2.55. The proposition "If $.\overline{99} = \frac{9}{10} + \frac{9}{100} + \frac{9}{1000} + \cdots$, then $.\overline{99} \neq 1$" is *false*. Write its (true) negation, as a conjunction.

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

Definition 2.56. A compound proposition that is always false is called a **contradiction**. A compound proposition that is always true is called a **tautology**.

Theorem 2.57. For any proposition A, the proposition $\neg A \wedge A$ is a contradiction.

Exercise 2.58. 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 2.59 (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.* 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 equivalent to $A \wedge \neg B$ (see Corollary **??**).

Skeleton Proof 2.60 (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.* 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. □

Establish the following theorem in two ways: (i) prove the contrapositive, and (ii) prove via contradiction.

Theorem 2.61. Assume that $x \in \mathbb{Z}$. If x is odd, then 2 does not divide x. (Prove in two different ways.)

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

Theorem 2.62. Assume that $x, y \in \mathbb{N}$.[3] If x divides y, then $x \leq y$.

2.4 Introduction to Quantification

The sentence "$x > 0$" is not itself a proposition because x is a **free variable**. A sentence with a free variable is a **predicate**. To turn a predicate into a proposition, we must either substitute values for each free variable, or else "quantify" the free variables.

Function notation is a convenient way to represent predicates. 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"

The notation := indicates a definition. Also, note that the use of the quotation marks above removed 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 "$x^2 - 4 = 0$".

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).

Exercise 2.63. 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? Explain.

[3] $\mathbb{N} = \{1, 2, 3, \ldots\}$ is the set of **natural numbers**. Some mathematicians (set theorists, in particular) include 0 in $\mathbb{N}$, but this will not be our convention. The given statement is not true if we replace $\mathbb{N}$ with $\mathbb{Z}$. Do you see why?

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.

Exercise 2.64. 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 $x \in \mathbb{R}$, $x^2 - 4 = 0$.[4]

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

Definition 2.65. "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."

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 universe 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 set of acceptable values for a variable is called the **universe (of discourse)**.

Exercise 2.66. 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!*

Exercise 2.67. 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 exercise illustrates that at least some of the possibilities listed in the previous exercise are *not* equivalent to each other.

Exercise 2.68. Suppose the universe of discourse is the set of people. Consider the predicate $M(x, y) :=$ "x is married to y". Discuss the meaning of each of the following.

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

(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 $M(x, y)$.

Exercise 2.69. Consider the predicate $F(x, y) :=$ "$x = y^2$". Discuss the meaning of each of the following.

(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 $y \in \mathbb{R}$, for all $x \in \mathbb{R}$, $F(x, y)$.

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 "Let $x \in \ldots$" bind the variable x and remove ambiguity.

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, the formal definition of $\lim_{x \to c} f(x) = L$ 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 2.70. 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 "$(\forall x \in \mathbb{N})(\exists y \in \mathbb{N})(y < x)$."

Exercise 2.71. 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 a number 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 real number x, x^2 is greater than or equal to zero.

Exercise 2.72. Express the formal definition of a limit (given above Definition **??**) in logical symbols.

If $A(x)$ and $B(x)$ are predicates, then it is standard practice for 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). In this case, we say that the universal quantifier is implicit.

Exercise 2.73. 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 replaced with the simpler expression $(\forall x, y)$ as long as x and y are elements of the same universe.

Exercise 2.74. 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.

Exercise 2.75. Rewrite the following statements in words and determine whether each 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…." 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

Mathematical proofs 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 will provide us with a way to talk about the meta-concepts surrounding the construction of proofs.

Definition 2.76. Two quantified propositions are **equivalent in a given universe of discourse** if and only if they have the same truth value in that universe. Two quantified propositions are **equivalent** if and only if they are equivalent in every universe of discourse.

Exercise 2.77. Consider the propositions $(\exists x)(x^2 - 4 = 0)$ and $(\exists x)(x^2 - 2 = 0)$.

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

(b) Give two different universes of discourse that yield different truth values for these propositions.

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

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 equivalent. For example, $(\forall x)(P(x) \implies Q(x))$ is 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 tell us how to negate logical forms involving quantifiers.

Theorem 2.78. Let $P(x)$ be a predicate. Then

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

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

Exercise 2.79. Negate each of the following. 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) For all $x \in \mathbb{N}$, $x^2 + x + 41$ is prime.

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

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

Using Theorem **??** 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 equivalent to $(\forall x \in \mathbb{R})(\exists y \in \mathbb{R})(x + y \neq 0)$.

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 equivalent to $(\exists x)[x > 0 \wedge \neg(\exists y)(y < 0 \wedge xy > 0)]$, which happens to be equivalent to $(\exists x)[x > 0 \wedge (\forall y)(y \geq 0 \vee xy \leq 0)]$. Can you identify the previous theorems that were used when negating this proposition?

Exercise 2.80. Negate each of the following. Disregard the truth value and the universe of discourse.

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

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

(c) For all positive real numbers x, there exists a real number y such that $y^2 = x$.

(d) 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 2.81 (Direct Proof of $(\forall x)P(x)$)**.** Here is the general structure for a direct proof of the proposition $(\forall x)P(x)$.

Proof. Let $x \in U$. *[U is the universe of discourse]*

... [Use definitions and known results.] ...

Therefore, $P(x)$ is true. Since x was arbitrary, for all x, $P(x)$. □

Skeleton Proof 2.82 (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.

Proof. For sake of a contradiction, assume that there exists $x \in U$ such that $\neg P(x)$. *[U is the universe of discourse]*

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

This is a contradiction. Therefore, for all x, $P(x)$ is true. □

Skeleton Proof 2.83 (Direct Proof of $(\exists x)P(x)$)**.** Here is the general structure for a direct proof of the proposition $(\exists x)P(x)$.

> *Proof. … [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 such that $P(x)$. □

Skeleton Proof 2.84 (Proof of $(\exists x)P(x)$ by Contradiction)**.** Here is the general structure for a proof of the proposition $(\exists x)P(x)$ via contradiction.

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

Note that if $Q(x)$ is a proposition for which $(\forall x)Q(x)$ is false, then a counterexample to this proposition amounts to showing $(\exists x)(\neg Q(x))$, which might be proved via the third scenario above.

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 such that $P(x)$ and $\neg Q(x)$.

Problem 2.85. 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 2.86. 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 $x \in A$. Otherwise, we write $x \notin A$. The set containing no elements is called the **empty set**, and is denoted by the symbol $\emptyset$.

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, $A \notin A$.

Definition 3.2. 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.

- **Real Numbers:** $\mathbb{R}$ denotes the set of real numbers.
- **Integers:** $\mathbb{Z} := \{0, \pm 1, \pm 2, \pm 3, \ldots\}$
- **Natural numbers:** $\mathbb{N} := \{1, 2, 3, \ldots\}$. Since this set consists of the positive integers, the natural numbers are sometimes denoted by $\mathbb{Z}^+$. Some books will include zero in the set of natural numbers, but we will not do that.

- **Rational Numbers:** $\mathbb{Q} := \{a/b \mid a, b \in \mathbb{Z} \text{ and } b \neq 0\}$.

Exercise 3.3. 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) $D = \{m \in \mathbb{R} \mid m = 1 - \frac{1}{n}, \text{ where } n \in \mathbb{N}\}$

Exercise 3.4. 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 3.5. 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 also 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 3.6. Suppose A and B are sets. Describe a skeleton proof for proving that $A \subseteq B$.

Every set always has two rather boring subsets.

Theorem 3.7. Let S be a set. Then

(a) $S \subseteq S$ (b) $\emptyset \subseteq S$.

Exercise 3.8. List all of the subsets of $A = \{1, 2, 3\}$.

Theorem 3.9 (Transitivity of subsets)**.** Suppose that A, B, and C are sets. If $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C$.

Definition 3.10. 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]

The following definitions should look familiar from precalculus.

Definition 3.11 (Interval Notation)**.** For $a, b \in \mathbb{R}$ with $a < b$, we define the following.

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

(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 $(-\infty,b]$.

Definition 3.12. 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 3.13. If two sets A and B have the property that $A \cap B = \emptyset$, then we say that A and B are **disjoint** sets.

Exercise 3.14. 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) $A^c \cap B^c$

Exercise 3.15. 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 3.16. Let A and B be sets. If $A \subseteq B$, then $B^c \subseteq A^c$.

Definition 3.17. 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.

Theorem 3.18. 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 3.19 (DeMorgan's Law)**.** Let A and B be sets. Then

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

Theorem 3.20 (Distribution of Union and Intersection)**.** Let A, B, and C be sets. Then

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

3.2 Power Sets and Paradoxes

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 3.21. 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 $\mathcal{P} = \{\emptyset, \{a\}, \{b\}, S\}$.

