Course Notes for Introduction to Proof

D.C. Ernst

Typeset on May 5, 2014

Part of this work is an adaptation of notes written by Stan Yoshinobu of Cal Poly and Matthew Jones of California State University, Dominguez Hills.

\[\text{cc BY SA}\]

\[\text{Northern Arizona University, Dana.Ernst@nau.edu}\]
## Contents

Preface

1 **Introduction to Mathematics**
   1.1 A Taste of Number Theory .............................................. 2
   1.2 Logic, Negation, Contrapositive .................................... 4
   1.3 Negating Implications and Proof by Contradiction ............... 7
   1.4 Introduction to Quantification ....................................... 9
   1.5 More on Quantification ............................................. 11
   1.6 And Even More on Quantification ................................... 13

2 **Introduction to Set Theory and Topology**  
   2.1 Sets .......................................................... 17
   2.2 Power Sets and Paradoxes ......................................... 21
   2.3 Indexing Sets ..................................................... 24
   2.4 Basic Topology of $\mathbb{R}$ ...................................... 28
   2.5 Induction ....................................................... 31

3 **Two Famous Theorems**  
   3.1 The irrationality of $\sqrt{2}$ ........................................ 33
   3.2 The infinitude of primes ........................................... 36

4 **Relations and Functions**  
   4.1 Relations ...................................................... 37
   4.2 Equivalence Relations ............................................. 41
   4.3 Partitions ........................................................ 43
   4.4 Introduction to Functions ....................................... 45
   4.5 Compositions and Inverses ....................................... 49
Preface

What is Meant by Foundations?

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 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!
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 . . .

Lastly, it is highly important to respect learning and to respect other people’s ideas. Whether you disagree or agree, please praise and encourage your fellow classmates. Use ideas from others as a starting point rather than something to be judgmental about. Judgement is not the same as being judgmental. Helpfulness, encouragement, and compassion are highly valued.

An Inquiry-Based Approach

This course will likely be different than any other math class that you have taken before for two main reasons. First, you are used to being asked to do things like: “solve for x”, “take the derivative of this function”, “integrate this function”, etc. Accomplishing tasks like these usually amounts to mimicking examples that you have seen in class or in your textbook. The steps you take to “solve” problems like these are always justified by mathematical facts (theorems), but rarely are you
paying explicit attention to when you are actually using these facts. Furthermore, justifying (i.e., proving) the mathematical facts you use may have been omitted by the instructor. And, even if the instructor did prove a given theorem, you may not have taken the time or have been able to digest the content of the proof.

Unlike previous courses, this course is all about “proof”. Mathematicians are in the business of proving theorems and this is exactly our endeavor. For the first time, you will be exposed to what “doing” mathematics is really all about. This will most likely be a shock to your system. Considering the number of math courses that you have taken before you arrived here, one would think that you have some idea what mathematics is all about. You must be prepared to modify your paradigm. The second reason why this course will be different for you is that the method by which the class will run and the expectations I have of you will be different. In a typical course, math or otherwise, you sit and listen to a lecture. (Hopefully) These lectures are polished and well-delivered. You may have often been lured into believing that the instructor has opened up your head and is pouring knowledge into it. I absolutely love lecturing and I do believe there is value in it, but I also believe that in reality most students do not learn by simply listening. You must be active in the learning you are doing. I’m sure each of you have said to yourselves, “Hmm, I understood this concept when the professor was going over it, but now that I am alone, I am lost.” In order to promote a more active participation in your learning, we will incorporate ideas from an educational philosophy called the Moore method (after R.L. Moore). Modifications of the Moore method are also referred to as inquiry-based learning (IBL) or discovery-based learning.

Loosely speaking, IBL is a student-centered method of teaching mathematics. At the college-level, one form of IBL is the Modified Moore Method, named after R.L. Moore. In 1966, Moore wrote

That student is taught the best who is told the least.

According to the Academy of Inquiry-Based Learning, IBL engages students in sense-making activities. Students are given tasks requiring them to:

- solve problems,
- conjecture,
- experiment,
- explore,
- create,
- 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. Effective IBL courses encourage deep engagement in rich mathematical activities and provide opportunities to collaborate with peers (either through class presentations or group-oriented work).

Perhaps this is sufficiently vague, but I believe that there are two essential elements to IBL:

1. Students should as much as possible be responsible for guiding the acquisition of knowledge.
2. Students should as much as possible be responsible for validating the ideas presented. That is, students should not be looking to the instructor as the sole authority.

For me, the guiding principle of IBL is the following question:
Where do I draw the line between content I must impart to my students versus the content they can produce independently?

E. Lee May (Salisbury State University) may have said it best:

Inquiry-based learning (IBL) is a method of instruction that places the student, the subject, and their interaction at the center of the learning experience. At the same time, it transforms the role of the teacher from that of dispensing knowledge to one of facilitating learning. It repositions him or her, physically, from the front and center of the classroom to someplace in the middle or back of it, as it subtly yet significantly increases his or her involvement in the thought-processes of the students.

For additional information, see AIBL’s What is IBL? and Why use IBL? pages.

Much of the course will be devoted to students proving theorems 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!

Furthermore, it is important to understand that proving theorems is difficult and takes time. You should not expect to complete a single proof in 10 minutes. Sometimes, you might have to stare at the statement for an hour before even understanding how to get started.

In this course, everyone will be required to

- read and interact with course notes on your own;
- write up quality proofs to assigned problems;
- present proofs on the board to the rest of the class;
- participate in discussions centered around a student’s presented 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. This will be new to many of you and there may be some growing pains associated with it.

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 1.13, we see that . . .”

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!
Chapter 1

Introduction to Mathematics

Before you get started, make sure you’ve read the Preface, which sets the tone for the work we will begin doing here.
1.1 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 \( \mathbb{Z} \).

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!

**Definition 1.1.** An integer \( n \) is **even** if \( n = 2k \) for some integer \( k \).

**Definition 1.2.** An integer \( n \) is **odd** if \( n = 2k + 1 \) for some integer \( k \).

**Theorem 1.3** The sum of two consecutive integers is odd.

**Theorem 1.4** If \( n \) is even, then \( n^2 \) is even.

**Problem 1.5** (*) Prove or provide a counterexample: The sum of an even number and an odd number is odd.

**Question 1.6** Did Theorem 1.3 need to come before Problem 1.5? Could we have used Problem 1.5 to prove Theorem 1.3? 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 1.5? Is one approach better than the other?

**Problem 1.7** Prove or provide a counterexample: The product of an odd number and an even number is odd.

**Problem 1.8** (*) Prove or provide a counterexample: The product of an odd number and an odd number is odd.

**Problem 1.9** (*) Prove or provide a counterexample: The product of two even numbers is even.

**Definition 1.10.** An integer \( n \) divides the integer \( m \), written \( n|m \), if and only if there exists an integer \( k \) such that \( m = nk \). In the same context, we may also write that \( m \) is divisible by \( n \).

In this section on number theory, we allow addition, subtraction, and multiplication. 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 \( \frac{n}{n} \). When you feel the urge to divide, switch to an equivalent formulation using multiplication.

**Problem 1.11** Let \( n \) be an integer. Prove or provide a counterexample: If 6 divides \( n \), then 3 divides \( n \).

**Problem 1.12** Let \( n \) be an integer. Prove or provide a counterexample: If 6 divides \( n \), then 4 divides \( n \).

**Theorem 1.13** (*) Assume \( n, m, \) and \( a \) are integers. If \( a|n \), then \( a|m n \).

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

**Corollary 1.14** Assume \( n \) and \( a \) are integers. If \( a \) divides \( n \), then \( a \) divides \( n^2 \).
Problem 1.15  Assume $n$ and $a$ are integers. Prove or provide a counterexample: If $a$ divides $n^2$, then $a$ divides $n$.

Theorem 1.16  Assume $a$ and $n$ are integers. If $a$ divides $n$, then $a$ divides $-n$.

Theorem 1.17  Assume $a$, $m$, and $n$ are integers. If $a$ divides $m$ and $a$ divides $n$, then $a$ divides $m + n$.

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 1.18  Assume $a$, $m$, and $n$ are integers. If $a$ divides $m$ and $a$ divides $n$, then $a$ divides $m - n$.

Problem 1.19  Assume $a$, $b$, and $m$ are integers. 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 1.20  If $a$, $b$, and $c$ are integers where $a$ divides $b$ and $b$ divides $c$, then $a$ divides $c$.

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

Theorem 1.21  The sum of any three consecutive integers is always divisible by three.
1.2 Logic, Negation, Contrapositive

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 1.21.** A **proposition** (or **statement**) is a sentence that is either true or false.

For example, the sentence “All liberals are hippies” 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 1.22** Determine whether the following are propositions or not. Explain.

1. All cars are red.
2. Van Gogh was the best artist ever.
3. If my name is Joe, then my name starts with the letter J.
4. If my name starts with the letter J, then my name is Joe.
5. $f$ is continuous.
6. All functions are continuous.
7. If $f$ is a differentiable function, then $f$ is continuous function.
8. The president had eggs for breakfast the morning of his tenth birthday.
9. What time is it?
10. There exists an $x$ such that $x^2 = 4$.
11. $x^2 = 4$.
12. $\sqrt{2}$ is an irrational number.
13. For all real numbers $x$, $x^3 = x$.
14. There exists a real number $x$ such that $x^3 = x$.
15. $p$ is prime.

Given two propositions, we can form more complicated propositions using the logical connectives “and”, “or”, and “If..., then...”.

**Definition 1.23.** Let $A$ and $B$ be propositions. The proposition “$A$ and $B$” is true if and only if both $A$ and $B$ are true. The statement “$A$ and $B$” is expressed symbolically as

$$A \land B$$

and is known as the **conjunction** of $A$ and $B$.

**Definition 1.24.** Let $A$ and $B$ be propositions. The proposition “$A$ or $B$” is true if and only if at least one of $A$ or $B$ is true. The statement “$A$ or $B$” is symbolically represented as

$$A \lor B$$

and is known as the **disjunction** of $A$ and $B$.  

Definition 1.25. Let $A$ be a proposition. The negation of $A$, denoted $\neg A$, is true if and only if $A$ is false.

Exercise 1.26. Describe the meaning of $\neg(A \land B)$ and $\neg(A \lor B)$.

