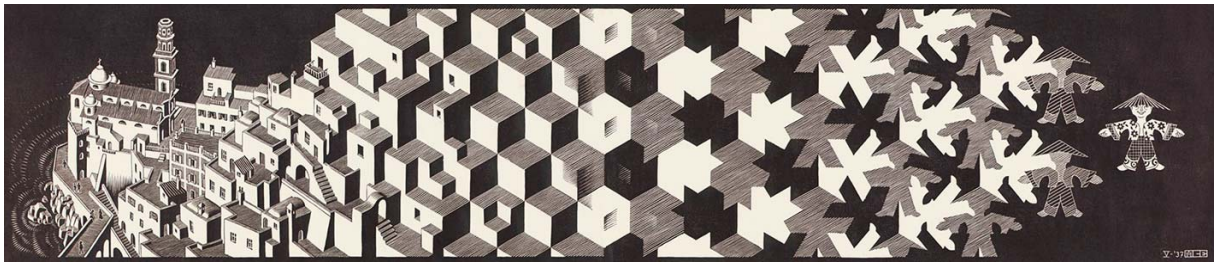


Transition to Advanced Mathematics

Math 215 Lecture notes

Subhadip Chowdhury, PhD

The College of Wooster

Fall 2021

$*110{\cdot}643.\ \vdash .\ 1 +_c 1 = 2$

Dem.

$$\vdash .\ *110{\cdot}632 .\ *101{\cdot}21{\cdot}28 .\ \supset$$

$$\vdash .\ 1 +_c 1 = \hat{\xi}\{(\exists y) .\ y \in \xi .\ \xi - \iota`y \in 1\}$$

$$[*54{\cdot}3] \quad = 2 .\ \supset \vdash .\ \text{Prop}$$

The above proposition is occasionally useful. It is used at least three times, in $*113{\cdot}66$ and $*120{\cdot}123{\cdot}472$.

--- Whitehead & Russell (1912). **Principia Mathematica**. Volume II, 1st edition, p. 86

Contents

Acknowledgement

A significant portion of the content in these lecture note has been directly copied or adapted from notes by Dana Earnst[i], Jen Bowen, Robert Kelvey, and Colby Long. My sincerest thanks to all of them. Other references are cited in the context. More info about the banner image can be found here.

[i] Dana C. Ernst. **An Introduction to Proof via Inquiry-Based Learning**. URL: https://github.com/dcernst/IBL-IntroToProof.

Introduction

§0.1 What is Transitions to Advanced Mathematics?

First and foremost, Transitions to Advanced Mathematics is a course designed to develop and improve your mathematical writing, speaking, and thinking skills. We aim to do this by actively practicing the art of doing mathematics. One key element in doing mathematics is that of **proof**. Hence, a large part of this course involves us discussing various methods of proof. But before we can discuss methods of proof, we must understand the underlying logic that supports all of mathematics. Closely connected to logic is the theory of sets, from which almost all of mathematics can be shown to arise from. Mathematicians often refer to logic and set theory as the **foundations** of mathematics.

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

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

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

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

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

§0.2 Inquiry-Based Learning

You have likely taken a math course that is taught via the "traditional" lecture style. Typically, this means you show up to class, sit and listen to the instructor profess facts, theorems, proofs and examples, all

while trying to write everything down. Hopefully, you have experienced some very good lecturers (I greatly apologize if you have not!). But have you ever thought to yourself after a lecture class period when studying, ''I thought I understood this when the professor was doing it, but now on my own, I don't get it.'' Indeed, there is now decades of education research that definitively shows that lecturing is not the best way for students to learn!

It is my philosophical belief that taking a more active style approach in the mathematics classroom is the best way for students to learn mathematics. Hence, in our class, we will incorporate ideas from an educational philosophy called **inquiry-based learning** or IBL[ii] for short. Loosely speaking, IBL is a student-centered method of teaching mathematics that engages students in sense-making activities. Students are given tasks requiring them to solve problems, conjecture, experiment, explore, create, and communicate. Rather than showing facts or a clear, smooth path to a solution, the instructor guides and mentors students via well-crafted problems through an adventure in mathematical discovery.

Perhaps this is sufficiently vague, but I believe that there are two essential elements to IBL. Students should as much as possible be responsible for:

(a) Guiding the acquisition of knowledge, and

(b) Validating the ideas presented. That is, students should not be looking to the instructor as the sole authority.

This last point is important. I would hope that all of you, regardless of major or courses taken at the College of Wooster, will leave here with the skill of independent validation; to be able to *think*, *analyze*, *and reach logical conclusions on your own*, and communicate those conclusions in a clear, persuasive manner. I hope that this course gives you a safe environment to try, to fail, and to succeed in bettering yourself in this way.

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

Many of the concepts you learn and problems you work on will be new to you and ask you to stretch your thinking. You will experience **frustration** and **failure** before you experience **understanding**. This is part of the normal learning process. *If you are doing things well, you should be confused at different points in the semester.* The material is too rich for a human being to completely understand it immediately. Your viability as a professional in the modern workforce depends on your ability to embrace this learning process and make it work for you.

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

In this course, everyone will be required to

- read and interact with course notes and textbook on your own;
- write up quality solutions/proofs to assigned problems;
- present solutions/proofs on the board to the rest of the class;
- participate in discussions centered around a student's presented solution/proof;

[ii] You can find more info about IBL here, and here.

- 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.

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.

§0.3 Structure of Lecture Note

These notes vaguely follow the textbooks mentioned in the syllabus, albeit in a different order. It is recommended to read the corresponding section of the textbooks alongside reading these notes for additional text, examples, and - the heart of it all - questions for you to complete for class.

The questions on course handouts sometimes mirror examples from the textbook, hence will help gauge your understanding after reading. Questions may also mimic the exercises found in your textbook, but don't let that stop you from examining those problems, too. Indeed, most of the odd-numbered problems in your book have solutions in the back (even the proofs!). Please use this as much as you need to in aiding your understanding. Some handouts may contain explicit recommendations on textbook exercises to examine for further practice.

The items labeled as **Definition** and **Example** are meant to be read and digested. However, the items labeled as **Question** require action on your part. Some questions are computational in nature and aimed at solidifying your understanding of a particular concept. Other questions ask you to to make conjectures, produce counterexamples, and prove theorems. There are many situations where you will want to refer to an earlier definition or theorem/corollary/question. In this case, you should reference the statement by number. For example, you might write something like, ''By Theorem 2.14, we see that. . . ."

§0.4 How to Complete the Questions

A significant portion of of your daily/weekly work will be completing **Questions** from this lecture note. You should devote much time and energy to thinking about these questions. Write out scratch work on separate paper. Once you believe you have a solution, you should write out a clean, neat, organized solution. If scratch work is all you have, find the time to write down a summary of what you tried when working on the question. Perhaps you know how to start the question and you know what the conclusion should be, but the middle of the problem escapes you. Write this down! What question developed as you worked on the problem? Write those down, too! When discussing problems in class or watching presentations, you will be able to pose these question to your peers and build your understanding. You can also come see me (or the TA) in office hours to discuss any problems like this.

§0.5 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. 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 your peers.

- 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. Periodically during the semester, I will ask you to submit some of these reflections. 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 . . .

§0.6 Rules of the Game

Reviewing material from previous courses and looking up definitions and theorems you may have forgotten is fair game. However, when it comes to completing assignments for this course, you should **not** look to resources outside the context of this course for help. That is, you should not be consulting the web, other texts, other faculty, or students outside of our course in an attempt to find solutions to the problems you are assigned. On the other hand, you may use each other, this lecture note, the two textbooks mentioned in the syllabus, me, and your own intuition. In this class, earnest failure outweighs counterfeit success; you need not feel pressure to hunt for solutions outside your own creative and intellectual reserves. If you feel you need additional resources, please come talk to me and we will come up with an appropriate plan of action.