Exercise 3.22. For each of the following sets, find the power set.

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

(b) $B = \{a, \{a\}\}$ (d) $D = \{\emptyset\}$

Conjecture 3.23. 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 Exercise **??**. 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 3.24. Let S and T be sets. Then $S \subseteq T$ if and only if $\mathcal{P}(S) \subseteq \mathcal{P}(T)$.[2]

Theorem 3.25. Let S and T be sets. Then $\mathcal{P}(S) \cap \mathcal{P}(T) = \mathcal{P}(S \cap T)$.

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

Theorem 3.26. Let S and T be sets. Then $\mathcal{P}(S) \cup \mathcal{P}(T) \subseteq \mathcal{P}(S \cup T)$.

Problem 3.27. 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 **??** 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?

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

Problem **??** is an example of a **paradox**. What do you think paradox means? 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 3.29. 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 3.30. 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**. Okay, 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 is not a set itself.

Problem 3.31. Pick any two of the paradoxes below and for each one explain why it is a paradox.

(a) **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?

(b) **Liar's Paradox.** Consider the statement: this sentence is false. Is it true or false?

(c) **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!

(d) **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.

(e) **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.

3.3 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:

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

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 3.32. 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 "$\cap$").

Exercise 3.33. 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) $\displaystyle\bigcup_{n\in\mathbb{N}} I_n$ (b) $\displaystyle\bigcap_{n\in\mathbb{N}} I_n$

Exercise 3.34. Let $\{A_n\}_{n=1}^{26}$ be the collection from earlier in the section. Find each of the following.

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

Exercise 3.35. Let $S_n = \{x \in \mathbb{R} \mid n-1 < x < n\}$, where $n \in \mathbb{N}$. Find each of the following.

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

Exercise 3.36. 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) $\displaystyle\bigcup_{n=1}^{\infty} T_n$ (b) $\displaystyle\bigcap_{n=1}^{\infty} T_n$

Exercise 3.37. 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) $\displaystyle\bigcup_{r\in\mathbb{Q}} N_r$ (b) $\displaystyle\bigcap_{r\in\mathbb{Q}} N_r$

Definition 3.38. A collection of sets $\{A_\alpha\}_{\alpha\in\Delta}$ is **pairwise disjoint** if $A_\alpha \cap A_\beta = \emptyset$ for $\alpha \neq \beta$.

Exercise 3.39. Draw a Venn diagram of a collection of 3 sets that are pairwise disjoint.

Exercise 3.40. 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 3.41 (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) $B \cup \left(\bigcap_{\alpha \in \Delta} A_\alpha \right) = \bigcap_{\alpha \in \Delta} (B \cup A_\alpha)$, (b) $B \cap \left(\bigcup_{\alpha \in \Delta} A_\alpha \right) = \bigcup_{\alpha \in \Delta} (B \cap A_\alpha)$.

Theorem 3.42 (Generalized DeMorgan's Law)**.** Let $\{A_\alpha\}_{\alpha \in \Delta}$ be a collection of sets. Then

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

3.4 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 3.43. If p and q are two different real numbers in $\mathbb{R}$, then there is a number between them.

Exercise 3.44. 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 exercise is asking you to produce an actual candidate.

Axiom 3.45. (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 3.46. If p is a real number, then there exists $q, r \in \mathbb{R}$ such that $q < p < r$.

Axiom 3.47. (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 3.48. 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 $a < b$.

Exercise 3.49. 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 3.50. 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 3.51. Prove that the set $I = (1, 2)$ is an open set.

Theorem 3.52. Every open interval is an open set.

Theorem 3.53. The set of real numbers forms an open set.

Exercise 3.54. Provide an example of an open set that is not a single open interval.

Theorem 3.55. Every closed interval is not an open set.

Theorem 3.56. If $x \in \mathbb{R}$, then the set $\{x\}$ is not open.

Exercise 3.57. Determine whether $\{4, 17, 42\}$ is an open set. Briefly justify your assertion.

Theorem 3.58. Let A and B be open sets. Then

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

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

Theorem 3.59. Let $\{U_\alpha\}_{\alpha\in\Delta}$ be a collection of open sets. Then $\bigcup_{\alpha\in\Delta} U_\alpha$ is an open set.

Exercise 3.60.

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

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

Remark 3.61. Taken together, Theorems **??–??** and Exercise **??** 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.

Exercise 3.62. 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 3.63. 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 3.64. 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 3.65. A point p is a limit point of (a, b) if and only if $p \in [a, b]$.

Problem 3.66. Prove that the point $p = 0$ is a limit point of $S = \{\frac{1}{n} : n \in \mathbb{N}\}$. Are there any other limit points?

Exercise 3.67. Provide an example of a set S such that 1 is a limit point of S, $1 \neq S$, and S contains no intervals.

Exercise 3.68. Provide an example of a set T with exactly two limit points.

Theorem 3.69. If $p \in \mathbb{R}$, then p is a limit point of $\mathbb{Q}$.

Definition 3.70. A set is called **closed** if and only if it contains all of its limit points.

Exercise 3.71. 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 3.72. The set $[a, b]$ is closed.

Theorem 3.73. The set U is open if and only if U^C is closed.

Theorem 3.74. Every finite set is closed.

Problem 3.75. Prove or provide a counterexample: If a set S is not open, then it is closed.

Theorem 3.76. The set of real numbers is both open and closed.

Theorem 3.77. The set of rational numbers is neither open nor closed.

Theorem 3.78. The empty set is both open and closed.

Theorem 3.79. Let $\{A_\alpha\}_{\alpha \in \Delta}$ be a collection of closed sets. Then $\bigcap_{\alpha \in \Delta} A_\alpha$ is a closed set.

Problem 3.80. Prove or provide a counterexample: If A and B are closed sets, then $A \cup B$ is also closed.

Exercise 3.81. 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.

Remark 3.82. You should compare what happened in Theorem **??** and Exercise **??** to what we stated in Remark **??**.

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't actually true. We need a rigorous way of capturing "and so on" and a way to verify whether it really is "and so on."

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 $S = \mathbb{N}$.

Recall that an axiom is a basic mathematical assumption. That is, we are assuming that the Axiom of Induction is true, which I'm hoping that you can agree is a pretty reasonable assumption. We can think of the first hypothesis as saying that we have a first rung of a ladder. The second hypothesis says that if we have 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.

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** 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.

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 the PMI, $P(n)$ is true for all $n \in \mathbb{N}$. □

Prove the next few theorems using induction.

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

[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 $\mathbb{N}$.

[3] Recall that $\displaystyle\sum_{i=1}^{n} i = 1 + 2 + 3 + \cdots + n$, by definition. Also, this theorem should look familiar from calculus.

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 **??** depicts one possible covering for the case involving $n = 2$.

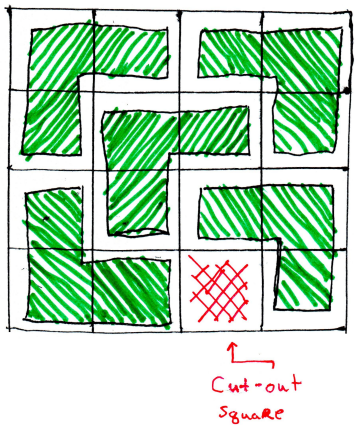

Figure 4.1: One possible covering for the case involving $n = 2$ for Problem **??**.

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 **??** 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

(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 **??** 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 the PMI, $P(n)$ is true for all integers $n \geq a$. □

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 $6 \cdot 7^n - 2 \cdot 3^n$.

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.

[4] *Hint:* Mimic the proof of Theorem **??**, 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 **??** (see Conjecture **??**), 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 4.21. 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.

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

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, a formula for $S(n)$ which may involve some of the previous terms $\{S(n-1), S(n-2), \ldots\}$. (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 **??** and **??**) 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 the PCMI, $P(n)$ is true for all integers $n \geq a$. □

Recall that Theorem **??** generalized Theorem **??** 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 **??**) and the Axiom of Induction (Axiom **??**) 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**.

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

Exercise 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 **??** 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 **??**). To prove Euclid's Lemma, we will utilize a special case of Bezout's Lemma (Lemma **??**), 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 **??**) 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.

Exercise 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 $\gcd(m, n)$, 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**.

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

Exercise 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 **??**), which we then use to prove uniqueness for the Fundamental Theorem of Arithmetic (Theorem **??**).

[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 **??**), 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]

Exercise 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 **??**. 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 **??**.

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 be 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 **??**). 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 **??**), 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 **??** 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 **??**, 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 **??**).

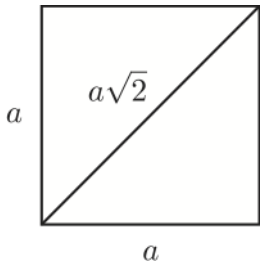

Figure 5.1: The side and diagonal of a square are incommensurable.