Definition 1.27. A truth table is a table that illustrates all possible truth values for a proposition.

Example 1.28. Let $A$ and $B$ be propositions. Then the truth table for the conjunction $A \land B$ is given by the following.

<table>
<thead>
<tr>
<th>$A$</th>
<th>$B$</th>
<th>$A \land B$</th>
</tr>
</thead>
<tbody>
<tr>
<td>T</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
<td>F</td>
</tr>
<tr>
<td>F</td>
<td>T</td>
<td>F</td>
</tr>
<tr>
<td>F</td>
<td>F</td>
<td>F</td>
</tr>
</tbody>
</table>

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 $A \land B$ given the possible truth values for $A$ and $B$.

Exercise 1.29. Create a truth table for each of $A \lor B$, $\neg A$, $\neg(A \land B)$, and $\neg A \land \neg B$. Feel free to add additional columns to your tables to assist you with intermediate steps.

Exercise 1.30. Suppose $P$ is a complex proposition built out of the propositions $A$, $B$, and $C$. How many rows would the truth table for $P$ require?

Definition 1.31. Let $A$ and $B$ represent propositions. The conditional proposition “If $A$, then $B$” is expressed symbolically as

$$A \implies B$$

and has the following truth table.

<table>
<thead>
<tr>
<th>$A$</th>
<th>$B$</th>
<th>$A \implies B$</th>
</tr>
</thead>
<tbody>
<tr>
<td>T</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
<td>F</td>
</tr>
<tr>
<td>F</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>F</td>
<td>F</td>
<td>T</td>
</tr>
</tbody>
</table>

Exercise 1.32. 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.

1. $A \land B$
2. $A \lor B$
3. $\neg A$
4. $\neg B$
5. $\neg(A \land B)$
6. $\neg(A \lor B)$
Problem 1.33 Suppose I am the coach of our co-ed dodgeball team and you all are the players. I tell you “If we win tonight, then I will buy you pizza tomorrow.” After reviewing the definition of conditional proposition, determine the case(s) in which you can rightly claim to have been lied to.

Definition 1.34. Two statements are logically equivalent (or equivalent if the context is clear) if and only if they have the same truth table. That is, proposition $P$ is true exactly when proposition $Q$ is true, and $P$ is false exactly when $Q$ is false. When $P$ and $Q$ are logically equivalent we denote this symbolically as

$$ P \iff Q, $$

which we read “$P$ if and only if $Q$”. It is common to abbreviate “if and only if” as “iff”.

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

Theorem 1.35 If $A$ is a proposition, then $\neg(\neg A)$ is equivalent to $A$.

Theorem 1.36 If $A$ and $B$ are propositions, then $\neg (A \land B) \iff \neg A \lor \neg B$. (Note: This theorem is referred to as DeMorgan’s Law.)

Problem 1.37 (*) Let $A$ and $B$ be propositions. Conjecture a statement similar to Theorem 1.36 for the proposition $\neg (A \lor B)$ and then prove it.

Definition 1.38. The converse of $A \implies B$ is $B \implies A$.

Definition 1.39. The contrapositive of $A \implies B$ is $\neg B \implies \neg A$.

Exercise 1.40 Let $A$ and $B$ represent the statements from Exercise 1.32. Express the following in ordinary English sentences.

1. The converse of $A \implies B$

2. The contrapositive of $A \implies B$

Exercise 1.41 Find the contrapositive of the following statements:

1. If $n$ is an even natural number, then $n + 1$ is an odd natural number.

2. If it rains today, then I will bring my umbrella.

3. If it does not rain today, then I will not bring my umbrella.

Exercise 1.42 Provide an example of a true conditional proposition whose converse is false.

Theorem 1.43 Assume $A$ and $B$ are statements. Then $A \implies B$ is equivalent to its contrapositive.

The upshot of Theorem 1.43 is that if you want to prove a conditional proposition, you can prove its contrapositive instead. Prove each of the next two propositions using the contrapositive of the given statement.

Theorem 1.44 (*) Assume $x$ and $y$ are integers. If $xy$ is odd, then both $x$ and $y$ are odd. (Prove using contrapositive.)

Theorem 1.45 (*) Assume $x$ and $y$ are integers. If $xy$ is even, then $x$ or $y$ is even. (Prove using contrapositive.)

\[\text{Despite the fact that each of “$n$ is an even natural number” and “$n + 1$ is an odd natural number” are not propositions (since we cannot determine their truth values without knowing what $n$ is), the implication is a proposition. We discuss this further when we introduce predicates.}\]
1.3 Negating Implications and Proof by Contradiction

So far we have discussed how to negate propositions of the form \( A, A \land B, \) and \( A \lor B \) for propositions \( A \) and \( B \). However, we have yet to discuss how to negate propositions of the form \( A \Rightarrow B \).

**Problem 1.46** Let \( A \) and \( B \) be propositions. Conjecture an equivalent way of expressing the conditional proposition \( A \Rightarrow B \) as a proposition involving the disjunction symbol \( \lor \) and possibly the negation symbol \( \neg \), but not the implication symbol \( \Rightarrow \). Prove your conjecture using a truth table.

**Exercise 1.47** Let \( A \) and \( B \) be the propositions “Darth Vader is a hippie” and “Sarah Palin is a liberal”, respectively. Using Problem 1.46, express \( A \Rightarrow B \) as an English sentence involving the disjunction “or.”

**Problem 1.48** (*) Let \( A \) and \( B \) be two propositions. Conjecture an equivalent way of expressing the proposition \( \neg(A \Rightarrow B) \) as a proposition involving the conjunction symbol \( \land \) and possibly the negation symbol \( \neg \), but not the implication symbol \( \Rightarrow \). Prove your conjecture using previous results.

**Exercise 1.49** Let \( A \) and \( B \) be the propositions in Exercise 1.47. Using Problem 1.48, express \( \neg(A \Rightarrow B) \) as an English sentence involving the conjunction “and.”

**Exercise 1.50** The following proposition is false. Negate this proposition to obtain a true statement. Write your statement as a conjunction.

\[
\text{If } 0.99 = \frac{9}{10} + \frac{9}{100} + \frac{9}{1000} + \cdots, \text{ then } 0.99 \neq 1.
\]

You do not need to prove your new statement.

Recall that a proposition is exclusively either true or false. That is, a proposition can never be both true and false. This idea leads us to the next definition.

**Definition 1.51.** A compound proposition that is always false is called a **contradiction**. A compound statement that is always true is called a **tautology**.

**Theorem 1.52** Let \( A \) be a proposition. Then \( \neg A \land A \) is a contradiction.

**Exercise 1.53** Provide an example of a tautology using arbitrary positions and any of the logical connectives \( \neg, \land, \) and \( \lor \). Then prove that your example is in fact a tautology.

Suppose that we want to prove some proposition \( P \) (which might be something like \( A \Rightarrow B \) or possibly more complicated). One approach, called **proof by contradiction**, involves assuming \( \neg P \) and then logically deducing a contradiction of the form \( Q \land \neg Q \), where \( Q \) is some proposition (possibly equal to \( P \)). Since this is absurd, it cannot be the case that \( \neg P \) is true, which implies that \( P \) is true. The tricky part about a proof by contradiction is that it is not usually obvious what the statement \( Q \) is going to be. Here is what the general structure for a proof by contradiction looks like.

**Skeleton Proof 1.54** (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 \( \neg P \).

\[ \vdots \]

(Use definitions and previous theorems to derive some \( Q \) and its negation \( \neg Q \).)

\[ \vdots \]

This is a contradiction. Therefore, \( P \).

Among other situations, proof by contradiction can be useful for proving statements of the form \( A \implies B \), where \( B \) is worded negatively or \( \neg B \) is easier to “get your hands on.”

**Skeleton Proof 1.55** (Proof of \( A \implies B \) by contradiction). If you want to prove the proposition \( A \implies B \) via a proof by contradiction, then the structure of the proof is as follows.

Proof. For sake of a contradiction, assume \( A \) and \( \neg B \).

\[ \vdots \]

(Use definitions and previous theorems to derive some \( Q \) and its negation \( \neg Q \).)

\[ \vdots \]

This is a contradiction. Therefore, if \( A \), then \( B \). 

**Question 1.56** In Skeleton Proof 1.55, why did we start by assuming \( A \) and \( \neg B \)?

Prove the following theorem in two ways: (i) prove the contrapositive, and (ii) prove using a proof by contradiction.

**Theorem 1.57** (*) 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 by contradiction.

**Theorem 1.58** (*) Assume that \( x, y \in \mathbb{N} \). If \( x \) divides \( y \), then \( x \leq y \). (Prove using a proof by contradiction.)

**Question 1.59** What obstacles (if any) are there to proving the previous theorem directly without using proof by contradiction?

---

\(^{ii}\)Note that \( \mathbb{N} = \{1, 2, 3, \ldots\} \) is the set of natural numbers. Notice that we did not include 0 in the set of natural numbers. It is worth pointing out that there is some disagreement about this—some mathematicians (like set theorists) 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?
1.4 Introduction to Quantification

Recall that sentences of the form “$x > 0$” are not propositions (unless the context of $x$ is perfectly clear). In this case, we call $x$ a free variable. In order to turn a sentence with free variables into a proposition, for each free variable, we need to either substitute in a value (not necessarily a number) for the free variable or we must “quantify” the free variable.

**Definition 1.61.** A sentence with a free variable is called a predicate.

**Exercise 1.62** Give 3 examples of mathematical predicates involving 1, 2, and 3 free variables, respectively.

It is convenient to borrow function notation 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 “:=” is often used in mathematics to show that we are defining something (as opposed to stating something is mathematically equal). Also, note that the use of the quotation marks above removed some ambiguity. If we wrote $S(x) = x^2 - 4 = 0$, it would look 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, then $P(x_0)$ is now a proposition (and may be true or false).

**Exercise 1.63** Consider $S(x)$ and $L(a, b)$ from the discussion above. Determine the truth values of $S(2)$, $S(0)$, $S(-2)$, $L(1, 2)$, $L(2, 1)$, and $L(-3, -2)$.

**Exercise 1.64** Again, consider $L(a, b)$ from above. Is $L(2, b)$ a proposition or a predicate? Explain your answer.

Besides substituting specific values in for free variables in a predicate, there are (at least) two other ways in which we can use predicates to build propositions. We do this by making a claim about which values of the free variables apply to the predicate.