§0.7 Tentative Schedule

I have included a preliminary outline of the topics that we hope to cover in this course. This is an idealized plan, and it *may be adjusted as the semester progresses.*

Week of	Topics	Assignments (Due date)
Aug 25-27	Introduction to Math 215 and IBL Statements, Naive Set Theory	**Mon, Aug 23**: No Class **Wed, Aug 25**: No homework. **Fri, Aug 27**: Submit Reflection Task 1.

Aug 30 - Sep 3	And, Or, Not Conditionals and Biconditionals Intro to LaTeX	**Mon, Aug 30**: Read Appendix A. **Fri, Sep 3**: HW 1
Sep 6-10	Tautology, Contradiction, Logical Equivalence Quantifiers, Hidden Translation	**Mon, Sep 6**: Submit Reflection Task 2. **Fri, Sep 10**: HW 2
Sep 13-17	Negation Annoying Sets Divisibility	 **Wed, Sep 15**: Read Appendix B. **Fri, Sep 17**: HW 3 and Reflection Task 3.
Sep 20-24	Direct Proof Counterexamples Cases	 **Wed, Sep 22**: Submit Reflection Task 4 and 5 (optional) and Read Appendix C. **Fri, Sep 24**: HW 4 (Reading/Evaluating Proofs)
Sep 27 - Oct 1	Contrapositive Congruence Contradiction	**Mon, Sep 27**: **Wed, Sep 29**: P^3 1 first draft **Fri, Oct 1**: HW 5
Oct 4-8	Contradiction contd. Biconditional, Equivalent Review	 **Wed, Oct 6**: P^3 2 first draft **Fri, Oct 8**: HW 6, Quiz 1 (Logic and Proof Structures)
Oct 11-15	Fall Break	
Oct 18-22	Existence Uniqueness Proof By Induction	**Mon, Oct 18**: EP topic choice **Wed, Oct 20**:P^3 3 first draft **Fri, Oct 22**: EP topic choice final deadline
Oct 25-29	More Induction Strong Induction Cartesian Product	**Mon, Oct 25**: HW 7 **Fri, Oct 29**: EP summary and discussion
Nov 1-5	Subsets, Power sets Set operations and Venn Diagram Set proofs ($A \subseteq B$)	**Mon, Nov 1**: HW 8, P^3 1,2,3 final draft **Wed, Nov 3**: P^3 4 first draft. **Fri, Nov 5**: EP outline and annotated bibliography
Nov 8-12	Set proofs ($A = B$) Set proofs Indexed Sets	**Mon, Nov 8**: HW 9 **Wed, Nov 3**: P^3 5 first draft. **Fri, Nov 12**: Quiz 2 (E&U, Induction, Set Theory)
Nov 15-19	Relation and their Properties Equivalence Class and Partition Function Functions - Domain, Range, Composition	 **Fri, Nov 19**: HW 10
Nov 22	Bijections	**Mon, Nov 22**: **Wed, Nov 17**: P^3 6 first draft.

	No class	**Wed, Nov 24**: EP full first draft **Fri, Nov 26**: Thanksgiving
Nov 29 - Dec 3	Presentations Inverse Functions and Presentations Equinumerosity and Presentations	 **Fri, Dec 3**: HW 11
Dec 6-10	Equinumerosity contd. Countable and uncountable Sets Review	**Mon, Dec 6**: P^3 4,5,6 final draft **Wed, Dec 8**: EP Peer Reviews **Fri, Dec 10**: HW 12
Dec 15	Cumulative Quiz	

§0.8 Tips for Starting Out

We will begin writing proofs in earnest once we reach Chapter 2 in these lecture notes. As we start out, 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 start exploring mathematics!

Chapter 1 | Logic

§1.1 Statements

- Math is concerned with the formation of a **theory**: *a collection of true statements*, that describe patterns or relationships.
- This process is characterized by **deductive reasoning**: *the process of using logic to develop and extend a theory by drawing conclusions based on statements accepted as true.* In math, we start with obvious statements (axioms) or previously proven true statements.
- This is in contrast to **inductive reasoning**: *forming a theory by collecting information and making observations about particular cases of patterns or relationships among quantities and structures.*
- Mathematicians give **proofs** to demonstrate that our conclusions are true.

Definition 1.1.1

A (mathematical) **statement** (or **proposition**) is a declarative sentence or expression that is either true (T) or false (F), but not both.

The key here is that there must be no ambiguity, whether a **statement** is true or not should not be a matter of personal opinion. Additionally it must be a grammatically correct sentence with a subject and a verb.

Question 1. □

Determine whether the given sentence is a statement or not. If it is a statement, decide if it is true or false (if possible).

(a) *Today is Friday.*

(b) *Is today Friday?*

(c) *Marie Curie won one Nobel Prize.*

(d) $3+1=5$.

(e) 7.

(f) $\sqrt{2} \in \mathbb{Q}$.

(g) *Wow!*

(h) *Every function is continuous.*

(i) $x^2-7x+10=0$.

(j) *The equation* $x^2-7x+10=0$ *has a real solution.*

(k) *Solve the equation* $x^2-7x+10=0$.

We often use uppercase letters to denote statements. For example,

P: *Every differentiable function is continuous.*

This way we can simply refer to the statement as P without writing the sentence out every time. For example, we can simply say **"P is true"**.

Definition 1.1.2

A sentence whose truth depends upon the value of one or more variables is called an **open sentence** (or a **predicate**).

Question 2.

Consider the open sentence "the integer x is a multiple of 7," which we denote by $\mathrm{M}(x)$*. This sentence is open since its truth depends on x.*

(a) Is $\mathrm{M}(15)$ *true?*

(b) Is $\mathrm{M}(21)$ *true?*

Note: Open sentences can also rely on more than one variable, e.g.

$$\mathrm{R}(x,y) : x+y \text{ is even.}$$

Then $\mathrm{R}(3,5)$ is true, but $\mathrm{R}(5,6)$ is false.

Question 3.

Determine if the given sentence or expression is a ***statement*** *or an* ***open sentence*** *or* ***neither****. If a statement, decide if it is true or false (if possible). If it's an open sentence, give one example for which it is true and one examples for which it is false.*

(a) The integer 5 *is even.*

(b) $x^2 = 4$.

(c) x is a real number and $x^2 = -1$.

(d) Chocolate ice cream is the best.

(e) If n is an even integer, then n^2 is even.

(f) $x^2 + 1 = 5$.

(g) $x + y - 3 = 9$.

(h) The function $f(x) = \sin x$ *is an even function.*

(i) For all integers x, y, z and for all natural numbers $n > 2$, $x^n + y^n \neq z^n$.

(j) This sentnece has a typo.

1.1.1 How Do We Decide If a Statement Is True or False?

In mathematics, we often establish that a statement is true by writing a *mathematical proof*. To establish that a statement is false, we often find a so-called *counterexample*. We will explore the details later, but for now, here are some approaches on *how to get started*.

- **Guesswork and conjectures.** Make a guess beforehand as to whether the statement is true or false.
- **Construct appropriate examples.** Look at a bunch of examples to check whether your conjecture holds or not. If you happen to find an example that shows your conjecture to be false, we call it a counterexample.

Exploration Activity

Play this puzzle from The New York Times[a] to learn about cognitive bias, and why it is important in Math to first try to find possible *counterexamples*. If we can not find a counterexample for a conjecture, that doesn't necessarily mean that the conjecture is true. It might just be the case that we merely didn't look hard enough!

[a] If you run into a paywall, come talk me about how to get around it.