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 **??** 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 **??** 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 **??**.

5.3 The Infinitude of Primes

The highlight of this section is Theorem **??**, 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 **??**, 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

6.1 Introduction to Relations

Definition 6.1. An **ordered pair** is an object of the form (x, y). Two ordered pairs (x, y) and (a, b) are **equal** if and only if $x = a$ and $y = b$.

Definition 6.2. An n-**tuple** is an object of the form $(x_1, x_2, \ldots, x_n)$. Each x_i is referred to as the ith **component**.

Note that an ordered pair is just a 2-tuple.

Definition 6.3. If X and Y are sets, the **Cartesian product** of X and Y is defined by

$$X \times Y = \{(x, y) \mid x \in X, y \in Y\}.$$

That is, $X \times Y$ is the set of all ordered pairs where the first element is from X and the second element is from Y. The set $X \times X$ is sometimes denoted by X^2. We similarly define the Cartesian product of n sets, say $X_1, \ldots, X_n$, by

$$\prod_{i=1}^{n} X_i = X_1 \times \cdots \times X_n = \{(x_1, \ldots, x_n) \mid \text{each } x_i \in X_i\}.$$

Example 6.4. Let $A = \{a, b, c\}$ and $B = \{☺, ☹\}$. Then

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

Exercise 6.5. Using the sets A and B from the previous example, find $B \times A$.

Exercise 6.6. Using the set B from the previous examples, find $B \times B$.

Exercise 6.7. What general conclusion can you make about $X \times Y$ versus $Y \times X$? When will they be equal?

Exercise 6.8. If X and Y are both finite sets, then how many elements will $X \times Y$ have? Be as specific as possible.

Exercise 6.9. Let $A = \{1, 2, 3\}$, $B = \{1, 2\}$, and $C = \{1, 3\}$. List the elements of the set $A \times B \times C$.

Exercise 6.10. Let $A = \mathbb{N}$ and $B = \mathbb{R}$. Describe the elements of the set $A \times B$.

Exercise 6.11. Let A be the set of all differentiable functions on the open interval $(0, 1)$, and let B equal the set of all derivatives of functions in A evaluated at $x = \frac{1}{2}$. Describe the elements of the set $A \times B$.

Exercise 6.12. Three space, $\mathbb{R}^3$, is a Cartesian product. Unpack the meaning of $\mathbb{R}^3$ using the Cartesian product, and write the complete set notation version.

Exercise 6.13. Let $X = [0, 1]$ and let $Y = \{1\}$. Describe geometrically (e.g., draw a picture) what $X \times Y$, $Y \times X$, $X \times X$, and $Y \times Y$ look like.

Definition 6.14. Let X and Y be sets. A **relation** from a set X to a set Y is a subset of $X \times Y$. A relation on X is a subset of $X \times X$.

Example 6.15. You may not realize it, but you are familiar with many relations. For example, on the real numbers, we have the relation $\leq$. We could say that $(3, \pi)$ is in the relation $\leq$ since $3 \leq \pi$. However, $(1, -1)$ is not in the relation since $1 \not\leq -1$. Order matters!

Different notations for relations are used in different contexts. When talking about relations in the abstract, we indicate that a pair (a, b) is in the relation by some notation like $a \sim b$, which is read "a is related to b."

Example 6.16. Let P_f denote the set of all people with accounts on Facebook. Define F via xFy if and only if x is friends with y. Then F is a relation on P_f.

We can often represent relations using graphs or digraphs. Given a finite set X and a relation $\sim$ on X, a **digraph** (short for *directed graph*) is a discrete graph having the members of X as vertices and a directed edge from x to y if and only if $x \sim y$.

Example 6.17. Figure **??** depicts a digraph that represents a relation R given by

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

Exercise 6.18. Let $A = \{a, b, c\}$ and define $\sim = \{(a, a), (a, b), (b, c), (c, b), (c, a)\}$. Draw the digraph for $\sim$.

Exercise 6.19. Let $A = \{1, 2, 3, 4, 5, 6\}$. Define $|$ on A via $x|y$ if and only if x divides y. Draw the digraph for $|$ on A.

When X or Y is infinite, it is not practical to draw a digraph. However, you are familiar with the graphs of some relations involving infinite sets.

Example 6.20. 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 $x^2 + y^2 = 1$. In set notation:

$$\{(x, y) \mid x^2 + y^2 = 1\}$$

The graph of this relation in $\mathbb{R}^2$ is the standard unit circle.

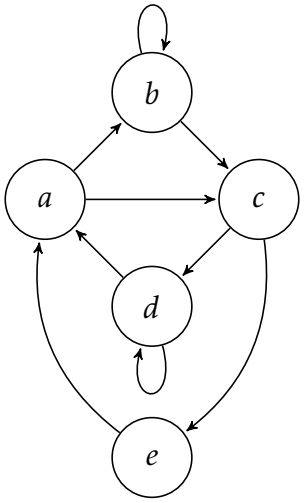

Figure 6.1: An example of a digraph for a relation.

Exercise 6.21. Define $\sim$ on $\mathbb{R}$ via $x \sim y$ if and only if $x \leq y$. Draw a picture of this relation in $\mathbb{R}^2$. In other words, draw all points (x, y) where $x \sim y$.

Definition 6.22. Let $\sim$ be a relation on a set A.

(a) $\sim$ is **reflexive** if for all $x \in A$, $x \sim x$ (every element is related to itself).

(b) $\sim$ is **symmetric** if for all $x, y \in A$, if $x \sim y$, then $y \sim x$.

(c) $\sim$ is **transitive** if for all $x, y, z \in A$, if $x \sim y$ and $y \sim z$, then $x \sim z$.

Example 6.23.

(a) $\leq$ on $\mathbb{R}$ is reflexive and transitive, but not symmetric. $<$ on $\mathbb{R}$ is transitive, but not symmetric and not reflexive.

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

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

Exercise 6.24. Given a finite set A and a relation $\sim$, describe what each of reflexive, symmetric, and transitive look like in terms of a digraph. That is, draw a picture that represents reflexive, symmetric, and transitive.

Exercise 6.25. Let P be the set of people at a party and define N via $(x, y) \in N$ if and only if x knows the name of y. Describe what it would mean for N to be reflexive, symmetric, and transitive.

Exercise 6.26. Determine whether each of the following relations is reflexive, symmetric, or transitive.

(a) Let P_f denote the set of all people with accounts on Facebook. Define F via xFy if and only if x is friends with y.

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

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

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

(e) 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.

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

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

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

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

6.2 Equivalence Relations

Let $\sim$ be a relation on a set A. Recall the following definitions:

(a) $\sim$ is **reflexive** if for all $x \in A$, $x \sim x$ (every element is related to itself).

(b) $\sim$ is **symmetric** if for all $x, y \in A$, if $x \sim y$, then $y \sim x$.

(c) $\sim$ is **transitive** if for all $x, y, z \in A$, if $x \sim y$ and $y \sim z$, then $x \sim z$.

As we've seen in the previous section of notes, these conditions are independent. That is, a relation may have some combination of these properties, but not necessarily all of them. However, we have a special name for when a relation does satisfy all three.

Definition 6.27. Let $\sim$ be a relation on a set A. Then $\sim$ is called an **equivalence relation** if and only if $\sim$ is reflexive, symmetric, and transitive.

Exercise 6.28. Given a finite set A and a relation $\sim$ on A, describe what the corresponding digraph would have to look like in order for $\sim$ to be an equivalence relation.

Exercise 6.29. Let $A = \{a, b, c, d, e\}$. Make up an equivalence relation on A by drawing a digraph such that a is not related to b and c is not related to b.

Exercise 6.30. Let $S = \{1, 2, 3, 4, 5, 6\}$ and define

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

Justify that this is an equivalence relation.

Exercise 6.31. Determine which of the following are equivalence relations. Some of these occurred in the last section of notes and you are welcome to use your answers from those problems.

(a) Let P_f denote the set of all people with accounts on Facebook. Define F via xFy if and only if x is friends with y.

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

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

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

(e) 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.

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

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

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

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

(i) Define $\sim$ on $\mathbb{Z}$ via $a \sim b$ if and only if $a-b$ is a multiple of 5.

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

(k) Define $\sim$ on $\mathbb{R}$ via $x \sim y$ 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 $\lfloor 4 \rfloor = 4$).

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

Definition 6.32. Let $\sim$ be a relation on a set A (not necessarily an equivalence relation) and let $x \in A$. Then we define the **set of relatives of x with respect to** $\sim$ via

$$[x]_\sim = \{y \in A \mid x \sim y\}.$$

We also define

$$\Omega_\sim = \{[x] \mid x \in A\}.$$

If $\sim$ is clear from the context, we will often write $[x]$ in place of $[x]_\sim$. Another common notation for the set of relatives of x is $\overline{x}$. Notice that $\Omega_\sim$ is a set of sets. In particular, an element in $\Omega_\sim$ is a subset of A—equivalently, an element of $\mathcal{P}(A)$.