**Example 1.65.** The following sentences are both propositions.

1. For all $x \in \mathbb{R}$, $x^2 - 4 = 0$.
2. There exists $x \in \mathbb{R}$ such that $x^2 - 4 = 0$.

**Exercise 1.66** Determine the truth value of the two propositions from Example 1.65. What would it take to prove your answers?

**Definition 1.67.** “For all” is called the universal quantifier and “there exists...such that” is called the existential quantifier.
The variables in propositions associated with quantifiers are called **bound variables**. In order for a sentence containing variables to be a proposition, all variables must be bound. In other words, to be a proposition, all variables need to be quantified so that there is no ambiguity.

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

We must also take care that the universe of acceptable values for bound variables is clear. Consider for a moment the proposition “For all \( x \), \( x > 0 \).” Is this proposition true or false? The answer depends on what \( x \)’s we are taking all of. For example, if the universe of discourse is the set of integers, then the proposition is false. However, if we take the universe of acceptable values to be the natural numbers, then the proposition is true. We must be careful to avoid such ambiguities. Often, the context can resolve such ambiguities, but otherwise, we need to write things like: “For all \( x \in \mathbb{Z} \), \( x > 0 \)” or “For all \( x \in \mathbb{N} \), \( x > 0 \).”

**Exercise 1.68** Suppose our universe of acceptable values is the set of integers.

1. Provide an example of a predicate \( P(x) \) such that “For all \( x \), \( P(x) \)” is true.

2. 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 1.69** Let \( P(x,y) \) be a predicate with the free variables \( x \) and \( y \) (and let’s assume the universe of discourse is clear). Write down all possible ways (where order matters) that the variables could be quantified. To get you started, here’s one: For all \( x \), there exists \( y \) such that \( P(x,y) \). Find the rest.

**Problem 1.70** Are there any propositions on your list from Exercise 1.69 that are equivalent to others on your list?

**Exercise 1.71** Suppose that the universe of acceptable values is the set of married people. Consider the predicate \( M(x,y) := “x \ is married to \( y “ \). Discuss the meaning of each of the following.

1. For all \( x \), there exists \( y \) such that \( M(x,y) \).

2. There exists \( y \) such that for all \( x \), \( M(x,y) \).

**Exercise 1.72** Suppose that the universe of acceptable values is the set of real numbers. Consider the predicate \( R(x,y) := “x = y^2 \). Discuss the meaning of each of the following.

1. There exists \( x \) such that there exists \( y \) such that \( R(x,y) \).

2. There exists \( y \) such that there exists \( x \) such that \( R(x,y) \).

**Exercise 1.73** Repeat the exercise above but replace the existential quantifiers with universal quantifiers.

**Problem 1.74** Conjecture a summary of the various possibilities for quantifying predicates involving two variables. You do not need to prove your conjecture.

**Exercise 1.75** Suppose that the universe of acceptable values is the set of real numbers. Consider the predicate \( G(x,y) := “x > y \). Find all possible distinct ways to bind the variables to create propositions and then determine the truth value of each (you do not need to prove your answers).
1.5 More on Quantification

In the last section, we introduced the universal quantifier “for all” and the existential quantifier “there exists... such that.” Here are a couple of important points to remember about quantification:

1. In order to have a proposition, all variables must be bound. That is, all variables must be quantified. This can happen in at least two ways:
   
   (a) The variables are explicitly bound by quantifiers in the same sentence, or
   
   (b) The variables are implicitly bound by preceding sentences and/or by context. *Note:* Statements of the form “Let $x = ...$” and “Let $x \in ...$” bind the variable $x$ and remove ambiguity.

2. The order of the quantification is important. Reversing the order of the quantifiers can substantially change the meaning of a proposition.

Using our logical connectives (“and”, “or”, “If..., then...”, and “not”) together with quantification, we can build very complex mathematical statements.

**Example 1.76.** Let $f$ be a function and consider the formal definition of the calculus statement

$$\lim_{x \to c} f(x) = L.$$ 

This statement about the limit of $f(x)$ at $x = c$ is equivalent to:

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

**Exercise 1.77** Identify all the quantifiers from Example 1.76 and any logical connectives. Are there any implicit bound variables?

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

**Definition 1.78.** We use the symbol $\forall$ to denote the universal quantifier “for all” and the symbol $\exists$ to denote the existential quantifier “there exists... such that”.\(^{iii}\)

Using our abbreviations for the logical connectives and quantifiers, we can symbolically represent mathematical propositions.

**Example 1.79.** For each of the following, suppose our universe of discourse is the set of real numbers.

1. Consider the following (true) proposition:

   There exists $x$ such that $x^2 - 1 = 0$.

   This proposition can be denoted symbolically as $(\exists x)(x^2 - 1 = 0)$.

2. Consider the following (false) proposition:

   For all $x \in \mathbb{N}$, there exists $y \in \mathbb{N}$ such that $y < x$.

   This one can be represented symbolically as $(\forall x)(x \in \mathbb{N} \implies (\exists y)(y \in \mathbb{N} \implies y < x))$ or more simply as $(\forall x \in \mathbb{N})(\exists y \in \mathbb{N})(y < x)$.

\(^{iii}\)The \TeX symbol commands are \texttt{\textbackslash forall} and \texttt{\textbackslash exists}, respectively. Here’s something fun: What does $\forall \exists \exists$ mean? Answer in the next section.
3. Consider the following (true) proposition:

Every positive real number has a multiplicative inverse.

There are several ways of representing this statement symbolically. However, if you unpack what a multiplicative inverse is, you’ll get something like \((\forall x)(x > 0 \implies (\exists y)(xy = 1))\). Alternatively, you can shorten the statement to \((\forall x > 0)(\exists y)(xy = 1)\).

**Exercise 1.80** Convert the following statements into statements using only logical symbols. Assume that the universe of discourse is the set of real numbers.

1. There exists a number \(x\) such that \(x^2 + 1\) is greater than zero.
2. There exists a natural number \(n\) such that \(n^2 = 36\).
3. For every real number \(x\), \(x^2\) is greater than or equal to zero.

**Exercise 1.81** Express the definition of the limit in Example 1.76 using only logic symbols.

**Remark 1.82.** If \(A(x)\) and \(B(x)\) are predicates, then it is standard practice for the statement \(A(x) \implies B(x)\) 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 1.83** Find at least two examples earlier in the notes that exhibit the claim made in Remark 1.82. Attempt to write the statements symbolically using explicit quantifiers.

**Exercise 1.84** Convert the following proposition into a statement using only logical symbols. The universe of discourse is the set of real numbers. (Watch out for implicit quantifiers.)

If \(\epsilon > 0\), then there exists \(N \in \mathbb{N}\) such that \(\frac{1}{N} < \epsilon\).

Is this statement true?

**Exercise 1.85** In the last exercise, you should end up with more than one quantifier. Reverse the order of the quantifiers to get a new statement. Does the meaning of the statement change? If so, how does it change? Is the new statement true?

**Remark 1.86.** The symbolic expression \((\forall x)(\forall y)\) can be replaced with the simpler expression \((\forall x, y)\) as long as \(x\) and \(y\) are coming from the same set.

**Exercise 1.87** For each of the following statements, (i) unpack the statement into words, and (ii) determine whether the statement is true or false.

1. \((\forall n \in \mathbb{N})(n^2 \geq 5)\)
2. \((\exists n \in \mathbb{N})(n^2 - 1 = 0)\)
3. \((\exists N \in \mathbb{N})(\forall n > N)(\frac{1}{n} < 0.01)\)
4. \((\forall m, n \in \mathbb{Z})(2|m \land 2|n \implies 2|(m + n))\)
5. \((\forall x \in \mathbb{N})(\exists y \in \mathbb{N})(x - 2y = 0)\)
6. \((\exists x \in \mathbb{N})(\forall y \in \mathbb{N})(y \leq x)\)

To whet your appetite for the next section, tackle the following questions.

**Question 1.88** If a statement is false, then its negation is true. How would you go about negating a statement involving quantifiers? In particular, if \(P(x)\) is a predicate, what are the negations of \((\forall x)(P(x))\) and \((\exists x)(P(x))\), respectively?
1.6 And Even More on Quantification

Before we get started, it is important to remind you that we will not be explicitly using 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 1.89.** Two quantified propositions are **equivalent in a given universe of discourse** iff they have the same truth value in that universe. Two quantified propositions are **equivalent** iff they are equivalent in every universe of discourse.

**Exercise 1.90** Consider the propositions \((\forall x)(x > 3)\) and \((\forall x)(x \geq 4)\). Are these propositions equivalent if the universe of discourse is the set of integers? (Hint: What are their truth values in this case?) Come up with two different universes of discourse that yield different truth values for these propositions. What can you conclude?

**Remark 1.91.** At this point 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, the logical form is neither true or false. 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.

**Theorem 1.92** Let \(P(x)\) be a predicate. Then

1. \(\neg(\forall x)P(x)\) is equivalent to \((\exists x)(\neg P(x))\);

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

**Exercise 1.93** Negate each of the following. Disregard the truth value and the universe of discourse.

1. \((\forall x)(x > 3)\)

2. \((\exists x)(x \text{ is prime} \land x \text{ is even})\)

3. All cars are red.

4. Every Wookiee is named Chewbacca.

5. Some hippies are republican.

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

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

8. There does not exist a function \(f\) such that if \(f\) is continuous, then \(f\) is not differentiable.

Using Theorem 1.92 and our previous results involving quantification, we can negate complex mathematical propositions by working from left to right.
Example 1.94. Consider the proposition
\[(\exists x \in \mathbb{R})(\forall y \in \mathbb{R})(x + y = 0)\].

It turns out that this statement is false, which means that its negation is true. That is,
\[\neg(\exists x \in \mathbb{R})(\forall y \in \mathbb{R})(x + y = 0),\]
which is equivalent to
\[(\forall x \in \mathbb{R})(\exists y \in \mathbb{R})(x + y \neq 0),\]
is true.