- **Use your prior knowledge.** We cannot start from square one every time we explore a statement. We must make use of our acquired mathematical knowledge. That means we might have to use our precalculus and calculus knowledge, or look it up if we do not remember them.
- **Cooperation and brainstorming.** Working together is often more fruitful than working alone. When we work with someone else, we can compare notes and articulate our ideas. Thinking out loud is often a useful brainstorming method that helps generate new ideas.

1.1.2 Different Types of Math Problems

Most Math problems fall largely in to three categories:

- 'Show that . . . ' or 'Evaluate . . . ' questions, in which a certain statement has to be proved true, or a certain expression has to be simplified using pre-established rules;
- 'Find a . . . ' or 'Find all . . . ' questions, which requires one to find something (or everything) that satisfies certain requirements (and prove that the object indeed satisfies the requirements or show that you have exhausted all possibilities);
- 'Is there a . . . ' questions, which either require you to prove a statement or provide a counterexample (and thus is one of the previous two types of problem).

In the next page there are three questions for you to start with! Don't worry too much about formatting and correctness right now, instead try to come up with ideas on how to write/communicate your argument with the most amount of clarity on paper. Skim over appendix C after you are done.

Question 4.

Prove that the sentence

"This sentence is false."

is not a Mathematical statement.

Question 5.

Find all four-digit number $\overline{abcd}$ *such that* $4 \cdot \overline{abcd} = \overline{dcba}$.

> **Hint:** There is only one such number. Make sure to justify why only one such number exists.

Question 6.

You have a chessboard (8×8) *plus a big box of dominoes (each* 2×1*). I use a marker pen to put an "X" in two squares at diagonally opposite corners. Is it possible to cover the remaining* 62 *squares using the dominoes without any of them sticking out over the edge of the board and without any of them overlapping?*

§1.2 Naïve Set Theory

Set theory gives us a foundation for almost all mathematical theories. Together with logic, sets form a common language for mathematical expression. *For now*, we will say that a **set** is just a collection of objects, called its **elements**.

Example 1.2.3

One example of a set could be the collection of all students in MATH 215 whose first name starts with 'A'. The students who belong to this set would be its elements.

Notation. We use curly braces { , } to denote sets, with elements listed inside the braces separated by commas.

Example 1.2.4

Here are three sets:

$$A = \{1, 2, 3, 4\} \qquad B = \{\{a, b\}, c, d\} \qquad C = \{\square, \triangle, \bigcirc\}$$

Note:

- In general, we use capital letters for sets and lowercase letters for elements of a set.
- A has 4 elements, B has 3 elements, and C has three elements.
- B is a set and one of its elements is also a set!

Sets are completely determined by their elements. This means that the order does not matter and two sets with the same elements are **equal**. Also,

- We do not allow duplicates in sets.
- We use the notation $\in$ for "is an element of" and $\notin$ for "is not an element of".

Example 1.2.5

For the sets in the last example, $1 \in A$. Likewise, $2 \in A$, $c \in B$, and $\square \in C$. However, $5 \notin A$ and $a \notin B$.

Question 7. □

Let $S = \{\{1\}, 2, \{3, \{4\}\}\}$.

(a) How many elements are in the set S*?*

(b) Is $1 \in S$*?*

(c) Is $2 \in S$*?*

(d) Is $\{4\}$ *in* S*?*

(e) Is it true that $S = \{2, \{1\}, \{\{4\}, 3\}\}$*?*

The number of elements in a set is called the **cardinality** of the set[i]. If this is a natural number, then the set is **finite**. If a set is not **finite** then it is **infinite**. We use the symbols $|\cdot|$ around a set to denote its size.

[i] for now!

Example 1.2.6

Consider the set $A = \{a, b, c, d, \ldots, y, z\}$, the set of all letters in the English alphabet. A is a finite set. The cardinality of A is 26, so we would write $|A| = 26$.

Warning: Sets are not always just letters and numbers.

Example 1.2.7

Consider the set of all current Wooster students on the swim team that are majoring in Mathematics and History (there may be not be any elements in this set).

Sometimes, it is not possible to list all of the elements of a set.

Example 1.2.8

Consider the set of all differentiable functions from $\mathbb{R}$ to $\mathbb{R}$. This is an infinite set which you have encountered before in Calculus.

Here are some other sets that you are probably already familiar with and the notation we use for them.

$\mathbb{N} = \{1, 2, 3, \ldots\}$ is the set of **natural numbers** or positive integers.
$\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$ is the set of **integers**.
$\mathbb{Q}$ is the the set of **rational numbers**.
$\mathbb{R}$ is the the set of **real numbers**.

Exploration Activity

Clearly $\mathbb{N}, \mathbb{Z}, \mathbb{Q}$, and $\mathbb{R}$ are infinite sets. However, the cardinality of these sets are not the same! The cardinality of $\mathbb{N}$ and $\mathbb{Z}$ is denoted as $\aleph_0$ (called the countable infinity), whereas the cardinality of $\mathbb{Q}$ and $\mathbb{R}$ is denoted as $\mathfrak{c}$ (called the continuum). We will come back to this discussion at the end of the semester.

§1.3 The Set Builder Notation

The most basic way of specifying the elements of a set is to list the elements of that set - called the **roster method**. For larger sets, it is sometimes inconvenient to list all of the elements of the set. In this case, we often list several of them and then write a series of three dots (...) to indicate that the pattern continues. For example,

$$D = \{1, 3, 5, 7, \ldots, 49\}$$

is the set of all odd natural numbers from 1 to 49, inclusive. However, we quickly run into obvious issues in describing infinite sets in the same way.

One convenient way to describe sets, (especially those with an infinite number of elements) is with **set-builder notation**. We write

$$\{x : P(x)\} \text{ or } \{x \mid P(x)\}$$

to describe a set whose typical element x has to satisfy a one-variable open sentence property described by $P(x)$. As a modified form, we also sometimes use the notation

$$T = \{x \in S : P(x)\}$$

to denote a set T made up of elements from a bigger set S that have the property $P(x)$.

Example 1.3.9

Here are two examples of sets you have seen before, using set-builder notation. These are intervals of real numbers, like in Calculus:

$$(0, 1) = \{x \in \mathbb{R} : 0 < x < 1\}$$

$$[4, 6) = \{x \in \mathbb{R} : 4 \leq x < 6\}.$$

We often read a set like this aloud by pronouncing the colon or the vertical line as *"such that*." For example, we could say the first set above as "the set of all real numbers x, such that x is greater than zero and less than one."

Question 8.

Write out the elements of each of the following sets using roster method.

(a) $\{x \in \mathbb{Z} : |x| < 4\} =$

(b) $\{x \in \mathbb{R} : x^2 - 2 = 0\} =$

Question 9.

It is sometimes possible to modify the set builder notation by putting the predicate first. For example, consider the set

$$\{2n + 1 : n \in \mathbb{Z}\}$$

We would read this aloud as "The set of all numbers ***of the form*** $2n + 1$*, where n is an integer" or equivalently "the set of all integers* ***of the form*** $2n + 1$*." Write down some elements of the set using the roster method. Can you figure out how to change it to the set builder notation? If you get stuck, don't worry, we will come back to it later.*

Question 10.

Write each of the following sets in set-builder notation (in either of the two possible methods we discussed above).

(a) $\{3,4,5,6,7,8\} =$

(b) *The set of all even integers* $=$

Question 11.

To make sure you understand the set builder notation, sketch the following sets of points in the xy-plane. You can think of each element (x,y) *as the coordinates of a point in the xy-plane.*

(a) $\{(x,y) : x \in (-1,1], y = 1\}$

(b) $\{(x,x^2) : x \in \mathbb{R}\}$

(c) $\{(x,x+y) : x \in \mathbb{R}, y \in \mathbb{Z}\}$.