Exercise 6.33. Let P_f and F be as in part **??** of Exercise **??**. Describe [Bob] (assume you know which Bob we're talking about). What is Ω_F?

Exercise 6.34. Using your digraph in Exercise **??**, find $\Omega_\sim$.

Exercise 6.35. Consider the relation $\leq$ on $\mathbb{R}$. If $x \in \mathbb{R}$, what is $[x]$?

Exercise 6.36. Find $[1]$ and $[2]$ for the relation given in part **??** of Exercise **??**. How many different sets of relatives are there? What are they?

Exercise 6.37. Find $[x]$ for all $x \in S$ for S and $\sim$ from Exercise **??**. Any observations?

Theorem 6.38. Suppose $\sim$ is an equivalence relation on a set A and let $a, b \in A$. Then $[a] = [b]$ if and only if $a \sim b$.

Theorem 6.39. Suppose $\sim$ is an equivalence relation on a set A. Then

(a) $\bigcup_{x \in A} [x] = A$, and

(b) For all $x, y \in A$, either $[x] = [y]$ or $[x] \cap [y] = \emptyset$.

In light of Theorem **??**, we have the following definition.

Definition 6.40. If $\sim$ is an equivalence relation on a set A, then we refer to each $[x]$ as the **equivalence class** of x.

When $\sim$ is an equivalence relation on a set A, the collection of equivalence classes is denoted by $A/\sim$, which is read as "A modulo $\sim$" or "A mod $\sim$". The collection $A/\sim$ is sometimes referred to as the **quotient set of** A **by** $\sim$. Note that $\Omega_\sim$ equals $A/\sim$ whenever $\sim$ is an equivalence relation.

The upshot of Theorem **??** is that given an equivalence relation, every element lives in exactly one equivalence class. We'll see in the next section of notes 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 (like the bins of my kid's toys), then this determines an equivalence relation. More on this later.

Example 6.41. The collection of sets of relatives that you found in part **??** of Exercise **??** is the set of equivalence classes modulo 5.

Exercise 6.42. If $\sim$ is an equivalence relation on a finite set A, then what is the connection between the equivalence classes and the corresponding digraph?

Exercise 6.43. For each of the equivalence relations in Exercise **??**, describe the equivalence classes as best as you can.

6.3 Partitions

Theorems **??** and **??** 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 $a \in A$. Furthermore, each pair of elements in the same set of relatives are related via $\sim$.

As you've probably already noticed, equivalence relations are intimately related to the following concept.

Definition 6.44. 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) Given $X, Y \in \Omega$, either $X = Y$ or $X \cap Y = \emptyset$, and

(c) $\bigcup_{X \in \Omega} X = A$.

That is, the elements of Ω are pairwise disjoint and their union is all of A.

Notice that in the second condition of Definition **??**, we cannot have both $X = Y$ and $X \cap Y = \emptyset$ at the same time.

Example 6.45. The following are all examples of partitions of the given set. Perhaps you can find exceptions in these examples, but please take them at face value.

(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 6.46. Let $A = \{a, b, c, d, e, f\}$ and $\Omega = \{\{a\}, \{b, c, d\}, \{e, f\}\}$. Then Ω is a partition of A since the elements of Ω are nonempty subsets of A, pairwise disjoint, and their union is all of A.

Exercise 6.47. Consider the set A from Example **??**.

(a) Find a partition of A that has 4 subsets in the partition.

(b) Find a collection of subsets of A that does *not* form a partition.

Exercise 6.48. Find a partition of $\mathbb{N}$ that consists of 3 subsets, where one of the sets is finite and the remaining two sets are infinite.

Exercise 6.49. Let P be the set of prime numbers, N be the set of odd natural numbers that are not prime, and E be the set of even natural numbers. Explain why this is not a partition of $\mathbb{N}$.

The next theorem spells out half of the close connection between partitions and equivalence relations. Hopefully you were anticipating this.

Theorem 6.50. Let $\sim$ be an equivalence relation on a set A. Then $\Omega_\sim$ forms a partition of A.

Exercise 6.51. 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 $\Omega_\sim$.

It turns out that we can reverse the situation, as well. That is, given a partition, we can form an equivalence relation. Before proving this, we need a definition.

Definition 6.52. Let A be a set and Ω any collection of subsets of A (not necessarily a partition). If $a, b \in A$, we will define a to be Ω-related to b if there exists an $R \in \Omega$ that contains both a and b. This relation is denoted by $\sim_\Omega$ and is called the **relation on** A **associated to** Ω.

This definition may look more awkward than the actual underlying concept. The idea is that if two elements are in the same subset, then they are related. For example, when my kids pick up all their toys and put them in the appropriate toy bins, we say that two toys are related if they are in the same bin.

Notice that we have two notations that look similar: $\Omega_\sim$ and $\sim_\Omega$.

(a) $\Omega_\sim$ is the collection of subsets of A determined by the relation $\sim$.

(b) $\sim_\Omega$ is the relation determined by the collection of subsets Ω.

Exercise 6.53. Let $A = \{a,b,c,d,e,f\}$ and let $\Omega = \{X_1, X_2, X_3\}$, where $X_1 = \{a,c\}$, $X_2 = \{b,c\}$, and $X_3 = \{d,f\}$. List the elements of $\sim_\Omega$ by listing ordered pairs or drawing a digraph.

Exercise 6.54. Let A and Ω be as in Example **??**. List the elements of $\sim_\Omega$ by listing ordered pairs or drawing a digraph.

Theorem 6.55. Let A be a set and let Ω be a collection of subsets of A (not necessarily a partition). Then $\sim_\Omega$ is symmetric.

Exercise 6.56. Give an example of a set A and a collection Ω from $\mathcal{P}(A)$ such that the relation $\sim_\Omega$ is not reflexive.

Theorem 6.57. Let A be a set and let Ω be a collection of subsets of A (not necessarily a partition). If

$$\bigcup_{R \in \Omega} R = A,$$

then $\sim_\Omega$ is reflexive.

Theorem 6.58. Let A be a set and let Ω be a collection of subsets of A (not necessarily a partition). If the elements of Ω are pairwise disjoint, then $\sim_\Omega$ is transitive.

Corollary 6.59. Let A be a set and let Ω be a partition of A. Then $\sim_\Omega$ is an equivalence relation.

The previous corollary says that every partition determines a natural equivalence relation. Namely, two elements are related if and only if they are elements of the same set in the partition.

Exercise 6.60. Let $A = \{\circ, \triangle, \blacktriangle, \square, \blacksquare, \bigstar, ☺, ☹\}$. Make up a partition Ω on A and then draw the digraph corresponding to $\sim_\Omega$.

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 6.61. For each $m \in \mathbb{N}$, define $m\mathbb{Z}$ to be the set of all integers that are divisible by m; in set-builder notation, we have $m\mathbb{Z} = \{n \in \mathbb{Z} \mid n = mk \text{ for some } k \in \mathbb{Z}\}$.

For example, $5\mathbb{Z} = \{\ldots, -10, -5, 0, 5, 10, \ldots\}$ (the integers divisible by 5), and $2\mathbb{Z}$ is the set of even integers. What is $3\mathbb{Z}$? What about $1\mathbb{Z}$?

Exercise 6.62. 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 $3\mathbb{Z} \cap 5\mathbb{Z} = m\mathbb{Z}$ for some m; what is m? Describe $15\mathbb{Z} \cap 20\mathbb{Z}$ 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 6.63. Let $m \in \mathbb{N}$. If $a, b \in m\mathbb{Z}$, then $-a$, $a+b$, and ab are also in $m\mathbb{Z}$.[1]

Definition 6.64. For each $m \in \mathbb{N}$, define a relation on $\mathbb{Z}$ via $a \equiv_m b$ if and only if $(a-b) \in m\mathbb{Z}$. We read $a \equiv_m b$ as "a is congruent to b modulo m."

Theorem 6.65. For $m \in \mathbb{N}$, the relation $\equiv_m$ is an equivalence relation on $\mathbb{Z}$.

Since we know that $\equiv_m$ is an equivalence relation, we introduce some more notation.

Definition 6.66. For $m \in \mathbb{N}$, let $[a]_m$ denote the equivalence class of a with respect to $\equiv_m$ (see Definitions **??** and **??**). The class $[a]_m$ is called the **class of** a **modulo** m. The set of all equivalence classes determined by $\equiv_m$ is denoted $\mathbb{Z}/m\mathbb{Z}$.