Example 1.95. Consider the proposition
\[(\forall x)(x > 0 \implies (\exists y)(y < 0 \land xy > 0))\]
(which happens to be false). Then
\[\neg(\forall x)[x > 0 \implies (\exists y)(y < 0 \land xy > 0)]\]
is equivalent to
\[(\exists x)[x > 0 \land \neg(\exists y)(y < 0) \land xy > 0],\]
which is equivalent to
\[(\exists x)[x > 0 \land (\forall y)(y \geq 0 \lor xy \leq 0)].\]

Exercise 1.96  What previous theorems were used when negating the proposition in the previous example?

Exercise 1.97  Negate each of the following. Disregard the truth value and the universe of discourse.

1. \((\forall n \in \mathbb{N})(\exists m \in \mathbb{N})(m < n)\)
2. \((\forall x, y, z \in \mathbb{Z})(xy \text{ is even} \land yz \text{ is even}) \implies xy \text{ is even}\)
3. For all positive real numbers \(x\) there exists a real number \(y\) such that \(y^2 = x\).
4. 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 1.98 (Direct Proof of \((\forall x)P(x)\)). Here is what the general structure for a direct proof of the proposition \((\forall x)P(x)\) looks like.

\[\text{Proof. Let } x \in U \text{ (where } U \text{ is whatever the universe of discourse is).}\]
\[\vdots\]
\[(\text{Use definitions and previous results.})\]
\[\vdots\]

Therefore, \(P(x)\) is true. Since \(x\) was arbitrary, for all \(x\), \(P(x)\).
1.6. **AND EVEN MORE ON QUANTIFICATION**

**Skeleton Proof 1.99** (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 \(x \in U\) (where \(U\) is whatever the universe of discourse is) such that \(\neg P(x)\).

\[
\vdots
\]

(Do something to derive a contradiction.)

\[
\vdots
\]

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

**Skeleton Proof 1.100** (Direct Proof of \((\exists x)P(x)\)). Here is what the general structure for a direct proof of the proposition \((\exists x)P(x)\) looks like.

**Proof.** (Either use definitions and previous results to deduce that an \(x\) exists such that \(P(x)\) is true or if you think you have an \(x\) that works, just verify that it does.)

\[
\vdots
\]

(Do stuff.)

\[
\vdots
\]

Therefore, there exists \(x\) such that \(P(x)\).

**Skeleton Proof 1.101** (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 \(x\), \(\neg P(x)\).

\[
\vdots
\]

(Do something to derive a contradiction.)

\[
\vdots
\]

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

**Question 1.102** Suppose \(P(x)\) is a proposition such that \((\forall x)P(x)\) is false. Which of the above proof situations is identical to providing a counterexample to this proposition?

**Remark 1.103.** 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 1.104** 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.

1. For all \(n \in \mathbb{N}\), \(n^2 \geq 5\).
2. There exists \(n \in \mathbb{N}\) such that \(n^2 - 1 = 0\).
3. There exists \(x \in \mathbb{N}\) such that for all \(y \in \mathbb{N}\), \(y \leq x\).
4. For all $x \in \mathbb{Z}$, $x^3 \geq x$.

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

6. There exists integers $a$ and $b$ such that $2a + 7b = 1$.

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

8. For all integers $a, b, c$, if $a$ divides $bc$, then either $a$ divides $b$ or $a$ divides $c$.

\text{iv}

What does $\forall \exists \exists$ mean? For every upside-down A, there exists a backwards E, of course :).
Chapter 2

Introduction to 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.

2.1 Sets

**Definition 2.1.** 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 $x \notin A$.

**Definition 2.2.** 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 containing some stuff, then the empty set is a box with nothing in it.

**Definition 2.3.** The language associated to sets is specific. We will often define sets using the following notation, called set builder notation.

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

The first part “$x \in A$” denotes what type of $x$ is being considered. The statements to the right of the colon 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 $A$.

**Exercise 2.4** Unpack each of the following sets into a description using a sentence and see if you can determine exactly what elements each set contains.

1. $M = \{ x \in \mathbb{R} : x \geq 2 \}$
2. $A = \{ x \in \mathbb{N} : x = 3k \text{ for some } k \in \mathbb{N} \}$
3. $T = \{ t \in \mathbb{R} : t^2 \leq 2 \}$
4. $H = \{ t \in \mathbb{R} : t = 1 - \frac{1}{n}, \text{ where } n \in \mathbb{N} \}$

Often, a vertical bar is used instead of a colon, like $S = \{ x \in A \mid x \text{ satisfies some condition} \}$. 

17
**Exercise 2.5** Write each of the following sentences using set builder notation.

1. Suppose \( R \) is the set of all real numbers \( x \) such that \( x \) is less than \(-\sqrt{2}\).
2. Suppose \( A \) is the set of all real numbers \( y \), such that \( y \) is greater than \(-12\) and less than \(42.4\).
3. Suppose \( D \) is the set of all even natural numbers.

**Definition 2.6.** If \( A \) and \( B \) are sets, then we say that \( A \) is a **subset** of \( B \), written \( A \subseteq B \), provided that every element of \( A \) is also an element of \( B \).

**Remark 2.7.** 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 \( A \subseteq B \).

**Question 2.8** Suppose that \( A \) and \( B \) are sets. Describe a general strategy for proving that \( A \subseteq B \).

**Theorem 2.9** Let \( S \) be a set. Then

1. \( S \subseteq S \),
2. \( \emptyset \subseteq S \).

**Exercise 2.10** List all of the subsets of \( A = \{1, 2, 3\} \). Any conjectures about how many there might be for a set with \( n \) elements?

**Theorem 2.11** (*, Transitivity of subsets) Suppose that \( A, B, \) and \( C \) are sets. If \( A \subseteq B \) and \( B \subseteq C \), then \( A \subseteq C \).

**Definition 2.12.** If \( A \subseteq B \), then \( A \) is called a **proper subset** provided that \( A \neq B \). In this case, we may write \( A \subset B \) or \( A \nsubseteq B \).\(^i\)

**Definition 2.13** (Interval Notation). For \( a, b \in \mathbb{R} \) with \( a < b \), we define the following.

1. \((a, b) = \{x \in \mathbb{R} : a < x < b\}\)
2. \((a, \infty) = \{x \in \mathbb{R} : a < x\}\)
3. \((-\infty, b) = \{x \in \mathbb{R} : x < b\}\)
4. \([a, b] = \{x \in \mathbb{R} : a \leq x \leq b\}\)

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

**Exercise 2.14** Provide two examples of proper subsets of the interval \([0, 1]\).

Here are some more definitions. In each case, take \( U \) to be the universe of discourse.

**Definition 2.15.** The **union** of the sets \( A \) and \( B \) is \( A \cup B = \{x \in U : x \in A \text{ or } x \in B\} \).

**Definition 2.16.** The **intersection** of the sets \( A \) and \( B \) is \( A \cap B = \{x \in U : x \in A \text{ and } x \in B\} \).

**Definition 2.17.** The **set difference** of the sets \( A \) and \( B \) is \( A \setminus B = \{x \in U : x \in A \text{ and } x \notin B\} \).

\(^i\)Warning: Some books use \( \subset \) to mean \( \subseteq \).
Definition 2.18. The complement of $A$ (relative to $U$) is the set $A^c = U \setminus A = \{x \in U : x \notin A\}$.

Definition 2.19. 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 2.20 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.

1. $A \cap C$
2. $A \cap B$
3. $A \cup C$
4. $A \cup B$
5. $A \setminus B$
6. $B \setminus A$
7. $C \setminus B$
8. $B \cap C$
9. $B^c$
10. $A^c$
11. $(A \cup B)^c$
12. $A^c \cap B^c$

Exercise 2.21 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.

1. $A^c$
2. $A \cap C$
3. $A \cap B$
4. $A \cup C$
5. $A \cup B$
6. $(A \cap B)^c$
7. $(A \cup B)^c$
8. $A \setminus B$
9. $A \setminus (B \cup C)$
10. $B \setminus A$
11. $B \cap C$

Theorem 2.22 (\*) Let $A$ and $B$ be sets. If $A \subseteq B$, then $B^c \subseteq A^c$. 
Definition 2.23. Two sets $A$ and $B$ are equal if and only if $A \subseteq B$ and $B \subseteq A$. In this case we write $A = B$.

Remark 2.24. 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 $B \subseteq A$.

Theorem 2.25 (*). Let $A$ and $B$ be sets. Then $A \setminus B = A \cap B^c$.

Theorem 2.26 (*, DeMorgan’s Law). Let $A$ and $B$ be sets. Then

1. $(A \cup B)^c = A^c \cap B^c$;
2. $(A \cap B)^c = A^c \cup B^c$.

(You only need to prove one of these; the other is similar.)

Theorem 2.27 (*, Distribution of Union and Intersection). Let $A$, $B$, and $C$ be sets. Then

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

(You only need to prove one of these; the other is similar.)
2.2 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 2.28.** 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 $P(S)$.

**Remark 2.29.** It follows immediately from the definition that $A \subseteq S$ if and only if $A \in P(S)$. It is important to pay close attention to whether “⊆” or “∈” is the proper symbol to use.

**Example 2.30.** If $S = \{a, b\}$, then $P(S) = \{\emptyset, \{a\}, \{b\}, S\}$.

**Question 2.31** Implicit in the definition of power set is that $S$ is a subset of some fixed universe $U$. What universe does it make sense for $P(S)$ to live in?

**Exercise 2.32** For each of the following sets, find the power set.

1. $W = \{\circ, \triangle, \square\}$
2. $O = \{a, \{a\}\}$
3. $R = \emptyset$
4. $D = \{\emptyset\}$

**Conjecture 2.33** 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.

**Exercise 2.34** Do your best to describe $P(N)$. You cannot write down all of $P(N)$. Why not?

**Remark 2.35.** 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 $P(A)$. This can get confusing rather quickly. Consider the set $O$ from the previous example. The set $\{a\}$ happens to be an element of $O$, a subset of $O$, and an element of $P(O)$.

**(Theorem 2.36)** Let $S$ and $T$ be sets. Then $S \subseteq T$ if and only if $P(S) \subseteq P(T)$.

**(Theorem 2.37)** Let $S$ and $T$ be sets. Then $P(S) \cap P(T) = P(S \cap T)$.

**(Theorem 2.38)** Let $S$ and $T$ be sets. Then $P(S) \cup P(T) \subseteq P(S \cup T)$.

**Exercise 2.39** Let $S$ and $T$ be sets.

1. Provide a counterexample to show that it is not necessarily true that $P(S) \cup P(T) = P(S \cup T)$.
2. Is it ever true that $P(S) \cup P(T) = P(S \cup T)$ or are $P(S) \cup P(T)$ and $P(S \cup T)$ always different sets?