(d) $\{(x,y) : x,y \in \mathbb{R}, x^2+y^2 = 1\}$

Definition 1.3.10

The set of rational numbers can be written in set builder notation as

$$\mathbb{Q} := \left\{ r \in \mathbb{R} \;\middle|\; r = \frac{p}{q} \text{ where } p, q \in \mathbb{Z} \text{ and } q \neq 0 \right\}.$$

Warning: Stop and make sure that you understand the definition of $\mathbb{Q}$ and will never forget it. Can you repeat it **verbatim** without looking at it? Call me over if you are having trouble parsing the notations. Skim appendix A at home before next class.

Note: An important point of note before we move on - observe that

$$\{x \in \mathbb{N} : 3 < x < 7\} = \{y \in \mathbb{N} : 3 < y < 7\} = \{z \in \mathbb{N} : 3 < z < 7\} = \{4, 5, 6\}$$

The point is, that the particular choice of variable x or y or z or p or φ has no significance at all. The set-builder notation of a set A does not create any particular link between the set A and the letter used to describe its elements, e.g. x.

Definition 1.3.11

The **empty set** or **null set**, denoted $\emptyset$, is the unique set with no elements.

Note that the symbol for null set is not zero, it's a letter from the Danish-Norwegian alphabet.

Example 1.3.12

Since $x^2 \geq 0$ for every $x \in \mathbb{R}$,

$$\{x \in \mathbb{R} : x^2 + 1 = 0\} = \emptyset.$$

Question 12.

What are the elements of the set $S = \{x \in \mathbb{Z} : x^2 - 2 = 0\}$*?*

□

Question 13.

Is the set $\{\emptyset\}$ *equal to* $\emptyset$*? Explain your reasoning for why or why not.*

□

§1.4 Logical Operators: And, Or, Not

The words **and**, **or**, and **not** can be used to combine statements to form new statements. These form the basics of what is called the **statement calculus** or **propositional logic**.

Question 14.

Consider the following statements. Which would you say are true and which are false?

*(a) Today is a weekday **and** the temperature outside is less than 40° F.*

*(b) Today is a weekday **and** all primes are odd.*

*(c) 4 is a prime number **or** 2 + 2 = 4.*

*(d) Today is Friday **or** today is Wednesday.*

Definition 1.4.13

Let P and Q be statements.

(a) The statement "P **and** Q" is true if and only if both P and Q are true. This is known as **conjunction**, and it is written symbolically as

$$P \wedge Q.$$

(b) The statement "P **or** Q" is true if and only if P is true, Q is true, or both P and Q are true. This is known as **disjunction**, and it is written symbolically as

$$P \vee Q.$$

We use **truth tables** to succinctly describe all the true/false possibilities of a statement.

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

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

Note: A statement has only the two possible truth values: true or false. Hence, if a compound statement P is built-up from n statements, then the truth table for P will have 2^n rows.

Warning: The meaning of 'or' in mathematics is slightly different than how it is usually used in English! For example, consider the statement:

Move your car or you will get a ticket.

We understand that this means that either you move your car or you will get a ticket, **but not both**. In mathematics, 'or' is always the **inclusive or**. For us, 'or' means **one or both** of P or Q is true.

If we ever needed to express the fact that exactly one of P or Q is true, we would use one of the following constructions:

P or Q, but not both
Either P or Q
Exactly one of P or Q.

Definition 1.4.14

The **negation** of a statement P, denoted $\sim$ P, is the statement 'not P'. The statement $\sim$ P is true exactly when P is false.

P	$\sim$ P
T	**F**
F	**T**

Question 15.

Let P *be the statement "*$f(x) = x^2 + 1$ *is continuous" and* Q *be the statement "m is a multiple of 3." Express the following as ordinary English sentences. Then state whether the statement is true or false. Part (a) has been done for you as an example.*

(a) $\sim$P

Solution. **Good answers:** "The function $f(x) = x^2+1$ is not continuous." or "The function $f(x) = x^2+1$ is discontinuous."

Bad answers: "It is not the case that $f(x) = x^2+1$ is continuous" or "$\sim(f(x) = x^2+1$ is continuous)". ■

(b) P $\wedge$ Q

(c) P $\vee$ Q

(d) $\sim$Q

Question 16.

For this question, you are trying to translate written sentences into mathematical statements. Because human language is more ambiguous than mathematics, this might be tricky!

Express each statement or open sentence in one of the forms P $\wedge$ Q, P $\vee$ Q, *or* $\sim$ P. *State exactly what the statements* P *and* Q *stand for. Part (a) has been done for you as an example.*

(a) I'm not going to class and you can't make me!

Solution. **Good answers:**

- P: "I'm going to class."
  Q: "You can make me go to class"
  Answer: $(\sim P) \wedge (\sim Q)$
- P: "I'm not going to class."
  Q: "You can't make me go to class"
  Answer: P $\wedge$ Q

Bad answers:

- P: ''going to class and you can't make me''

  Answer: $\sim$ P
- I'm $\sim$ going to class $\wedge$ you can't make me!

■

(b) *The number* 8 *is both even and a power of* 2.

(c) $x \neq y$.

(d) *There is a test scheduled for Wednesday or Friday.*

■ Question 17. □

For the statements

$$\text{P} : 15 \textit{ is odd.} \qquad \text{Q} : 15 < 17$$

write each of the following statements in symbolic form using the operators $\wedge, \vee$, *and* $\sim$.

(a) $15 \geq 17$.

(b) *15 is even or* $15 < 17$.

(c) *15 is odd or* $15 \geq 17$.

(d) *15 is odd and* $15 \geq 17$.

§1.5 Conditional Statements

Much of mathematics involves stating and proving theorems, and almost all mathematical theorems are (or can be) stated as a **conditional statement** (also referred to as **implication**) in the following form:

If "certain conditions are met," then "something happens."

Example 1.5.15

Consider the following statement. I say to you

"If you attend the next lecture, then I will give you a candy!"

Treat this as a contract or an agreement between us. There are four possible scenarios, depending on whether or not you attend the lecture, and whether or not I give you a candy. Describe each of these scenarios in English and decide the circumstance in which you can rightly claim a clear violation of the agreement (i.e. the statement is false)?

Scenario 1: You attend the next lecture and I give you a free candy. **(In this scenario, the contract is upheld, so the statement is true.)**

Scenario 2:

Scenario 3:

Scenario 4:

Definition 1.5.16

Let P and Q be two statements. The **conditional statement** $P \implies Q$, read as 'P implies Q', is the statement 'If P, then Q.'

'$P \implies Q$' has the same truth value as the compound statement 'not P or Q'.

Note: In a conditional statement $P \implies Q$, P is called the **hypothesis** (or **antecedent**) and Q is the **conclusion** (or **consequent** if you want to be fancy).

Question 18.

Use the definition of $P \implies Q$ *to complete the following truth table:*

P	Q	$P \implies Q$
T	*T*	
T	*F*	
F	*T*	
F	*F*	

The last two rows of the truth table for $P \implies Q$ are sometimes an initial shock. Hopefully above example clarifies our reasons for entering into this contract. Here's another **true** statement:

If London is in France, then the Eiffel Tower is in Bolivia.

Such statements are said to be **vacuously true**.

Question 19.

For each pair of statements, write out and determine the validity of the conditional statement $P \implies Q$.

(a) $P : 3 + 2 = 5$
$Q : 3 + 1 + 1 = 5$.

(b) P : *Unicorns exists.*
$Q : 7 < 2$.

(c) P : *You are the President of the United States.*
$Q : 10 > 5$.