Example 6.67. You computed $[1]_5$ and $[2]_5$ in Exercise **??**. Now, let's compute $[2]_7$ together. Tracing back through the definitions, we find that

$$n \in [2]_7 \iff n \equiv_7 2 \iff (n-2) \in 7\mathbb{Z} \iff n - 2 = 7k \text{ for some } k \in \mathbb{Z}.$$

Thus, $n \in [2]_7 \iff n = 7k + 2$ for some $k \in \mathbb{Z}$, so the elements of $[2]_7$ are those numbers that are 2 more than a multiple of 7. The multiples of 7 are $7\mathbb{Z} = \{\ldots, -14, -7, 0, 7, 14, \ldots\}$, so we can find $[2]_7$ by adding 2 to each element of $7\mathbb{Z}$ to get $[2]_7 = \{\ldots, -12, -5, 2, 9, 16, \ldots\}$.

Exercise 6.68. Find five elements in $[4]_7$ with at least one greater than 70 and one less than 70. Repeat for $[-3]_7$ and $[7]_7$.

Exercise 6.69. Describe $[0]_3$, $[1]_3$, $[2]_3$, $[4]_3$, and $[-2]_3$ with lists as in Example **??**. Which of these are equal? How many (different) classes are in $\mathbb{Z}/3\mathbb{Z}$? (Theorem **??** is helpful.)

[1] You are encouraged to make use of what you proved in Chapter **??**.

Theorem 6.70. For $m \in \mathbb{N}$ and $a, b \in \mathbb{Z}$, $[a]_m = [b]_m$ if and only if $(a - b)$ is divisible by m.[2]

Theorem 6.71. For $m \in \mathbb{N}$ and $a \in \mathbb{Z}$, $[a]_m = [0]_m$ if and only if a is divisible by m.

Theorem 6.72. Let $m \in \mathbb{N}$, and let $a_1, a_2, b_1, b_2 \in \mathbb{Z}$. If $[a_1]_m = [a_2]_m$ and $[b_1]_m = [b_2]_m$, then

(a) $[a_1 + b_1]_m = [a_2 + b_2]_m$,[3] and

(b) $[a_1 \cdot b_1]_m = [a_2 \cdot b_2]_m$.[4]

The previous theorem allows us to define addition and multiplication for $\mathbb{Z}/m\mathbb{Z}$.

Definition 6.73. Let $m \in \mathbb{N}$. For $[a]_m, [b]_m \in \mathbb{Z}/m\mathbb{Z}$, define the sum $[a]_m + [b]_m$ to be $[a+b]_m$, and define the product $[a]_m \cdot [b]_m$ to be $[a \cdot b]_m$.

Example 6.74. By Definition **??**, $[2]_7 + [6]_7 = [2 + 6]_7 = [8]_7$. Since $[8]_7 = [1]_7$ (by Theorem **??**), we can write this as $[2]_7 + [6]_7 = [1]_7$. Similarly, $[2]_7 \cdot [6]_7 = [2 \cdot 6]_7 = [12]_7 = [5]_7$.

Addition and multiplication for $\mathbb{Z}/m\mathbb{Z}$ has many familiar (and some not so familiar) properties. For example, addition and multiplication are both associative and commutative. But, it is possible for $[a]_m \cdot [b]_m = [0]_m$ even when $[a]_m \neq [0]_m$ and $[b]_m \neq [0]_m$.

Exercise 6.75. Find a and b such that $[a]_6 \cdot [b]_6 = [0]_6$ but $[a]_6 \neq [0]_6$ and $[b]_6 \neq [0]_6$. Do the same in $\mathbb{Z}/15\mathbb{Z}$: find a and b such that $[a]_{15} \cdot [b]_{15} = [0]_{15}$ but $[a]_{15} \neq [0]_{15}$ and $[b]_{15} \neq [0]_{15}$.

Theorem 6.76. Let $m \in \mathbb{N}$. If m is not prime, then there exists $[a]_m, [b]_m \in \mathbb{Z}/m\mathbb{Z}$ such that $[a]_m \cdot [b]_m = [0]_m$ but $[a]_m \neq [0]_m$ and $[b]_m \neq [0]_m$.

Theorem 6.77. Let $m \in \mathbb{N}$. Then addition in $\mathbb{Z}/m\mathbb{Z}$ is associative and commutative.[5]

Theorem 6.78. Let $m \in \mathbb{N}$. Then multiplication in $\mathbb{Z}/m\mathbb{Z}$ is associative and commutative.

Exercise 6.79. 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 $[14]_7[x]_7 = [1]_7$?

Theorem 6.80. Let $m \in \mathbb{N}$. For all $k \in \mathbb{N}$, if $[a_1]_m, [a_2]_m, \ldots, [a_k]_m \in \mathbb{Z}/m\mathbb{Z}$, then

(a) $[a_1]_m + [a_2]_m + \cdots + [a_k]_m = [a_1 + a_2 + \cdots + a_k]_m$, and

(b) $[a_1]_m[a_2]_m \cdots [a_k]_m = [a_1 a_2 \cdots a_k]_m$.

Remark 6.81. Part (b) of Theorem **??** implies that $([a]_m)^k = [a^k]_m$.

Exercise 6.82. For each of the following, find a number a with $0 \leq a \leq 6$ such that the given quantity is equal to $[a]_7$. The first one is done as an example.

(a) $[8^{179}]_7$ *Solution:* $[8^{179}]_7 = ([8]_7)^{179} = ([1]_7)^{179} = [1^{179}]_7 = [1]_7$. Thus, $\boxed{a = 1.}$ [6]

[2] Theorem **??** is very helpful.
[3] Consider using Theorem **??**.
[4] Hint: note that $a_1b_1 - a_2b_2 = a_1b_1 - a_2b_1 + a_2b_1 - a_2b_2$.
[5] This means for all $[a]_m, [b]_m, [c]_m \in \mathbb{Z}/m\mathbb{Z}$, $([a]_m + [b]_m) + [c]_m = [a]_m + ([b]_m + [c]_m)$ and $[a]_m + [b]_m = [b]_m + [a]_m$.
[6] Remark **??** was used twice. We also used that $[8]_7 = [1]_7$.

(b) $[6^{179}]_7$ (There is a hint in the footnotes.[7])

(c) $[2^{300}]_7$ (There is a hint in the footnotes.[8])

(d) $[2^{301}+5]_7$

Theorem 6.83. Let $n \in \mathbb{N}$, and let $a_k, a_{k-1}, \ldots, a_1, a_0$ be the digits of n, i.e. $n = a_k 10^k + a_{k-1}10^{k-1} + \cdots + a_1 10 + a_0$. Then $[n]_3 = [a_k + a_{k-1} + \cdots + a_1 + a_0]_3$.

Theorem 6.84. An integer is divisible by 3 if and only if the sum of its digits is divisible by 3.[9]

Exercise 6.85. Using modular arithmetic, prove that for all integers $n \geq 0$, $3^{2n} - 1$ is divisible by 8.[10] Did you find this easier than, harder than, or the same as using induction?

[7] Hint: $[6]_7 = [-1]_7$.
[8] Hint: $[2^3]_7 = [1]_7$.
[9] Consider using Theorem **??**.
[10] By Theorem **??**, you just need to show that $[3^{2n} - 1]_8 = [0]_8$.

Chapter 7

Functions

7.1 Introduction to Functions

Undoubtably, you have encountered the concept of function in your prior mathematical experience. In this section, we will introduce the concept of function as a special type of relation. As you shall see, this agrees with any previous definition of function that you may have learned.

Up until this point, you've probably 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. Loosely speaking, the basic building blocks of a function are a first set and a second sets, say X and Y, respectively, and a "correspondence" that assigns each 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** from set X to set Y, denoted $f : X \to Y$, is a relation (i.e., subset of $X \times Y$) such that:

(a) For each $x \in X$, there exists $y \in Y$ such that $(x, y) \in f$, and

(b) If $(x, y_1), (x, y_2) \in f$, then $y_1 = y_2$.

Note that if $(x, y) \in f$, we usually write $y = f(x)$ and say that "f maps x to y."

Part (a) of Definition **??** says that every element of X appears in the first coordinate of an ordered pair in the relation. Part (b) says that each element of X only appears once in the first coordinate of an ordered pair in the relation. It is important to note that there are no restrictions on whether an element of Y ever appears in the second coordinate. Furthermore, if an element of Y appears in the second coordinate, it may appear again in a different ordered pair.

Definition 7.2. The set X from Definition **??** is called the **domain** of f and is denoted by $\text{Dom}(f)$. The set Y is called the **codomain** of f and is denoted by $\text{Codom}(f)$. The set

$$\text{Rng}(f) = \{y \in Y \mid \text{there exists } x \text{ such that } y = f(x)\}$$

is called the **range** of f or the **image of** X under f. If f is a function and $(x, y) \in f$, then we may refer to x as the **input** of f and y as the **output** of f.