---

*Recall that “iff” is an abbreviation for “if and only if”, which is a statement of the form $A \iff B$ for propositions $A$ and $B$. Recall that this is short for both $A \implies B$ and $B \implies A$.

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

---
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 2.40** Discuss the Barber of Seville Paradox. Does the barber shave himself or not?

Problem 2.40 is an example of a paradox. I haven’t defined paradox. What do you think it means? Now, suppose that there is a set of all sets and call it \( U \). Then we can write \( U = \{ A : A \text{ is a set} \} \).

**Problem 2.41** Given our definition of \( U \), explain why it 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.

**Question 2.42** 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 the paradoxes is to conclude that there is no set of all sets. Here is some more evidence that we shouldn’t assume the existence of a set of all sets.

**Question 2.43** If \( U \) is the set of all sets, then what is the relationship between \( U \) and \( P(U) \)? What about \( P(P(U)) \)?

The upshot is that the collection of all sets is not a set! Here are some additional paradoxes.

**Problem 2.44** Pick any two of the paradoxes below and explain why it is a paradox.

**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?

**Liar’s Paradox.** Consider the statement: this sentence is false. Is it true or false?

**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!
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 $t \in \mathbb{N} - S$. 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.

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.
2.3 Indexing Sets

Suppose we wish to 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 on the capital letters 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 \( \{1, 2, \ldots, 26\} \).

**Remark 2.45.** 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. For example, we might use \( \Delta \) (capital delta) to refer to an indexing set and write \( \alpha \in \Delta \) for an individual index. Typically, if the indexing set is some subset of \( \mathbb{Z} \) (like \( \mathbb{N} \)), then we would use letters like \( k, m, n, l \) for an individual index. Likewise, if the indexing set is \( \mathbb{R} \), then we might use \( s, t, x, y \) as indices.

**Example 2.46.** Here are some examples of common notation that you will encounter.

1. If \( \Delta \) is a set and we have a collection of sets indexed by \( \Delta \), 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.”

2. If a collection of sets is indexed by the natural numbers, then we may write

\[ \{U_n\}_{n \in \mathbb{N}} \]

or

\[ \{U_n\}_{n=1}^\infty \]

3. Borrowing from this idea, we can write the collection \( \{A_1, \ldots, A_{26}\} \) from the beginning of the section as

\[ \{A_n\}_{n=1}^{26} \]
2.3. INDEXING SETS

Definition 2.47. Suppose we have a collection \( \{ A_\alpha \}_{\alpha \in \Delta} \).

1. The \textbf{union of the entire collection} is defined via
\[
\bigcup_{\alpha \in \Delta} A_\alpha = \{ x : x \in A_\alpha \text{ for some } \alpha \in \Delta \}.
\]

2. The \textbf{intersection of the entire collection} is defined via
\[
\bigcap_{\alpha \in \Delta} A_\alpha = \{ x : x \in A_\alpha \text{ for all } \alpha \in \Delta \}.
\]

Example 2.48. In the special case that \( \Delta = \mathbb{N} \), we write
\[
\bigcup_{n=1}^{\infty} A_n = \{ x : x \in A_n \text{ for some } n \in \mathbb{N} \} = A_1 \cup A_2 \cup A_3 \cup \cdots
\]
and
\[
\bigcap_{n=1}^{\infty} A_n = \{ x : x \in A_n \text{ for all } n \in \mathbb{N} \} = A_1 \cap A_2 \cap A_3 \cap \cdots
\]
Similarly, if \( \Delta = \{1, 2, 3, 4\} \), then
\[
\bigcup_{n=1}^{4} A_n = A_1 \cup A_2 \cup A_3 \cup A_4
\]
and
\[
\bigcap_{n=1}^{4} A_n = A_1 \cap A_2 \cap A_3 \cap A_4.
\]

Remark 2.49. Notice the difference between “\( \bigcup \)” and “\( \cup \)” (respectively, “\( \bigcap \)” and “\( \cap \)”). The larger versions of the union and intersection symbols very much like the notation that you’ve likely seen for sums (e.g., \( \sum_{i=1}^{\infty} i^2 \)).

Exercise 2.50. Let \( \{ I_n \}_{n \in \mathbb{N}} \) be the collection of open intervals from the beginning of the section. Find each of the following.

1. \( \bigcup_{n \in \mathbb{N}} I_n \)
2. \( \bigcap_{n \in \mathbb{N}} I_n \)

Exercise 2.51. Repeat the previous exercise, but assume that the sets are closed intervals.

Exercise 2.52. Let \( \{ A_n \}_{n=1}^{26} \) be the collection from earlier in the section. Find each of the following.

1. \( \bigcup_{n=1}^{26} A_n \)
2. $\bigcap_{n=1}^{26} A_n$

**Exercise 2.53** Let $S_n = \{x \in \mathbb{R} : n - 1 < x < n\}$, where $n \in \mathbb{N}$. Find each of the following.

1. $\bigcup_{n=1}^{\infty} S_n$
2. $\bigcap_{n=1}^{\infty} S_n$

**Exercise 2.54** Let $T_n = \{x \in \mathbb{R} : -\frac{1}{n} < x < \frac{1}{n}\}$, where $n \in \mathbb{N}$. Find each of the following.

1. $\bigcup_{n=1}^{\infty} T_n$
2. $\bigcap_{n=1}^{\infty} T_n$

**Exercise 2.55** 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.

1. $\bigcup_{r \in \mathbb{Q}} N_r$
2. $\bigcap_{r \in \mathbb{Q}} N_r$

**Definition 2.56.** We say that a collection of sets $\{A_\alpha\}_{\alpha \in \Delta}$ is **pairwise disjoint** if $A_\alpha \cap A_\beta = \emptyset$ whenever $\alpha \neq \beta$.

**Exercise 2.57** Draw a Venn diagram of a collection of 3 sets that are pairwise disjoint.

**Exercise 2.58** 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

$$\bigcap_{n=1}^{3} A_n = \emptyset.$$

**Theorem 2.59** (*, Generalized Distribution of Union and Intersection) Suppose we have a collection $\{A_\alpha\}_{\alpha \in \Delta}$. Let $B$ be any set. Then

1. $B \cup \left( \bigcap_{\alpha \in \Delta} A_\alpha \right) = \bigcap_{\alpha \in \Delta} (B \cup A_\alpha)$,
2. $B \cap \left( \bigcup_{\alpha \in \Delta} A_\alpha \right) = \bigcup_{\alpha \in \Delta} (B \cap A_\alpha)$.

(You only need to prove one of these; the other is similar.)
Theorem 2.60 (*, Generalized DeMorgan’s Law) Suppose we have a collection \( \{A_\alpha\}_{\alpha \in \Delta} \).

Then

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

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

(You only need to prove one of these; the other is similar.)
2.4 Basic Topology of $\mathbb{R}$

Remark 2.61. 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 2.62.** If $p$ and $q$ are two different real numbers in $\mathbb{R}$, then there is a number between them.

**Exercise 2.63** 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 example, but this exercise is asking you to produce an actual candidate.)

**Axiom 2.64.** (Linear ordering) If $a$, $b$, and $c$ are real numbers, then:
1. If $a < b$ and $b < c$, then $a < c$;
2. Exactly one of the following is true: (i) $a < b$, (ii) $a = b$, or (iii) $a > b$.

**Axiom 2.65.** If $p$ is a real number, then there exists $q, r \in \mathbb{R}$ such that $q < p < r$.

**Axiom 2.66.** (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 2.67.** 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.

**Remark 2.68.** In this class, we will always assume that any time we write $(a, b), [a, b], (a, b], or [a, b)$ that $a < b$.

**Exercise 2.69** Give an example of each of the following.
1. An open interval.
2. A closed interval.
3. An interval that is neither open nor closed.
4. An infinite set that is not an interval.

**Definition 2.70.** A set $U$ is called an **open set** iff 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 2.71** Prove that the set $I = (1, 2)$ is an open set.

**Theorem 2.72** (*) Every open interval is an open set.

**Theorem 2.73** The real numbers form an open set.

**Exercise 2.74** Provide an example of an open set that is not a single open interval.

**Theorem 2.75** (*) Every closed interval is not an open set.
Let $x \in \mathbb{R}$. Then the set $\{x\}$ is not open.

Determine whether $\{4, 17, 42\}$ is an open set, and briefly justify your assertion.

Let $A$ and $B$ be open sets. Then $A \cup B$ is an open set.

Let $A$ and $B$ be open sets. Then $A \cap B$ is an open set.

Let $\{U_\alpha\}_{\alpha \in \Delta}$ be a collection of open sets. Then

$$\bigcup_{\alpha \in \Delta} U_\alpha$$

is an open set.

1. Find a collection of open sets $\{U_\alpha\}_{\alpha \in \Delta}$ such that

$$\bigcap_{\alpha \in \Delta} U_\alpha$$

is not an open set.

2. Find a collection of open sets $\{B_\alpha\}_{\alpha \in \Delta}$ such that

$$\bigcap_{\alpha \in \Delta} B_\alpha$$

is an open set.

Taken together, Theorems 2.78–2.80 and Exercise 2.81 tell us that the union 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.

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

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

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

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

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

1. The points 1 and 2 are limit points of $S$.

2. If $p \in S$, then $p$ is a limit point of $S$.

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

A point $p$ is a limit point of $(a, b)$ iff $p \in [a, b]$. 

Problem 2.87  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 2.88  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 2.89  Provide an example of a set $T$ with exactly two limit points.

Theorem 2.90  If $p \in \mathbb{R}$, then $p$ is a limit point of $\mathbb{Q}$.

Definition 2.91. A set is called **closed** iff it contains all of its limit points.

Exercise 2.92  Provide an example of each of the following. You do not need to prove that your answers are correct.

1. A closed set.
2. A set that is not closed.
3. A set that is open and closed.
4. A set that neither open nor closed.

Theorem 2.93  (*) The set $[a, b]$ is closed.