(d) $P : 4$ *is an even integer.*
$Q : 5$ *is an even integer.*

Note: Unfortunately, there are many ways in English to say the exact same thing. This can make it difficult to translate between English phrases and conditional statements. For example, we can use $P \implies Q$ to represent **all** of these English phrases:

- If P, then Q
- P implies/guarantees Q
- P is a sufficient condition for Q
- For Q, it is sufficient that P.
- P only if Q
- Q, if P
- Q whenever P
- Q, provided that P
- Q is a necessary condition for P
- For P, it is necessary that Q.
- Q when P
- Whenever/Supposing P, then also Q.

Question 20.

Convert each of the following into a sentence of the form "If P*, then* Q*," without changing the meaning.* ***Look at the example in (a) and the phrases above!***

(a) Being divisible by 8 is a necessary condition for an integer to be divisible by 4.

Solution. If an integer is divisible by 4, then it is divisible by 8.

(b) A matrix is invertible provided that its determinant is not zero.

(c) You can be a Math major only if you pass Math 215.

Question 21.

Recall that a quadrilateral is a four-sided polygon. Let S *represent the following true conditional statement:*

If a quadrilateral is a square, then it is a rectangle.

Write this conditional statement in English using

(a) the word "whenever".

(b) the phrase "only if".

Question 22.

Necessary vs. Sufficient

Let x be a real number. Let $\mathrm{P} : x > 5$ *and* $\mathrm{Q} : x > 0$. *Each of the following statements is equivalent to either* $\mathrm{P} \implies \mathrm{Q}$ *or* $\mathrm{Q} \implies \mathrm{P}$. *Identify which ones are which (see the table above) and determine the validity of the given statement.*

(a) P *is a sufficient condition for* Q.

(b) P *is a necessary condition for* Q.

(c) Q *is a sufficient condition for* P.

(d) Q *is a necessary condition for* P.

The previous questions should have shown that the implications $\mathrm{P} \implies \mathrm{Q}$ and $\mathrm{Q} \implies \mathrm{P}$ are not the same. The latter has a special name.

Definition 1.5.17

Let P and Q be propositions.

The **converse** of $\mathrm{P} \implies \mathrm{Q}$ is the implication $\mathrm{Q} \implies \mathrm{P}$.

The **contrapositive** of $\mathrm{P} \implies \mathrm{Q}$ is the implication $(\sim \mathrm{Q}) \implies (\sim \mathrm{P})$.

Question 23.

For the given proposition, write out the converse and the contrapositive.

(a) ***Proposition:*** *If an animal is a cat, then it is a mammal.*

Converse:

Contrapositive:

(b) ***Proposition:*** *If* $x + 1 > 5$, *then* $x > 4$.

Converse:

Contrapositive:

1.5.1 Biconditional Statements

We saw above that the implication $P \implies Q$ and it's converse $Q \implies P$ sometimes have the same truth value and sometimes do not.

Example 1.5.18

The statement "If n is even then $n+1$ is odd" is a true conditional statement. The converse, "if $n+1$ is odd, then n is even", is also true. Hence, both $P \implies Q$ **and** $Q \implies P$ are true.

Question 24. □

Complete the truth table for the statement $(P \implies Q) \wedge (Q \implies P)$.

P	Q	$P \implies Q$	$Q \implies P$	$(P \implies Q) \wedge (Q \implies P)$
T	*T*			
T	*F*			
F	*T*			
F	*F*			

Definition 1.5.19

For propositions P and Q, the **biconditional sentence** $P \iff Q$ is read as 'P if and only if Q', and has the same truth values as $(P \implies Q) \wedge (Q \implies P)$.

Note: We sometimes abbreviate the statement 'P if and only if Q' as 'P iff Q'.

You can fill in the truth table for $P \iff Q$ using the last question.

P	Q	$P \iff Q$
T	T	
T	F	
F	T	
F	F	

Question 25. □

Determine the truth value for each of the following biconditional sentences.

(a) *The moon is made of cheese if and only if the earth is flat.*

(b) $1+1=2$ *if and only if* $\cos(\pi) = -1$.

All definitions in mathematics are usually understood to be 'if and only if'. For example, the definition ''An even integer is an integer that is divisible by 2" could be better stated ''An integer is even if and only if it is divisible by 2." Biconditionality is a good test of whether a statement can qualify as a definition or if it is just a description.

Note:

$P \iff Q$ translates the following phrases:

- P if and only if Q
- P iff Q
- P if, but only if Q
- P is equivalent to Q
- P is necessary and sufficient for Q
- if P then Q and conversely

§1.6 Tautologies and Contradictions

Definition 1.6.20

A **tautology** is a propositional form that is true for every assignment of truth values to its components. A **contradiction** is a propositional form that is false for every assignment of truth values to its components.

Observation. If S is a tautology, then $\sim$ S is a contradiction.

Question 26.

Determine if any of the given statements are tautologies or contradictions.

(a) $P \vee (\sim P)$

(b) $Q \implies (P \vee Q)$

(c) $P \wedge (\sim P)$

(d) $(\sim P \vee Q) \wedge (P \wedge \sim Q)$

□

Note: We will occasionally use the symbols $\mathscr{T}$ for a statement that is a tautology and $\mathscr{O}$ for a contradiction.

Question 27.

Show that $[(P \implies Q) \wedge (Q \implies R)] \implies (P \implies R)$ *is a tautology.*

In symbolic logic, this is an important logical argument form called **syllogism**.

□

1.6.1 More Examples of Compound Statements

What does $P \vee \sim Q \iff R \implies S$ mean? We don't know because it can be interpreted in multiple ways:

$$(P \vee (\sim Q)) \iff (R \implies S) \qquad \text{or} \qquad (P \vee (\sim Q \iff R)) \implies S.$$

Moral of the Story: **Use parentheses**!!!!

Question 28.

We wish to find the truth table for the statement $(P \wedge \sim Q) \implies R$.

Recall that if you are trying to form a truth table for a proposition with 3 component statements, then you will need $2^3 = 8$ *rows in your truth table. The next step is to determine the columns to be used. One way to do this is to work backward from the form of the given statement. For* $(P \wedge \sim Q) \implies R$, *the last step is to deal with the conditional operator* ($\implies$). *To do this, we need to know the truth values of* $(P \wedge \sim Q)$ *and* R. *To determine the truth values for* $(P \wedge \sim Q)$, *we need to apply the rules for the conjunction operator* ($\wedge$) *and we need to know the truth values for* $\sim Q$.

P	Q	R	$\sim Q$	$(P \wedge \sim Q)$	$(P \wedge \sim Q) \implies R$
T	*T*	*T*			
T	*T*	*F*			
T	*F*	*T*			
F	*T*	*T*			
T	*F*	*F*			
F	*T*	*F*			
F	*F*	*T*			
F	*F*	*F*			

Question 29.

Suppose the statement $((P \wedge Q) \vee R) \implies (R \vee S)$ *is false. Find the truth values of* P, Q, R, *and* S. *(This can be done without a truth table.)*

Question 30.

Suppose P *is false and the statement* $(R \implies S) \iff (P \wedge Q)$ *is true. Find the truth values of* R *and* S. *(This can be done without a truth table.)*

§1.7 Logical Equivalence

We have seen via several previous exercises and examples different statements that have identical truth tables. That is, for the same combination of T and F values, we obtain the same validity. For example, you saw in a previous question that an implication $P \implies Q$ and its contrapositive $(\sim Q) \implies (\sim P)$ have the exact same truth table.

Definition 1.7.21

Two statements are called **logically equivalent** if and only if they have the same truth tables.
We will use an equal sign "=" to denote logical equivalence between statements.

Question 31.

□

Prove that *the statements* $(P \wedge Q) \vee (P \wedge R)$ *and* $P \wedge (Q \vee R)$ *are logically equivalent. To do this, you can draw one truth table, or two, but in either case,* ***explain why your tables are proof that these statements are logically equivalent.***

Sometimes when we are attempting to prove a theorem, we may be unsuccessful in developing a proof for the original statement of the theorem. However, in some cases, it is possible to prove an equivalent statement. Knowing that the statements are equivalent tells us that if we prove one, then we have also proven the other.