It follows immediately from the definition that $\text{Rng}(f) \subseteq \text{Codom}(f)$. However, it is possible that the range of f is a proper subset of the codomain.

Exercise 7.3. Let $X = \{\circ, \square, \triangle, \smiley\}$ and $Y = \{a, b, c, d, e\}$. Determine whether each of the following represent functions. Explain. If the relation is a function, determine the domain, codomain, and range.

(a) $f : X \to Y$ defined via $f = \{(\circ, a), (\square, b), (\triangle, c), (\smiley, d)\}$.

(b) $g : X \to Y$ defined via $g = \{(\circ, a), (\square, b), (\triangle, c), (\smiley, c)\}$.

(c) $h : X \to Y$ defined via $h = \{(\circ, a), (\square, b), (\triangle, c), (\circ, d)\}$.

(d) $k : X \to Y$ defined via $k = \{(\circ, a), (\square, b), (\triangle, c), (\smiley, d), (\square, e)\}$.

(e) $l : X \to Y$ defined via $l = \{(\circ, e), (\square, e), (\triangle, e), (\smiley, e)\}$.

(f) $m : X \to Y$ defined via $m = \{(\circ, a), (\triangle, b), (\smiley, c)\}$.

(g) $\text{happy} : Y \to X$ defined via $\text{happy}(y) = \smiley$ for all $y \in Y$.

(h) $\text{id} : X \to X$ defined via $\text{id}(x) = x$ for all $x \in X$.

(i) $\text{nugget} : X \to X$ defined via

$$\text{nugget}(x) = \begin{cases} x, & \text{if } x \text{ is a geometric shape,} \\ \square, & \text{otherwise.} \end{cases}$$

One useful representation of functions on finite sets is via **bubble diagrams**. To draw a bubble diagram for a function $f : X \to Y$, draw one circle (i.e, a "bubble") for each of X and Y and for each element of each set, put a dot in the corresponding set. Typically, we draw X on the left and Y on the right. Next, draw an arrow from $x \in X$ to $y \in Y$ if $f(x) = y$ (i.e., $(x, y) \in f$). Note that we can draw bubble diagrams even if f is not a function.

Example 7.4. Figure **??** depicts a bubble diagram for a function from domain $X = \{a, b, c, d\}$ to codomain $Y = \{1, 2, 3, 4\}$. In this case, the range is equal to $\{1, 2, 4\}$.

Exercise 7.5. For each of the relations in Exercise **??** draw the corresponding bubble diagram.

Problem 7.6. What properties does a bubble diagram have to have in order to represent a function?

Exercise 7.7. Provide an example of each of the following. You may draw a bubble 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 $\text{Rng}(f) = \text{Codom}(f)$.

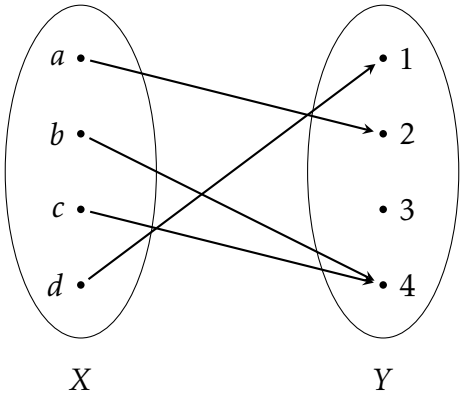

Figure 7.1: An example of a bubble diagram for a function.

(b) A function g from a set with 4 elements to a set with 3 elements such that $\text{Rng}(g)$ is strictly smaller than $\text{Codom}(g)$.

Problem 7.8. 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 $\text{Rng}(f) = \text{Codom}(f)$? Explain.

Problem 7.9. In high school I am sure that you were told that a graph represents a function if it passes the **vertical line test**. Using our terminology of ordered pairs, explain why this works.

Definition 7.10. Two functions are equal if they have the same domain, same codomain, and the same set of ordered pairs in the relation. That is, if $f : X \to Y$ and $g : X \to Y$ are functions, then $f = g$ if and only if $f(x) = g(x)$ for all $x \in X$.

If two functions are defined by the same algebraic formula, but have different domains, then they are *not* equal. For example, the function $f : \mathbb{R} \to \mathbb{R}$ defined via $f(x) = x^2$ is not equal to the function $g : \mathbb{N} \to \mathbb{N}$ defined via $g(x) = x^2$.

Definition 7.11. Let $f : X \to Y$ be a function.

(a) The function f is said to be **one-to-one** (or **injective**) if for all $y \in \text{Rng}(f)$, there is a unique $x \in X$ such that $y = f(x)$.

(b) The function f is said to be **onto** (or **surjective**) if for all $y \in Y$, there exists $x \in X$ such that $y = f(x)$.

(c) If f is both one-to-one and onto, we say that f is a **bijection** (or **one-to-one correspondence**).

Remark 7.12. Let $f : X \to Y$ be a function. To prove that f is one-to-one, start by assuming that $f(x_1) = f(x_2)$ and then work to show that $x_1 = x_2$. That is, a function f is one-to-one if and only if for all $x_1, x_2 \in X$, if $f(x_1) = f(x_2)$, then $x_1 = x_2$. To show that f is onto, you should start with an arbitrary $y \in Y$ and then work to show that there exists $x \in X$ such that $y = f(x)$.

Exercise 7.13. Provide an example of each of the following. You may draw a bubble diagram, write down a list of ordered pairs, or write a formula (as long as the domain and codomain are clear). Assume that X and Y are finite sets.

(a) A function $f : X \to Y$ that is one-to-one but not onto.

(b) A function $f : X \to Y$ that is onto but not one-to-one.

(c) A function $f : X \to Y$ that is a bijection.

(d) A function $f : X \to Y$ that is neither one-to-one nor onto.

Problem 7.14. Perhaps you've heard of the **horizontal line test** (i.e., every horizontal line hits the graph of $f : \mathbb{R} \to \mathbb{R}$ at most once). What is the horizontal line test testing for?

Exercise 7.15. 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 one-to-one but not onto.

(b) A function $f : \mathbb{R} \to \mathbb{R}$ that is onto but not one-to-one.

(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 one-to-one nor onto.

Exercise 7.16. Determine which of the following functions are one-to-one, onto, both, or neither. In each case, you should provide proofs and counterexamples as appropriate.

(a) $f : \mathbb{R} \to \mathbb{R}$ defined via $f(x) = x^2$

(b) $g : \mathbb{R} \to [0, \infty)$ defined via $g(x) = x^2$

(c) $h : \mathbb{R} \to \mathbb{R}$ defined via $h(x) = x^3$

(d) $k : \mathbb{R} \to \mathbb{R}$ defined via $k(x) = x^3 - x$

(e) $l : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ defined via $l(x_1, x_2) = x_1^2 + x_2^2$

(f) $N : \mathbb{N} \to \mathbb{N} \times \mathbb{N}$ defined via $N(n) = (n, n)$

Definition 7.17. If X is a nonempty set, then the function $i_X : X \to X$ defined via $i_X(x) = x$ is called the *identity function* on X.

Theorem 7.18. The identity function on a nonempty set X is a bijection.

Exercise 7.19. Let A and B be sets and let $S \subseteq A \times B$. 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 (respectively, π_2) the **projections** of S onto A (respectively, B).

(a) Provide examples to show that π_1 does not need to be one-to-one or onto.

(b) Suppose that S is a function (recall that a function is a set of ordered pairs, so this makes sense). Is π_1 one-to-one? Is π_1 onto? How about π_2?

Theorem 7.20. Let A be a nonempty set and suppose $\sim$ is an equivalence relation on A. Then the function $\phi : A \to A/\sim$ defined via $\phi(x) = [x]$ is onto.[1]

7.2 Images and Inverse Images of Functions

There are two important sets related to functions.

Definition 7.21. Let $f : X \to Y$ be a function.

(a) If $S \subseteq X$, the **image** of S under f is defined via

$$f(S) := \{f(x) \mid x \in S\}.$$

(b) If $T \subseteq Y$, the **inverse image** (or **preimage**) of T under f is defined via

$$f^{-1}(T) := \{x \in X \mid f(x) \in T\}.$$

You've likely encountered inverse *functions* before. But in this context, we are discussing inverse *images*. It's important to point out that the use of the notation f^{-1} does not make any assumptions about whether the inverse function exists. We will tackle inversion functions in the next section.

Note that the image of the domain is the same as its range. That is, $f(X) = \text{Rng}(f)$. Moreover, the inverse image of the codomain is the domain. That is, $f^{-1}(Y) = X$.

Exercise 7.22. Define $f : \mathbb{Z} \to \mathbb{Z}$ via $f(x) = x^2$. Find $f(\{-2, -1, 0, 1, 2\})$ and $f^{-1}(\{0, 1, 4\})$.