Theorem 2.94  The set $U$ is open iff $U^C$ is closed.

Theorem 2.95  (*) Every finite set is closed.

Problem 2.96  Prove or provide a counterexample: If a set $S$ is not open, then it is closed.

Theorem 2.97  The real numbers are both open and closed.

Theorem 2.98  The rational numbers are neither open nor closed.

Theorem 2.99  The empty set is both open and closed.

Theorem 2.100  (*) Let $\{A_\alpha\}_{\alpha \in \Delta}$ be a collection of closed sets. Then

$$\bigcap_{\alpha \in \Delta} A_\alpha$$

is a closed set.

Problem 2.101  Prove or provide a counterexample: If $A$ and $B$ are closed sets, then $A \cup B$ is also closed.

Exercise 2.102  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 2.103. You should compare what happened in Theorem 2.100 and Exercise 2.102 to what we stated in Remark 2.82.
2.5 Induction

In this section, we will explore a technique for proving statements of the form \((\forall n \in \mathbb{N})P(n)\), where \(P(n)\) is some predicate. Notice that this is a statement about natural numbers and not some other set. Consider the claims:

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

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

Let’s take a look at potential proofs.

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

"Proof" of Claim (2). 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? The answer is 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 2.104** (Axiom of Induction). Let \(S \subseteq \mathbb{N}\) such that both

1. \(1 \in S\), and
2. if \(k \in S\), then \(k + 1 \in S\).

Then \(S = \mathbb{N}\).

**Remark 2.105.** 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. I like to think of the first hypothesis of the Axiom of Induction as saying that we have a first rung of a ladder. The second hypothesis says that if we have some random rung, 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 so on. Again, we are assuming that the “and so on” works as expected here.

**Theorem 2.106** (Principle of Mathematical Induction, \(*\) Let \(P(1), P(2), P(3), \ldots\) be a sequence of statements, one for each natural number.\(^v\) Assume

1. \(P(1)\) is true, and
2. If \(P(k)\) is true, then \(P(k + 1)\) is true.

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

\(^v\) In this case, you should think of \(P(n)\) as a predicate, where \(P(1)\) is the statement that corresponds to substituting in the value 1 for \(n\).

\(^vi\) *Hint:* Let \(S = \{k \in \mathbb{N} : P_k\text{ is true}\}\) 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 \(\mathbb{N}\).
Remark 2.107. The Principal 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 (1) above is called the base step while (2) is called the inductive step.

Skeleton Proof 2.108 (Proof by induction for \((\forall n \in \mathbb{N})P(n)\)). Here is what the general structure for a proof by induction looks like. Remarks are in parentheses.

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. Don’t assume that they are equal!)

(ii) Inductive step: (Your goal is to prove that “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. (Now, do some stuff to show that \( P(k + 1) \) is true.) Therefore, \( P(k + 1) \) is true.

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

Theorem 2.109 (*) For all \( n \in \mathbb{N} \), \( \sum_{i=1}^{n} i = \frac{n(n + 1)}{2} \).

Theorem 2.110 (*) For all \( n \in \mathbb{N} \), \( 3 \) divides \( 4^n - 1 \).

Theorem 2.111 (*) For all \( n \in \mathbb{N} \), \( 6 \) divides \( n^3 - n \).

Theorem 2.112 (*) 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 \( \frac{n^2 - n}{2} \).

Theorem 2.113 (*) Let \( A \) be a set with \( n \) elements. Then \( P(A) \) is a set with \( 2^n \) elements.

---

\(^{\text{vii}}\)Recall that \( \sum_{i=1}^{n} i = 1 + 2 + 3 + \cdots + n \), by definition. Also, this theorem should look familiar from calculus.

\(^{\text{viii}}\)We encountered this theorem before as Conjecture 2.33.
Chapter 3

Two Famous Theorems

3.1 The irrationality of $\sqrt{2}$

In this section we will prove one of the oldest and most important theorems in mathematics. 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 3.1). In today’s language, Hipassus discovery is “$\sqrt{2}$ is irrational” (see Theorem 3.5).

![Figure 3.1: The side and diagonal of a square are incommensurable.](image)

Before tackling a proof of Theorem 3.5, we need a few tools. In particular, we will make use of the Fundamental Theorem of Arithmetic (see Corollary 3.4). The following result makes up half of the Fundamental Theorem of Arithmetic.

**Theorem 3.1** (*)  Let $n$ be a natural number greater than 1. Then $n$ can be expressed as a

---

1. This section is derived from work of Dave Richeson of Dickinson College.

2. Recall that a number is rational if it can be written in the form $\frac{m}{n}$, where $m, n \in \mathbb{Z}$ and $n \neq 0$. A number is irrational if it is not rational.
product of primes. That is, we can write
\[ n = p_1 p_2 \cdots p_k, \]
where each of \( p_1, p_2, \ldots, p_k \) are prime numbers (and there may possibly be repeats in this list).iii

The previous theorem states that we can write every natural number as a product of primes, but it does not say that the primes and the number of times the primes appear are unique. It turns out that this is fairly difficult to prove. We will need the following result known as the Division Algorithm, but we won’t worry about proving it. Instead, we will take it for granted and use it in the proof of Theorem 3.2, which we will then use to prove uniqueness.

**Theorem 3.1** (Division Algorithm). Suppose that \( m, n \in \mathbb{N} \). Then there exists unique \( q, r \in \mathbb{N} \) 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. Now, see if you can prove the following theorem, which is known as Euclid’s Lemma.

**Theorem 3.2** (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 \( b \).iv

Alright, let’s tackle the uniqueness of the product of primes now.

**Theorem 3.3** (*) Let \( n \) be a natural number greater than 1. Then the expression for \( n \) as the product of one or more primes is unique (up to the order in which they appear).v

The following corollary follows immediately from Theorem 3.1 and Theorem 3.3.

**Corollary 3.4** (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.

We are finally ready to prove that \( \sqrt{2} \) is irrational.

**Theorem 3.5** (*) The real number \( \sqrt{2} \) is irrational.vi

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.

Now, let’s tackle a few more problems dealing with irrational numbers.

**Problem 3.6** Determine whether \( \frac{1 + \sqrt{2}}{3 + 2\sqrt{2}} \) is rational or irrational and then prove that your answer is correct.

---

iii *Hint:* Use a proof by contradiction. Let \( n \) be the smallest natural number for which the theorem fails. 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 \( n \).

iv *Hint:* Use a proof by contradiction and apply the Division Algorithm to both \( a \) and \( b \). What can you say about \( ab \)?

v *Hint:* Use a proof by contradiction. Write \( n \) as both \( p_1 p_2 \cdots p_k \) and \( q_1 q_2 \cdots q_l \), where both are products of primes. Use Euclid’s Lemma to derive a contradiction.

vi *Hint:* Use a proof by contradiction. That is, suppose that there exist \( m, n \in \mathbb{Z} \) such that \( n \neq 0 \) and \( \sqrt{2} = \frac{m}{n} \). Next, square both sides and solve for \( m^2 \). How many factors of 2 does \( m^2 \) have? How many factors of 2 does \( 2n^2 \) have? Derive a contradiction using Corollary 3.4.
3.1. **THE IRRATIONALITY OF $\sqrt{2}$**

**Theorem 3.7** (*) Let $p$ be a prime number. Then $\sqrt{p}$ is irrational.

**Exercise 3.8** Let $p$ be a prime number. For which values of $n \in \mathbb{N}$ is $\sqrt{p}$ irrational? You do not need to prove your answer.

**Theorem 3.9** (*) Let $p$ and $q$ be distinct primes. Then $\sqrt{pq}$ is irrational.

**Problem 3.10** State a generalization of Theorem 3.9 and briefly describe how its proof would go. Be as general as possible.

**Remark 3.11.** It is important to point out that not every positive irrational number is equal to the square root of some natural number. For example, $\pi$ is irrational, but is not equal to the square root of a natural number.

It is 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 3.7.
3.2 The infinitude of primes

The highlight of this section is Theorem 3.16, which states that there are infinitely many primes. In case you forgot, here is the definition of a prime number.

**Definition 3.12.** A natural number $p$ is called **prime** iff $p$ is divisible by exactly two distinct natural numbers (namely, 1 and $p$ itself).

**Exercise 3.13** Is 1 a prime number? Explain your answer.

The first known proof of Theorem 3.16 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 3.16, we need to prove a couple lemmas. The proof of the first lemma is provided for you.

**Lemma 3.14.** 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 3.15** Let $p$ be a prime number and let $n \in \mathbb{Z}$. If $p$ divides $n$, then $p$ does not divide $n + 1$.

Now, we are ready to prove the following important theorem.

**Theorem 3.16** There are infinitely many prime numbers.
Chapter 4

Relations and Functions

4.1 Relations

Definition 4.1. An ordered pair is an object of the form \((x,y)\). Two ordered pairs \((x,y)\) and \((a,b)\) are equal if \(x = a\) and \(y = b\).

Definition 4.2. An \(n\)-tuple is an object of the form \((x_1,x_2,\ldots,x_n)\). Each \(x_i\) is referred to as the \(i\)th component.

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

Definition 4.3. If \(X\) and \(Y\) are sets, the Cartesian product of \(X\) and \(Y\) is defined by

\[ X \times Y = \{(x,y) : x \in X, y \in Y\}. \]

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

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

Example 4.4. Let \(A = \{a,b,c\}\) and \(B = \{\emptyset, \emptyset\}\). Then

\[ A \times B = \{(a, \emptyset), (a, \emptyset), (b, \emptyset), (b, \emptyset), (c, \emptyset), (c, \emptyset)\}. \]

Exercise 4.5 Using the sets \(A\) and \(B\) from the previous example, find \(B \times A\).

Exercise 4.6 Using the set \(B\) from the previous examples, find \(B \times B\).

Exercise 4.7 What general conclusion can you make about \(X \times Y\) versus \(Y \times X\)? When will they be equal?

Exercise 4.8 If \(X\) and \(Y\) are both finite sets, then how many elements will \(X \times Y\) have? Be as specific as possible.

Exercise 4.9 Let \(A = \{1,2,3\}\), \(B = \{1,2\}\), and \(C = \{1,3\}\). List the elements of the set \(A \times B \times C\).
Exercise 4.10 Let $A = \mathbb{N}$ and $B = \mathbb{R}$. Describe the elements of the set $A \times B$.