The following are some significant logical equivalences. You have already proven some of these and the rest can be verified by constructing truth tables.

Theorem 1.7.22

For statements P, Q, *and* R,

(a) Double Negation Law:
$P = \sim(\sim P)$

(b) Commutative Law:
$P \wedge Q = Q \wedge P$
$P \vee Q = Q \vee P$

(c) Associative Law:
$P \wedge (Q \wedge R) = (P \wedge Q) \wedge R$
$P \vee (Q \vee R) = (P \vee Q) \vee R$

(d) Distributive Law:
$P \wedge (Q \vee R) = (P \wedge Q) \vee (P \wedge R)$
$P \vee (Q \wedge R) = (P \vee Q) \wedge (P \vee R)$

(e) DeMorgan's Law:
$\sim(P \wedge Q) = \sim P \vee \sim Q$
$\sim(P \vee Q) = \sim P \wedge \sim Q$

The results in theorem 23 have been shown previously as examples, or proven by you in a previous question. These give the **Or-Form** of an implication, the contrapositive of an implication, and the defining equivalence of a biconditional statement.

Theorem 1.7.23

For statements P *and* Q,

(a) $P \implies Q$ *is equivalent to* $(\sim P) \vee Q$.

(b) $P \implies Q$ *is equivalent to* $(\sim Q) \implies (\sim P)$.

(c) $P \iff Q$ *is equivalent to* $(P \implies Q) \wedge (Q \implies P)$.

The following logical equivalences are the basis for some of our proof methods that we discuss in the next several chapters!

Theorem 1.7.24

For statements P, Q, *and* R,

(a) $(P \vee Q) \implies Q$ *is equivalent to* $P \implies Q$.

(b) $P \implies (Q \implies R)$ *is equivalent to* $(P \wedge Q) \implies R$.

(c) $(P \wedge (\sim Q)) \implies \mathscr{C}$ *is equivalent to* $P \implies Q$. *(Recall that* $\mathscr{C}$ *stands for a contradiction.)*

The following is a form of distribution for conditional statements.

Theorem 1.7.25

For statements P, Q, *and* R,

(a) $P \implies (Q \wedge R)$ *is equivalent to* $(P \implies Q) \wedge (P \implies R)$.

(b) $(P \vee Q) \implies R$ *is equivalent to* $(P \implies R) \wedge (Q \implies R)$.

(c) $P \implies (Q \vee R)$ *is equivalent to* $(P \implies Q) \vee (P \implies R)$.

Question 32.

Let a and b be integers. Suppose we are trying to prove the following:

If 3 is a factor of $a \cdot b$, then 3 is a factor of a or 3 is a factor of b.

Explain why we will have proven this statement if we prove the following:

If 3 is a factor of $a \cdot b$ and 3 is not a factor of a, then 3 is a factor of b.

Question 33.

Let a be a real number and let f be a real-valued function defined on an interval containing $x = a$. Consider the following conditional statement:

If f is differentiable at $x = a$, then f is continuous at $x = a$.

Which of the following statements have the same meaning as this conditional statement and which ones are negations of this conditional statement?

> ***Note:*** This is not asking which statements are true and which are false. It is asking which statements are logically equivalent to the given statement. It might be helpful to let P represent the hypothesis of the given statement, Q represent the conclusion, and then determine a symbolic representation for each statement. Instead of using truth tables, try to use already established logical equivalencies to justify your conclusions.

(a) *If f is continuous at $x = a$, then f is differentiable at $x = a$.*

(b) *If f is not differentiable at $x = a$, then f is not continuous at $x = a$.*

(c) *If f is not continuous at $x = a$, then f is not differentiable at $x = a$.*

(d) *f is not differentiable at $x = a$ or f is continuous at $x = a$.*

(e) *f is not continuous at $x = a$ or f is differentiable at $x = a$.*

(f) *f is differentiable at $x = a$ and f is not continuous at $x = a$.*

Question 34.

Challenge Question

Using as many component statements as you wish (e.g., P, Q, R, . . .) and the symbols $\sim$, $\vee$, $\wedge$, $\implies$, *and* $\iff$, *construct each of the following (if possible). The first one is done for you.*

(a) A statement such that there are ***exactly zero*** *assignments of truth values to the component statements that result in a true statement.*

Solution. $P \wedge (\sim P)$ ■

(b) A statement such that there is ***exactly one*** *assignments of truth values to the component statements that result in a true statement.*

(c) A statement such that there are ***exactly two*** *assignments of truth values to the component statements that result in a true statement.*

(d) A statement such that there are ***exactly three*** *assignments of truth values to the component statements that result in a true statement.*

Question 35.

Challenge Question 2

For every $n \in \mathbb{N}$, *is it possible to construct a statement such that there are exactly* n *assignments of truth values to the component statements that result in a true statement?*

The answer is Yes! Can you figure out how?

§1.8 Quantifiers

Recall that **open sentences** are sentences like:

$$P(x): x \geq 0, \quad Q(x,y): x^2 - y = 0, \quad R(x,y,z): \text{If } x^2 = y, \text{ then } z > y.$$

These are neither true nor false and only become a statement when the variable(s) is/are assigned a specific value.

Definition 1.8.26

An **open sentence** $P(x_1, x_2, \ldots, x_k)$ is a sentence containing one or more variables that becomes a statement only when the variables are assigned specific values.

The realm of all possible values that the variables may be assigned is called the **universe**, usually denoted by $\mathscr{U}$.

Definition 1.8.27

The collection of all values of the variables in the universe that make a true proposition upon substitution into the open sentence is called the **truth set** of the open sentence.

Before we can give an example, we must decide what objects are available for use; we must have a specified **universe of discourse** $\mathscr{U}$. Usually, it will be apparent from context what $\mathscr{U}$ should be. Often, $\mathscr{U}$ will be chosen from the following:

$$\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}.$$

Example 1.8.28

Consider the open statement $P(x): x^2 < 4$.

If $\mathscr{U}$ is $\mathbb{R}$ then the truth set would be $(-2, 2)$. If $\mathscr{U} = \mathbb{Z}$, then the truth set would be $\{-1, 0, 1\}$.

Question 36.

Determine the truth set for the given open sentence and universe of discourse.

(a) *For* $\mathscr{U} = \mathbb{R}$ *and* $P(x): x^2 = 2$.

(b) *For* $\mathscr{U} = \mathbb{Z}$ *and* $P(x): x^2 = 2$.

(c) *For* $\mathscr{U} = \mathbb{Z} \times \mathbb{Z}$ *and* $P(x,y): x = -5$ *and* y *is even.*

(d) *For* $\mathscr{U} = \mathbb{N}$ *and* $P(x):$ *If* x *is even, then* x *is a multiple of* 2.

Note: In elementary mathematics, the process of 'solving' an equation is essentially the same as determining the truth set for the equation, which is an open sentence. In this case, we often call the truth set the **solution set**.

Definition 1.8.29

With a universe specified, two open sentences $P(x)$ and $Q(x)$ are **equivalent** iff they have the same truth set.

Question 37.

□

(a) Find a universe of discourse that makes $x^2 + 1 = 5$ equivalent to $x = 2$.

*(b) Find a universe of discourse that makes $x^2 + 1 = 5$ **not** equivalent to $x = 2$.*

Question 38.

□

(a) Write an open sentence in the universe of cats that is true for no member of the universe.

(b) Write an open sentence in the universe of vegetables that is true for at least one but not every member of the universe.