Exercise 7.23. Define $f : \mathbb{R} \to \mathbb{R}$ via $f(x) = 3x^2 - 4$. Find each of the following.

(a) $f([-2, 4])$

(b) $f((-2, 4))$

(c) $f^{-1}([-10, 1])$

(d) $f^{-1}((-3, 3))$

(e) $f(\emptyset)$

(f) $f(\mathbb{R})$

(g) $f^{-1}(\emptyset)$

(h) $f^{-1}(\mathbb{R})$

[1] Recall that $A/\sim$ is the set of equivalence classes induced by the equivalence relation $\sim$.

(i) Find two non-empty subsets A, B of $\mathbb{R}$ such that $A \cap B = \emptyset$ but $f^{-1}(A) = f^{-1}(B)$

(j) Find two non-empty subsets A, B of $\mathbb{R}$ such that $A \cap B = \emptyset$ but $f(A) = f(B)$

Problem 7.24. 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 7.25. 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 the 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) $f(f^{-1}(C)) \supseteq C$.

Exercise 7.26. For each of the statements in previous problem that were false, determine conditions—if any—on the corresponding sets that would make the statement true.

7.3 Compositions and Inverse Functions

Definition 7.27. If $f : X \to Y$ and $g : Y \to Z$ are functions, then a new function $g \circ f : X \to Z$ can be defined by $(g \circ f)(x) = g(f(x))$ for all $x \in \text{Dom}(f)$.

It is important to notice that the function on the right is the one that "goes first."

Exercise 7.28. 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 bubble diagrams is sufficient.

(a) f is onto, but $g \circ f$ is not onto.

(b) g is onto, but $g \circ f$ is not onto.

(c) f is one-to-one, but $g \circ f$ is not one-to-one.

(d) g is one-to-one, but $g \circ f$ is not.

Theorem 7.29. If $f : X \to Y$ and $g : Y \to Z$ are both functions that are onto, then $g \circ f$ is also onto.

Theorem 7.30. If $f : X \to Y$ and $g : Y \to Z$ are both functions that are one-to-one, then $g \circ f$ is also one-to-one.

Corollary 7.31. If $f : X \to Y$ and $g : Y \to Z$ are both bijections, then $g \circ f$ is also a bijection.

Problem 7.32. 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 the statement is true, prove it. Otherwise, provide a counterexample.

(a) If $g \circ f$ is one-to-one, then f is one-to-one.

(b) If $g \circ f$ is one-to-one, then g is one-to-one.

(c) If $g \circ f$ is onto, then f is onto.

(d) If $g \circ f$ is onto, then g is onto.

The next theorem tells us that function composition is associative.

Theorem 7.33. If $f : X \to Y$, $g : Y \to Z$, and $h : Z \to W$ are functions, then $(h \circ g) \circ f = h \circ (g \circ f)$.

Theorem 7.34. Let $f : X \to Y$ be a function. Then f is one-to-one 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 function on X.

The function g in the previous theorem is often called a *left inverse* of f.

Theorem 7.35. Let $f : X \to Y$ be a function. Then f is onto 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 function on Y.

The function g in the previous theorem is often called a *right inverse* of f.

Exercise 7.36. 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.

Exercise 7.37. 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 7.38. 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. We say that g is a *two-sided inverse* of f.

Definition 7.39. Let $f : X \to Y$ be a function. The relation f^{-1}, called f **inverse**, is defined via

$$f^{-1} = \{(f(x), x) \in Y \times X \mid x \in X\}.$$

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.

Exercise 7.40. Provide an example of a function $f : X \to Y$ such that f^{-1} is *not* a function. A bubble diagram is sufficient.

Exercise 7.41. Provide an example of a function $f : X \to Y$ such that f^{-1} is a function. A bubble diagram is sufficient.

Theorem 7.42. Let $f : X \to Y$ be a function. Then f^{-1} is a function if and only if f is a bijection.

Theorem 7.43. 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 7.44. Let $f : X \to Y$ and $g : Y \to X$ be functions such that f is a bijection. If $g \circ f = i_X$ and $f \circ g = i_Y$, then $g = f^{-1}$.

The upshot of the previous two theorems is that if f^{-1} is a function, then it is the only one satisfying the two-sided inverse property exhibited in Corollary **??** and Theorem **??**.

Theorem 7.45. If $f : X \to Y$ is a bijection, then $f^{-1} : Y \to X$ is a bijection and $(f^{-1})^{-1} = f$.

Theorem 7.46. 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?

Theorem 7.47. Let $f : X \to Y$ be a function and define $\sim$ on X via $a \sim b$ if and only if $f(a) = f(b)$.

(a) The relation $\sim$ is an equivalence relation,

(b) Each equivalence class $[a]$ is equal to $f^{-1}(f(a))$,

(c) The function $g : X/\sim \to f(X)$ defined via $g([a]) = f(a)$ is a bijection.

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 one-to-one and onto. 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. If A and B have the same cardinality, then we write $\boxed{\text{card}(A) = \text{card}(B)}$.

Note that we have not defined $\text{card}(A)$ 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 $\text{card}(A) = \text{card}(B)$ (and later $\text{card}(A) \leq \text{card}(B)$ and $\text{card}(A) < \text{card}(B)$), we are asserting the existence of a certain type of function from A to B.

Problem 8.2. 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) If $A = \{a, b, c\}$ and $B = \{x, y, z\}$, then $\text{card}(A) = \text{card}(B)$.

(b) If $\mathcal{O}$ is the set of odd natural numbers, then $\text{card}(\mathbb{N}) = \text{card}(\mathcal{O})$.

(c) $\text{card}(\mathbb{N}) = \text{card}(\mathbb{Z})$.

(d) Let $a, b, c, d \in \mathbb{R}$ with $a < b$ and $c < d$. Then $\text{card}((a,b)) = \text{card}((c,d))$.[1]

(e) If $R = \{\frac{1}{2^n} \mid n \in \mathbb{N}\}$, then $\text{card}(\mathbb{N}) = \text{card}(R)$.

(f) If $\mathcal{F}$ is the set of functions from $\mathbb{N}$ to $\{0,1\}$, then $\text{card}(\mathcal{F}) = \text{card}(\mathcal{P}(\mathbb{N}))$.[2]

(g) If A is any set, then $\text{card}(A) = \text{card}(A \times \{x\})$.

Theorem 8.3. Let A, B, and C be sets.

(a) $\text{card}(A) = \text{card}(A)$.

(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 8.4. If X is a set, then "has the same cardinality as" is an equivalence relation on $\mathcal{P}(X)$.

Theorem 8.5. 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 8.6. Let A and B be sets. If there is a one-to-one function (i.e., injection) 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 8.7. 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 $\text{card}(B) \leq \text{card}(A)$.

[1] *Hint:* Try creating a linear function $f : (a,b) \to (c,d)$. Drawing a picture should help.
[2] *Hint:* Define $\phi : \mathcal{F} \to \mathcal{P}(\mathbb{N})$ so that $\phi(f)$ outputs a subset of $\mathbb{N}$ determined by when f outputs a 1.

It might be tempting to think that the existence of a one-to-one function from a set A to a set B that is *not* onto 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 exercise asks you to verify.

Exercise 8.8. Provide an example of sets A and B such that $\text{card}(A) = \text{card}(B)$ despite the fact that there exists a one-to-one function from A to B that is not onto.

Definition 8.9. Let A and B be sets. We write $\boxed{\text{card}(A) < \text{card}(B)}$ provided $\text{card}(A) \leq \text{card}(B)$ and $\text{card}(A) \neq \text{card}(B)$.

It is important to point out that 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 one-to-one but not onto." The statement $\text{card}(A) < \text{card}(B)$ is asserting that *every* one-to-one function from A to B is not onto. 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.

Definition 8.10. For each $n \in \mathbb{N}$, define $[n] = \{1, 2, \ldots, n\}$.

For example, $[5] = \{1, 2, 3, 4, 5\}$. Notice that our notation looks just like that for the set of relatives given a relation on some set (see Definition **??**), which is an equivalence class if the relation happens to be an equivalence relation. 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 8.11. 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.

Theorem 8.12. If A is finite and $\text{card}(A) = \text{card}(B)$, then B is finite.[3]

Theorem 8.13. If A has cardinality $n \in \mathbb{N} \cup \{0\}$ and $x \notin A$, then $A \cup \{x\}$ is finite and has cardinality $n + 1$.

Theorem 8.14. For every $n \in \mathbb{N}$, every subset of $[n]$ is finite.[4]

[3] Don't forget to consider the case when $A = \emptyset$.

[4] *Hint:* Use induction.

Theorem **??** 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 8.15. 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 8.16. 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.