Exercise 4.11 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 4.12 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 4.13 Let $X = [0, 1]$ and let $Y = \{1\}$. Describe geometrically what $X \times Y$, $Y \times X$, $X \times X$, and $Y \times Y$ look like.

Definition 4.14. 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 4.15. 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 since $3 \leq \pi$. However, $(1, -1)$ is not in the relation since $1 \not\leq -1$. (Order matters!)

Remark 4.16. 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 4.17. Let $P_f$ denote the set of all people with accounts on Facebook. Define $F$ via $x F y$ iff $x$ is friends with $y$. Then $F$ is a relation on $P_f$.

Remark 4.18. 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 $y$ iff $x \sim y$.

Example 4.19. Figure 4.1 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 4.20 Let $A = \{a, b, c\}$ and define $\sim = \{(a, a), (a, b), (b, c), (c, b), (c, a)\}$. Draw the digraph for $\sim$.

Exercise 4.21 Let $A = \{1, 2, 3, 4, 5, 6\}$. Define $|$ on $A$ via $x | y$ iff $x$ 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 4.22. 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:

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

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

Exercise 4.23 Define $\sim$ on $\mathbb{R}$ via $x \sim y$ iff $x \leq y$. Draw a picture of this relation in $\mathbb{R}^2$ (in other words, draw all points $(x, y)$ where $x \sim y$).
Definition 4.24. Let \( \sim \) be a relation on a set \( A \).

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

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

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

Example 4.25.

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

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

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

Exercise 4.26 Given a finite set \( A \) and a relation \( \sim \), describe what each of reflexive, symmetric, and transitive look like in terms of a digraph.

Exercise 4.27 Let \( P \) be the set of people at a party and define \( N \) via \( (x, y) \in N \) iff \( x \) knows the name of \( y \). Describe what it would mean for \( N \) to be reflexive, symmetric, and transitive.

Exercise 4.28 Determine whether each of the following relations is reflexive, symmetric, or transitive.

1. Let \( P_f \) denote the set of all people with accounts on Facebook. Define \( F \) via \( xFy \) iff \( x \) is friends with \( y \).

2. Let \( P \) be the set of all people and define \( H \) via \( xHy \) iff \( x \) and \( y \) have the same height.

3. Let \( P \) be the set of all people and define \( T \) via \( xTy \) iff \( x \) is taller than \( y \).

4. Consider the relation “divides” on \( \mathbb{N} \).
5. Let $L$ be the set of lines and define $|| l_1 ||_{l_2}$ iff $l_1$ is parallel to $l_2$.

6. Let $C[0,1]$ be the set of continuous functions on $[0,1]$. Define $f \sim g$ iff
   \[ \int_0^1 |f(x)| \, dx = \int_0^1 |g(x)| \, dx. \]

7. Define $\sim$ on $\mathbb{N}$ via $n \sim m$ iff $n + m$ is even.

8. Define $D$ on $\mathbb{R}$ via $(x, y) \in D$ iff $x = 2y$. 
4.2 Equivalence Relations

Remark 4.29. So that we have them handy, let’s recall the following definitions. Let ∼ be a relation on a set $A$. Then

1. ∼ is reflexive if for all $x \in A$, $x \sim x$ (every element is related to itself).
2. ∼ is symmetric if for all $x, y \in A$, if $x \sim y$, then $y \sim x$.
3. ∼ 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 mutually exclusive. 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 4.30. Let ∼ be a relation on a set $A$. Then ∼ is called an equivalence relation if ∼ is reflexive, symmetric, and transitive.

Exercise 4.31 Given a finite set $A$ and a relation ∼ on $A$, describe what the corresponding digraph would have to look like in order for ∼ to be an equivalence relation.

Exercise 4.32 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 4.33 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.

Problem 4.34 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.

1. Let $P_f$ denote the set of all people with accounts on Facebook. Define $F$ via $xFy$ iff $x$ is friends with $y$.
2. Let $P$ be the set of all people and define $H$ via $xHy$ iff $x$ and $y$ have the same height.
3. Let $P$ be the set of all people and define $T$ via $xTy$ iff $x$ is taller than $y$.
4. Consider the relation “divides” on $\mathbb{N}$.
5. Let $L$ be the set of lines and define $l_1 \parallel l_2$ iff $l_1$ is parallel to $l_2$.
6. Let $C[0,1]$ be the set of continuous functions on $[0,1]$. Define $f \sim g$ iff

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

7. Define ∼ on $\mathbb{N}$ via $n \sim m$ iff $n + m$ is even.
8. Define $D$ on $\mathbb{R}$ via $(x, y) \in D$ iff $x = 2y$.
9. Define ∼ on $\mathbb{Z}$ via $a \sim b$ iff $a - b$ is a multiple of 5.
10. Define $\sim$ on $\mathbb{R}^2$ via $(x_1, y_1) \sim (x_2, y_2)$ iff $x_1^2 + y_1^2 = x_2^2 + y_2^2$.

11. Define $\sim$ on $\mathbb{R}$ via $x \sim y$ iff $[x] = [y]$, where $[x]$ is the greatest integer less than or equal to $x$ (e.g., $[\pi] = 3$, $[-1.5] = -2$, and $[4] = 4$).

12. Define $\sim$ on $\mathbb{R}$ via $x \sim y$ iff $|x - y| < 1$.

**Definition 4.35.** 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 $x$ via

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

Also, define

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

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 $\mathcal{P}(A)$). Other common notations for $[x]$ include $\overline{x}$ and $R_x$.

**Exercise 4.36** Let $P_f$ and $F$ be as in part 1 of Exercise 4.34. Describe $[\text{Bob}]$ (assume you know which Bob we’re talking about). What is $\Omega_F$?

**Exercise 4.37** Using your digraph in Exercise 4.32, find $\Omega_{\sim}$ for all $x \in A$.

**Exercise 4.38** Consider the relation $\leq$ on $\mathbb{R}$. If $x \in \mathbb{R}$, what is $[x]$?

**Exercise 4.39** Find $[1]$ and $[2]$ for the relation given in part 9 of Exercise 4.34. How many different sets of relatives are there? What are they?

**Exercise 4.40** Find $[x]$ for all $x \in S$ for $S$ and $\sim$ from Exercise 4.33. Any observations?

**Theorem 4.41** (*) Suppose $\sim$ is an equivalence relation on a set $A$ and let $a, b \in A$. Then $[a] = [b]$ iff $a \sim b$.

**Theorem 4.42** (*) Suppose $\sim$ is an equivalence relation on a set $A$. Then

1. $\bigcup_{x \in A} [x] = A$, and
2. for all $x, y \in A$, either $[x] = [y]$ or $[x] \cap [y] = \emptyset$.

**Definition 4.43.** In light of Theorem 4.42, if $\sim$ is an equivalence relation on a set $A$, then we refer to each $[x]$ as the equivalence class of $x$. In this case, $\Omega_{\sim}$ is the set of equivalence classes determined by $\sim$.

**Remark 4.44.** The upshot of Theorem 4.42 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 4.45.** The set of relatives that you found in part 9 of Exercise 4.34 is the set of equivalence classes modulo 5.

**Exercise 4.46** 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 4.47** For each of the equivalence relations in Exercise 4.34, describe the equivalence classes as best as you can.
4.3 Partitions

Remark 4.48. The upshot of Theorems 4.41 and 4.42 is that if ∼ is an equivalence relation on a set $A$, then ∼ 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 ∼.

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

Definition 4.49. A collection $\Omega$ of nonempty subsets of a set $A$ is said to be a partition of $A$ if the elements of $\Omega$ satisfy:

1. Given $X, Y \in \Omega$, either $X = Y$ or $X \cap Y = \emptyset$ (We can’t have both at the same time. Do you see why?), and
2. $\bigcup_{X \in \Omega} X = A$.

That is, the elements of $\Omega$ are pairwise disjoint and their union is all of $A$.

Example 4.50. 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.

1. men, women (set of people)
2. Democrat, Republican, Independent, Green Party, Libertarian, etc. (set of registered voters)
3. freshman, sophomore, junior, senior (set of high school students)
4. evens, odds (set of integers)
5. rationals, irrationals (set of real numbers)

Example 4.51. Let $A = \{a, b, c, d, e, f\}$ and $\Omega = \{X_1, X_2, X_3\}$, where $X_1 = \{a\}$, $X_2 = \{b, c, d\}$, and $X_3 = \{e, f\}$. Then $\Omega$ is a partition of $A$ since the elements of $\Omega$ are pairwise disjoint and their union is all of $A$.

Exercise 4.52 Consider the set $A$ from Example 4.51.

1. Find a partition of $A$ that has 4 subsets in the partition.
2. Find a collection of subsets of $A$ that does not form a partition.

Exercise 4.53 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 4.54 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 4.55 (*) Let ∼ be an equivalence relation on a set $A$. Then $\Omega_{\sim}$ forms a partition of $A$. 
**Exercise 4.56** 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 \( \sim \).

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 4.57.** Let \( A \) be a set and \( \Omega \) any collection of subsets from \( P(A) \) (not necessarily a partition). If \( a, b \in A \), we will define \( a \) to be \( \Omega \)-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 \( \Omega \).

**Remark 4.58.** 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.

**Remark 4.59.** Notice that we have two notations that looks similar: \( \Omega_\sim \) and \( \sim_\Omega \).

1. \( \Omega_\sim \) is the collection of subsets of \( A \) determined by the relation \( \sim \).
2. \( \sim_\Omega \) is the relation determined by the collection of subsets \( \Omega \).

**Exercise 4.60** 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 4.61** Let \( A \) and \( \Omega \) be as in Example 4.51. List the elements of \( \sim_\Omega \) by listing ordered pairs or drawing a digraph.

**Theorem 4.62** \((*)\) Let \( A \) be a set and let \( \Omega \) be a collection of subsets from \( P(A) \) (not necessarily a partition). Then \( \sim_\Omega \) is symmetric.

**Exercise 4.63** Give an example of a set \( A \) and a collection \( \Omega \) from \( P(A) \) such that the relation \( \sim_\Omega \) is not reflexive.