Unfortunately, the logical connectives $\vee$, $\wedge$, $\iff$, and $\sim$ are not enough to yield every kind of statement we want to use in mathematics (see page 53 of book for a good example). Thus, we introduce **quantifiers** to expand the kinds of mathematical statements we can discuss with logic.

Definition 1.8.30

Let $P(x)$ be an open sentence and $\mathscr{U}$ the universe of discourse. The sentence

$$(\forall x \in \mathscr{U})[P(x)]$$

is a statement and is read as '**For all** $x \in \mathscr{U}$, $P(x)$'.

The statement $(\forall x \in \mathscr{U})[P(x)]$ is true if and only if the truth set of $P(x)$ is the **entire universe** $\mathscr{U}$.

The symbol $\forall$ is called the **universal quantifier**.

Question 39.

□

Determine if the following statements are true or false.

(a) $(\forall x \in \mathbb{R})(x^2 + 1 \geq 0)$

(b) $(\forall x \in \mathbb{Z})(\sqrt{x} \in \mathbb{Z})$

(c) $(\forall x \in \mathbb{Z})(x^2 \in \mathbb{Z})$

Definition 1.8.31

Let $P(x)$ be an open sentence and $\mathscr{U}$ the universe of discourse. The sentence

$$(\exists x \in \mathscr{U})[P(x)]$$

is a statement and is read as '**There exists** $x \in \mathscr{U}$ **such that** $P(x)$' or 'For some $x \in \mathscr{U}$, $P(x)$'.

The statement $(\exists x)[P(x)]$ is true if and only if the truth set of $P(x)$ is nonempty.

The symbol $\exists$ is called the **existential quantifier**.

Question 40.

Given the universe $\mathscr{U} = \mathbb{N}$, determine if the following statements are true or false.

(a) $(\exists x)(x - 3 = 0)$

(b) $(\exists x)(x^2 - 2x - 3 = 0)$

(c) $(\exists x)(x + 3 = 0)$

What if we changed the universe to be $\mathscr{U} = \{x \in \mathbb{R} : |x| = 3\}$?

(a) (b) (c)

Question 41.

Describe the set of all odd integers using a set builder notation.

Note:

- If the universe is understood, we will often just write $(\forall x)P(x)$ or $(\exists x)P(x)$.
- **Universal** - $\forall$: Look for key words like 'for all', 'for every', 'for each'
- **Existential** - $\exists$: Look for key words like 'some', 'at least one', 'there exist(s)', 'there is'
- An open sentence $P(x)$ does not have a truth value. But quantified sentences like $(\exists x)P(x)$ and $(\forall x)P(x)$ do have a truth value.
- To prove that $(\exists x)P(x)$ is false, we must show that the truth set is empty.

Question 42.

Write the given statement as an English sentence and determine the validity.

(a) $(\forall x \in \mathbb{R})(x^2 \geq 0)$

(b) $(\exists a \in \mathbb{Z})(3a \notin \mathbb{Z})$

(c) $(\exists a \in \mathbb{R})(\forall x \in \mathbb{R})(ax = x)$

(d) $(\forall x \in \mathbb{Z})(\exists y \in \mathbb{Z})(x^2 = y)$

The order in which quantifiers appear in a statement matters. If changed, the entire meaning (and validity) of the statement can be changed.

Question 43.

Order of Quantifiers

Consider $\mathcal{U} = \mathbb{R}$ *for this problem.*

(a) Consider the following statement:

$$(\forall x)(\exists y)(x < y).$$

Write out what this statement means and determine if it is true or false.

(b) Now swap the order of the quantifiers:

$$(\exists y)(\forall x)(x < y)$$

Write out what this statement means and determine if it is true or false.

1.8.1 More on Conditional Statements - Hidden Quanitifiers

This section contains a lot of text, but is important, so please read it carefully!

Let $\mathscr{U} = \mathbb{N}$ and Consider the sentence

$$\mathrm{R}(x): \underbrace{\textbf{If } x \textbf{ is even}}_{\mathrm{P}(x)}\textbf{, then } \underbrace{x \textbf{ is a multiple of } 4.}_{\mathrm{Q}(x)}$$

- It is certainly true if $x = 8$ (since P(8) is true and Q(8) is true).
- It is **vacuously true** if $x = 3$ (since P(3) is false and Q(3) is false).
- It is false if $x = 6$. (since P(6) is true and Q(6) is false)

Thus the above conditional sentence

$$\mathrm{R}(x): (\mathrm{P}(x) \implies \mathrm{Q}(x))$$

is in fact an open sentence.

However, this is not how mathematicians usually interpret the above implication. We secretly think of there being a **universal quantifier** at the front of the implication, like so:

$$(\forall x \in \mathscr{U})(\mathrm{P}(x) \implies \mathrm{Q}(x)).$$

Now we have an actual **statement**. A statement has exactly one truth value, either true or false. For example, consider the statement:

$$(\forall x \in \mathbb{N})(x \text{ is even} \implies x \text{ is a multiple of } 4).$$

Now we know that this is a **false** statement, since its truth set ($\{1, 3, 4, 5, 7, 8, 9, 11, 12, 13, \ldots\}$ is **not** equal to the entire universe $\mathbb{N}$.

To summarize[ii], from now on, **implications will be usually treated as statements.** What this means is

- if we have a conditional statement of the form "$\mathrm{P} \implies \mathrm{Q}$", we will translate it to English as "If P, then Q".
- On the other hand, when we have an implication that is also an open sentence of the form "$\mathrm{P}(x) \implies \mathrm{Q}(x)$", we will translate that as "For all x in the universe, if $\mathrm{P}(x)$ then $\mathrm{Q}(x)$". The hidden quantifier allows us to change the open sentence "$\mathrm{P}(x) \implies \mathrm{Q}(x)$" into a conditional statement that is either definitely true or definitely false.

  As an example, we will say that the next sentence is a false **statement** (as it is not true for all x).

  If x is even, then x is a multiple of 4.

■ **Question 44.** □

Come up with an open sentence $\mathrm{P}(x) \implies \mathrm{Q}(x)$ such that, for some x's, the implication is true, but for others, the implication is false. Then make the implication a statement by adding a universal quantifier in front. Is your statement true or false?

[ii] see also the definition given on page 57 of the text.

Vacuously True statements. A conditional statement is called **Vacuously True** if the truth set of the hypothesis is the null set, i.e. the antecedent cannot be satisfied within the specified universe. For example, the statement

$$(\forall x \in \mathbb{R})(\text{If } x^2 < 0, \text{ then } x = 5)$$

is vacuously true!

Question 45.

□

Consider the proposition "If $\varepsilon > 0$*, then there exists* $N \in \mathbb{N}$ *such that* $\frac{1}{N} < \varepsilon$*." Assume the universe is the set* $\mathbb{R}$*.*

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

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

§1.9 Translating English to Symbolic Logic

Question 46. □

Translate these sentences into symbolic logic. The first two have been done for you as examples.

(a) The number x is positive but the number y is not positive.

Solution. $(x > 0) \wedge (y \leq 0)$ ■

(b) Every natural number is greater than 0.

Solution. $(\forall x \in \mathbb{N})(x > 0)$

or you could write

$(x \in \mathbb{N}) \implies (x > 0)$ ■

(c) At least one of the integers x and y is even.

(d) For every prime number p there is another prime q with $q > p$.

(e) For every positive number ε, there is a positive number δ for which, $|x - a| < \delta$ implies $|f(x) - f(a)| < \varepsilon$.

(f) There exists an integer solution to $x^2 - 2x - 1 = 0$.