Theorem 8.17. If $A_1, A_2, \ldots, A_k$ is a finite collection of finite sets, then $\bigcup_{i=1}^{k} A_i$ is finite.[5]

The next theorem, called the Pigeonhole Principle, is surprisingly useful. It puts restrictions on when we may have a one-to-one 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.

Theorem 8.18 (Pigeonhole Principle)**.** If $n, k \in \mathbb{N}$ and $f : [n] \to [k]$ with $n > k$, then f is not one-to-one.[6]

8.3 Infinite Sets

In the previous section, we explored finite sets. Now, let's tinker with infinite sets.

Definition 8.19. 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 8.20. The set $\mathbb{N}$ of natural numbers is infinite.[7]

The next theorem is analogous to Theorem **??**, but for infinite sets. As we shall see later, the converse of this theorem is not generally true.

Theorem 8.21. If A is infinite and $\text{card}(A) = \text{card}(B)$, then B is infinite.[8]

[5] *Hint:* Use induction.

[6] *Hint:* Induct on the number of pigeons. The base case is $n = 2$.

[7] *Hint:* For sake of a contradiction, assume otherwise. Then there exists $n \in \mathbb{N}$ such that $\text{card}([n]) = \text{card}(\mathbb{N})$, which implies that there exists a bijection $f : [n] \to \mathbb{N}$. What can you say about the number $m := \max(f(1), f(2), \ldots, f(n)) + 1$?

[8] *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 $n \in \mathbb{N}$.

Exercise 8.22. Quickly verify that the following sets are infinite by appealing to Theorem **??**, Theorem **??**, and Problem **??**.

(a) The set of odd natural numbers.

(b) The set of even natural numbers.

(c) The integers.

(d) The set $R = \{\frac{1}{2^n} \mid n \in \mathbb{N}\}$.

(e) The set $\mathbb{N} \times \{x\}$.

Notice that Definition **??** tells what infinite sets are not, but it doesn't really tell us what they are. In light of Theorem **??**, 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 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[9], illustrates another way to think about infinite sets.

Problem 8.23. The Infinite Hotel has rooms numbered $1, 2, 3, 4, \ldots$. Every room in the Infinite Hotel is currently occupied. Is it possible to make room for one more guest (assuming they want a room all to themselves)? 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 in 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 Exercise **??**. Notice that Theorem **??** 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 8.24. Let A be a set. Then the following statements are equivalent.[10]

(i) A is an infinite set.

(ii) There exists a one-to-one function $f : \mathbb{N} \to A$.

(iii) A can be put in bijection with a proper subset of A (i.e., there exists a proper subset B of A such that $\text{card}(B) = \text{card}(A)$).

[9] The Hilbert Hotel is named after mathematician David Hilbert (1862–1942).

[10] *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.

Corollary 8.25. A set is infinite if and only if it has an infinite subset.

Corollary 8.26. If A is an infinite set, then $\text{card}(\mathbb{N}) \leq \text{card}(A)$.

It is worth mentioning that for the previous theorem, (iii) implies (i) follows immediately from the contrapositive of Theorem **??**.

Problem 8.27. Find a new proof of Theorem **??** that uses (iii) implies (i) from Theorem **??**.

Exercise 8.28. Quickly verify that the following sets are infinite by appealing to either Theorem **??** (use (ii) implies (i)) or Corollary **??**.

(a) The set of odd natural numbers.

(b) The set of even natural numbers.

(c) The integers.

(d) The set $\mathbb{N} \times \mathbb{N}$.

(e) The set of rational numbers $\mathbb{Q}$.

(f) The set of real numbers $\mathbb{R}$.

(g) The set of perfect squares.

(h) The interval $(0, 1)$.

(i) The set of complex numbers $\mathbb{C} := \{a + bi \mid a, b \in \mathbb{R}\}$.

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 8.29. 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 isn't an issue. This idea leads to the following definition.

Definition 8.30. 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.

Exercise 8.31. Quickly justify that each of the following sets is countable. Feel free to appeal to previous problems.

(a) The set $A := \{a, b, c\}$

(b) The set of odd natural numbers.

(c) The set of even natural numbers.

(d) The set $R := \{\frac{1}{2^n} \mid n \in \mathbb{N}\}$.

(e) The set of perfect squares.

(f) The integers.

(g) The set $\mathbb{N} \times \{x\}$, where $x \notin \mathbb{N}$.

Theorem 8.32. Let A and B be sets such that A is countable. If $f : A \to B$ is a bijection, then B is countable.

Theorem 8.33. Every subset of a countable set is countable.[11]

Theorem 8.34. A set is countable if and only if it has the same cardinality of some subset of the natural numbers.

Theorem 8.35. If $f : \mathbb{N} \to A$ is an onto 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 8.36. The set of rational numbers $\mathbb{Q}$ is countable.[12]

Theorem 8.37. 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 8.38. Let $\{A_n\}_{n=1}^{\infty}$ be a (countable) 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.

[11] *Hint:* Let A be a countable set. Consider the cases when A is finite versus infinite. The contrapositive of Corollary **??** should be useful for the case when A is finite.

[12] *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 **??**.

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

Theorem 8.39. Every countable union of countable sets is countable.[13]

Theorem 8.40. If A and B are countable sets, then $A \times B$ is countable.

Theorem 8.41. The set of all finite sequences of 0's and 1's (e.g., 0110010) is countable.

8.5 Uncountable Sets

Recall from Definition **??** 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 open interval $(0,1)$ is uncountable. By Exercise **??**(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 **??**. 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 $x = 0.a_1a_2a_3\ldots$ is said to be in **standard form** if and only if there is no k such that for all $i > k$, $a_i = 9$. That is, a decimal expansion is in standard form if and only if the expansion doesn't end with a repeating sequence of 9's. For example, 0.2 is in standard 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 form.

Problem 8.42. 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 $(0,1)$. Let $f(n) := 0.a_{1n}a_{2n}a_{3n}\ldots$, where a_{1n} is the first digit in the 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 form 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 form.

(b) Prove that for all $n \in \mathbb{N}$, $f(n) \neq b$.

[13] *Hint:* A countable union is a union of countably many sets. Recall that a countable set may be finite or infinite. Consider three cases: (1) finite union of countable sets (use induction with base case $n = 2$), (2) countably infinite union of finite sets, (3) countably infinite union of countably infinite sets.

(c) Prove that f is not onto.

(d) Explain why we have a contradiction.

(e) Explain why it follows that the open interval $(0,1)$ cannot be countable.

The steps above prove the following theorem.

Theorem 8.43. The open interval $(0,1)$ is uncountable.

Loosely speaking, what Theorem **??** 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!

One consequence of Theorem **??** is that we know there is at least one uncountable set. The next three results are useful for finding other uncountable sets.

Theorem 8.44. If A and B are sets such that $A \subseteq B$ and A is uncountable, then B is uncountable.[14]

Corollary 8.45. If A and B are sets such that A is uncountable and B is countable, then $A \setminus B$ is uncountable.

Theorem 8.46. If $f : A \to B$ is a one-to-one function and A is uncountable, then B is uncountable.

Theorem 8.47. The set $\mathbb{R}$ of real numbers is uncountable. Moreover, $\text{card}((0,1)) = \text{card}(\mathbb{R})$.[15]

Theorem 8.48. If $a, b \in \mathbb{R}$ with $a < b$, then (a,b), $[a,b]$, $(a,b]$, and $[a,b)$ are all uncountable.

Theorem 8.49. The set of irrational numbers is uncountable.

Theorem 8.50. The set $\mathbb{C}$ of complex numbers is uncountable.

Problem 8.51. 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 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 8.52. 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.

[14] *Hint:* Try a proof by contradiction. Take a look at Theorem **??**.

[15] *Hint:* To show that $\mathbb{R}$ is uncountable, appeal to Theorem **??**. 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.

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 8.53. If A is a set, then $\text{card}(A) < \text{card}(\mathcal{P}(A))$.[16]

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 **??** tells us that there are infinitely many "sizes of infinity."

Theorem 8.54. Consider the set S from Problem **??**. Then $\text{card}(\mathcal{P}(\mathbb{N})) = \text{card}(S)$.

[16] *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. I may refer to them, by number, in my comments on your homework and exams. 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. **"=" 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. **Say exactly what you mean.** Just as the $=$ 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.

10. **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.

11. **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 $\sqrt{12^2 + 5^2} = d$.

12. **Avoid circularity.** Be sure that no step in your proof makes use of the conclusion!

13. **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.

14. **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.

15. **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."

16. **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.

17. **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.

18. **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*.

19. **Write "Let $x = \ldots$," 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 $a^2 \neq b$?"

20. **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.

21. **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 **??**). 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.

22. **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. *Do not hand in your scratch work!*

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, Zermelo-Frankel axioms, 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 theory (Russell's paradox). The term paradox is often 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

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. (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 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.