**Theorem 4.64** \((*)\) Let \( A \) be a set and let \( \Omega \) be a collection of subsets from \( P(A) \). If \( \bigcup_{R \in \Omega} R = A \), then \( \sim_\Omega \) is reflexive.

**Theorem 4.65** \((*)\) Let \( A \) be a set and let \( \Omega \) be a collection of subsets from \( P(A) \). If the elements of \( \Omega \) are pairwise disjoint, then \( \sim_\Omega \) is transitive.

**Corollary 4.66** \((*)\) Let \( A \) be a set and let \( \Omega \) be a partition of \( A \). Then \( \sim_\Omega \) is an equivalence relation.

**Remark 4.67.** The previous corollary says that every partition determines a natural equivalence relation. Namely, two elements are related if they are in the same equivalence class.

**Exercise 4.68** Let \( A = \{\circ, \triangle, \bigtriangleup, \square, \blacksquare, \star, \odot, \oslash\} \). Make up a partition \( \Omega \) on \( A \) and then draw the digraph corresponding to \( \sim_\Omega \).
4.4 Introduction to Functions

The concept of function is one of the most important and fundamental ones in the field of mathematics. Functions are used in all branches of mathematics to model diverse situations and pull together ideas that at first seem unrelated. Functions are as vital as numbers.

Undoubtedly, 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 to each element of $X$ to exactly one element of $Y$. Let’s take a look at the actual definition.

**Definition 4.69.** 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:

1. For each $x \in X$, there exists $y \in Y$ such that $(x, y) \in f$, and
2. 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 $y$.”

**Remark 4.70.** Item 1 of Definition 4.69 says that every element of $X$ appears in the first coordinate of an ordered pair in the relation. Item 2 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 $B$ appears in the second coordinate, it may appear again in a different ordered pair.

**Definition 4.71.** The set $X$ from Definition 4.69 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

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

is called the range of $f$ or the image of $X$ under $f$.

**Remark 4.72.** It follows immediately from the definition that $\text{Rng}(f) \subseteq \text{Codom}(f)$. However, it is possible that the range of $f$ is strictly smaller.

**Remark 4.73.** 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 $f$.

**Exercise 4.74** Let $X = \{\diamond, \Box, \triangle, \bigodot\}$ 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.

1. $f : X \to Y$ defined via $f = \{(\diamond, a), (\Box, b), (\triangle, c), (\bigodot, d)\}$.
2. $g : X \to Y$ defined via $g = \{(\diamond, a), (\Box, b), (\triangle, c), (\bigodot, c)\}$.
3. $h : X \to Y$ defined via $h = \{(\diamond, a), (\Box, b), (\triangle, c), (\diamond, d)\}$.
4. $k : X \to Y$ defined via $k = \{(\diamond, a), (\Box, b), (\triangle, c), (\bigodot, d), (\Box, c)\}$.
5. \( l : X \to Y \) defined via \( l = \{(\circ, e), (\Box, e), (\triangle, e), (\odot, e)\} \).

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

7. \( \text{happy} : Y \to X \) defined via \( \text{happy}(y) = \odot \) for all \( y \in Y \).

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

9. \( \text{nugget} : X \to X \) defined via

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

**Definition 4.75.** 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. Now, draw an arrow from \( x \in X \) to \( y \in Y \) if \( f(x) = y \) (i.e., \( (x, y) \in f \)). In fact, we can draw bubble diagrams even if \( f \) isn’t a function.

**Exercise 4.76** For each of the relations in Exercise 4.74 draw the corresponding bubble diagram.

**Problem 4.77** What properties does a bubble diagram have to have in order to represent a function?

**Exercise 4.78** 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).

1. A function \( f \) from a set with 4 elements to a set with 3 elements such that \( \text{Rng}(f) = \text{Codom}(f) \).

2. 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 4.79** Let \( f : X \to Y \) be a function and suppose that \( X \) and \( Y \) have \( n \) and \( m \) elements in them, respectively. Also, suppose that \( n < m \). Is it possible for \( \text{Rng}(f) = \text{Codom}(f) \)? Explain.

**Problem 4.80** 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 4.81.** Two functions are equal if they have the same domain, same codomain, and the same set of ordered pairs in the relation.

**Remark 4.82.** 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 \( g(x) = x^2 \).

**Theorem 4.83** If \( f : X \to Y \) and \( g : X \to Y \) are functions, then \( f = g \) iff \( f(x) = g(x) \) for all \( x \in X \).

**Definition 4.84.** Let \( f : X \to Y \) be a function.

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

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

**Exercise 4.85** 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.

1. A function $f : X \to Y$ that is one-to-one but not onto.
2. A function $f : X \to Y$ that is onto but not one-to-one.
3. A function $f : X \to Y$ that is both one-to-one and onto.
4. A function $f : X \to Y$ that is neither one-to-one nor onto.

**Problem 4.86** 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? Explain.

**Exercise 4.87** 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.

1. A function $f : \mathbb{R} \to \mathbb{R}$ that is one-to-one but not onto.
2. A function $f : \mathbb{R} \to \mathbb{R}$ that is onto but not one-to-one.
3. A function $f : \mathbb{R} \to \mathbb{R}$ that is both one-to-one and onto.
4. A function $f : \mathbb{R} \to \mathbb{R}$ that is neither one-to-one nor onto.

**Theorem 4.88** (*) Let $f : X \to Y$ be a function. Then $f$ is one-to-one iff for all $x_1, x_2 \in X$, if $f(x_1) = f(x_2)$, then $x_1 = x_2$.

**Remark 4.89.** The previous theorem gives a technique for proving that a given function is one-to-one. Start by assuming that $f(x_1) = f(x_2)$ and then work to show that $x_1 = x_2$.

**Remark 4.90.** To show that a given function is onto, you should start with an arbitrary $y \in \text{Rng}(f)$ and then work to show that there exists $x \in X$ such that $y = f(x)$.

**Exercise 4.91** 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.

1. $f : \mathbb{R} \to \mathbb{R}$ defined via $f(x) = x^2$
2. $g : \mathbb{R} \to [0, \infty)$ defined via $g(x) = x^2$
3. $h : \mathbb{R} \to \mathbb{R}$ defined via $h(x) = x^3$
4. $k : \mathbb{R} \to \mathbb{R}$ defined via $k(x) = x^3 - x$
5. $l : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ defined via $l(x_1, x_2) = x_1^2 + x_2^2$
6. $N : \mathbb{N} \to \mathbb{N} \times \mathbb{N}$ defined via $N(n) = (n, n)$
Exercise 4.92  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 $\pi_1$ (respectively, $\pi_2$) the \textbf{projections} of $S$ onto $A$ (respectively, $B$).

1. Provide examples to show that $\pi_1$ does not need to be one-to-one or onto.

2. Suppose that $S$ is a function (recall that a function is a set of ordered pairs, so this makes sense). Is $\pi_1$ one-to-one? Is $\pi_1$ onto? How about $\pi_2$?
4.5 Compositions and Inverses

Definition 4.93. 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 \( x \in \text{Dom}(f)\).

Remark 4.94. It is important to notice that the function on the right is the one that “goes first.”

Exercise 4.95 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.

1. \( f \) is onto, but \( g \circ f \) is not onto.
2. \( g \) is onto, but \( g \circ f \) is not onto.
3. \( f \) is one-to-one, but \( g \circ f \) is not one-to-one.
4. \( g \) is one-to-one, but \( g \circ f \) is not.

Theorem 4.96 (*) If \( f : X \to Y \) and \( g : Y \to Z \) are both functions that are onto, then \( g \circ f \) is also onto.

Theorem 4.97 (*) 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 4.98 If \( f : X \to Y \) and \( g : Y \to Z \) are both one-to-one correspondences, then \( g \circ f \) is also a one-to-one correspondence.

Problem 4.99 Assume that \( f : X \to Y \) and \( g : Y \to Z \) are both functions. For each of the following statements, if the statement is true, then prove it. If the statement is false, provide a counterexample.

1. If \( g \circ f \) is one-to-one, then \( f \) is one-to-one.
2. If \( g \circ f \) is one-to-one, then \( g \) is one-to-one.
3. If \( g \circ f \) is onto, then \( f \) is onto.
4. If \( g \circ f \) is onto, then \( g \) is onto.

Definition 4.100. Let \( f : X \to Y \) be a function. The relation \( f^{-1} \), called \( f \) inverse, is defined via

\[
\text{f}^{-1} = \{(f(x), x) : x \in X\}.
\]

Remark 4.101. Notice that we called \( f^{-1} \) a relation and not a function. In some circumstances \( f^{-1} \) will be a function and sometimes it won’t be.

Exercise 4.102 Provide an example of a function \( f : X \to Y \) such that \( f^{-1} \) is not a function. A bubble diagram is sufficient.

Exercise 4.103 Provide an example of a function \( f : X \to Y \) such that \( f^{-1} \) is a function. A bubble diagram is sufficient.

Theorem 4.104 (*) Let \( f : X \to Y \) be a function. Then \( f^{-1} \) is a function iff \( f \) is ____________.

Theorem 4.105 (*) Let \( f : X \to Y \) be a function and suppose that \( f^{-1} \) is a function. Then
1. \((f \circ f^{-1})(x) = x\) for all \(x \in Y\), and
2. \((f^{-1} \circ f)(x) = x\) for all \(x \in X\).

(You only need to prove one of these statements; the other is similar.)

**Theorem 4.106** (*) Let \(f : X \to Y\) and \(g : Y \to X\) be functions such that \(f\) is a one-to-one correspondence. If \((f \circ g)(x) = x\) for all \(x \in Y\) and \((g \circ f)(x) = x\) for all \(x \in X\), then \(g = f^{-1}\).

**Remark 4.107.** 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 “undoing” property exhibited in Theorem 4.105.

The next theorem can be considered to be a converse of Theorem 4.106.

**Theorem 4.108** (*) Let \(f : X \to Y\) and \(g : Y \to X\) be functions satisfying \((f \circ g)(x) = x\) for all \(x \in Y\) and \((g \circ f)(x) = x\) for all \(x \in X\). Then \(f\) is a one-to-one correspondence.

**Theorem 4.109** (*) Let \(f : X \to Y\) and \(g : Y \to Z\) be functions. If \(f\) and \(g\) are both one-to-one correspondences, then \((g \circ f)^{-1} = f^{-1} \circ g^{-1}\).