Note: Usually, you can translate English sentences of the form 'All P(x) are Q(x)' as

$$(\forall x)(\mathrm{P}(x) \implies \mathrm{Q}(x)),$$

and sentences of the form 'Some P(x) are Q(x)' as

$$(\exists x)(\mathrm{P}(x) \wedge \mathrm{Q}(x)).$$

Example 1.9.32

'All integers divisible by 4 are even" translates as

$$(\forall x \in \mathbb{Z})(4 \text{ divides } x \implies x \text{ is even }).$$

''Some prime numbers are even" translates as

$$(\exists n \in \mathbb{Z})((n \text{ is prime }) \wedge (n \text{ is even })).$$

Question 47.

Consider the sentence "People dislike taxes." This sentence could be interpreted several ways. Give a symbolic translation for each of these interpretations. The first one has been done for you.

It might be helpful to let P *be the set of all people and* T *be the set of all taxes.*

(a) "All people dislike all taxes."

Solution.

$$(\forall p \in \mathrm{P})(\forall t \in \mathrm{T})(p \text{ dislikes } t)$$

(b) "All people dislike some taxes."

(c) "Some people dislike all taxes."

(d) "Some people dislike some taxes."

Question 48.

A real number x is ***rational*** *if and only if there are integers p and q, with $q \neq 0$ such that $x = \frac{p}{q}$. Translate this definition into symbols.*

Question 49.

Let $\mathrm{E}(k)$ *stand for "k* ***is even***", *and* $\mathrm{M}(p)$ *stand for "p* ***is a multiple of*** *7". Write a symbolic translation of "****There is a multiple of*** *7* ***which is even***" *using these open sentences.*

§1.10 Negating Statements

DeMorgan's Laws from theorem 22 tell us how to negate statements involving $\wedge$ and $\vee$.

Question 50. **Negating Statements**

Express each mathematical statement using $\wedge$, $\vee$, and $\sim$ as appropriate. Then write the negation of each.

(a) The number x equals 0, but the number y does not.

Statement: $(x = 0) \wedge (y \neq 0)$

Negation:

(b) The matrix A either has determinant zero or it is not invertible.

Statement:

Negation:

(c) The numbers x and y are both perfect squares.

Statement:

Negation:

Question 51. **Negating Quantifiers**

(a) Write the negation of the statement $(\forall x \in \mathbb{Z}, \sqrt{x} \in \mathbb{Z})$. Which is true and which is false?

(b) Write the negation of the statement $(\exists y \in \mathbb{R}, y^2 < 0)$. Which is true and which is false?

Theorem 1.10.33

If $P(x)$ *is an open sentence, then*

(a) $\sim(\forall x, P(x))$ *is equivalent to* $\exists x, \sim P(x)$

(b) $\sim(\exists x, P(x))$ *is equivalent to* $\forall x, \sim P(x)$

Question 52.

Re-write each sentence so that it has universal/existential quantifiers, and then write the negation. The first one has been done for you as an example. In most cases, we want to write this negation in a way that does not use the negation symbol.

(a) The area of a rectangle is its length times its width.

Solution. **Quantifiers:** For all rectangles R, the area of R is length times width.

Negation: There exists a rectangle R such that the area of R is not its length times width.

(b) The polynomial $x^2 + x + 1$ *has a real root.*

Quantifiers:

Negation:

(c) Every Wookie is named Chewbacca.

Quantifiers:

Negation:

(d) If all cats meow then some dogs bark.

Quantifiers:

Negation:

Question 53.

Negating Implications

How do we negate implication of the form $P \implies Q$ *when* P *and* Q *are open sentences? Firstly, recall from Section 1.8.1 that in this situation, we should think of* $P \implies Q$ *as*

$$(\forall x \in \mathscr{U})(P(x) \implies Q(x)).$$

Now recall that the conditional statement $P \implies Q$ *is defined as* $(\sim P \vee Q)$*. Use DeMorgan's law to check that this means*

$$\sim(P \implies Q) \text{ and } (P \wedge \sim Q)$$

are equivalent statements.

Therefore, $\sim (P \implies Q)$ is the same as

$$\sim (\forall x \in \mathscr{U}, P(x) \implies Q(x))$$

which is equivalent to

$$\exists x \in \mathscr{U}, \sim (P(x) \implies Q(x))$$

which is equivalent to

$$\exists x \in \mathscr{U}, [P(x) \wedge (\sim Q(x))].$$

Example 1.10.34

Let's negate the statement:

"If x is an even integer, then x^2 is even."

First, we translate into logical symbols:

$$(\forall x \in \mathbb{Z})(x \text{ even} \implies x^2 \text{ even }).$$

Now we negate:

$$\sim [(\forall x \in \mathbb{Z})(x \text{ even} \implies x^2 \text{ even})] \text{ is equivalent to}$$

$$(\exists x \in \mathbb{Z})[(x \text{ is even}) \wedge (x^2 \text{ is not even})]$$

In English, this reads

There exists an integer x such that x is even but x^2 is odd.

Question 54.

□

Write the negation of the statement in the form of an English sentence that does not use the symbols for negation or quantifiers.

(a) If x is a real number, then x^3 is greater than or equal to x^2.

(b) If $\sin(x) < 0$ then $x \notin [0, \pi]$.

Question 55.

□

If there are multiple quantifiers in a statement that you want to negate, you simply exchange each quantifiers one at a time and negate the inside (that is, $\forall$ become $\exists$ and $\exists$ become $\forall$). Write the negation of the following:

$$(\forall x \in \mathbb{Z})(\exists y \in \mathbb{Z})(\forall z \in \mathbb{Z})(x + y = z \text{ and } x - z = y).$$

Which is true: the original statement or the negation?

Question 56. Upper Bound for Subsets of $\mathbb{R}$

Let A *be a subset of the real numbers. A number* b *is called an upper bound for the set* A *provided that* $b \geq x$ *for each element* x *in* A.

(a) Write this definition in symbolic form by completing the following sentence:

Let $A \subseteq \mathbb{R}$. *A number* b *is called an upper bound for the set* A *provided that* _____ .

(b) Give examples of three different upper bounds for the set $A = \{x \in \mathbb{R} \mid 1 \leq x \leq 3\}$.

(c) Does the set $B = \{x \in \mathbb{R} \mid x > 0\}$ *have an upper bound? Explain.*

(d) Give examples of three different real numbers that are not upper bounds for the set $A = \{x \in \mathbb{R} \mid 1 \leq x \leq 3\}$.

(e) Complete the following in symbolic form: "Let A *be a subset of* $\mathbb{R}$. *A number* b *is* ***not*** *an upper bound for the set* A *provided that* _____ ."

(f) Without using the symbols for quantifiers, complete the following sentence: "Let A *be a subset of* $\mathbb{R}$. *A number* b *is not an upper bound for the set* A *provided that* _____ ."

(g) Are your examples in Part (d) consistent with your work in Part (f)? Explain.

Question 57. Least Upper Bound for a Subset of $\mathbb{R}$

Let A *be a subset of* $\mathbb{R}$. *A real number* α *is called the* ***least*** *upper bound for* A *provided that* α *is an upper bound for* A, *and if* β *is an upper bound for* A, *then* $\alpha \leq \beta$.

If we define

$$P(x) : x \text{ is an upper bound for } A,$$

then we can write the definition for least upper bound as follows: A real number α *is the least upper bound for* A *provided that*

$$P(\alpha) \wedge [(\forall \beta \in \mathbb{R})(P(\beta) \implies (\alpha \leq \beta))]$$

(a) Why is a universal quantifier used for the real number β?

(b) Complete the following sentence in symbolic form: "A real number α *is* ***not*** *the least upper bound for* A *provided that* _____ ."

(c) Complete the following sentence as an English sentence: "A real number α *is not the least upper bound for* A *provided that* _____ ."

§1.11 Annoying Sets and The Need for Rigor

When we defined sets for the first time, we used a very naïve definition of a set. More or less, we have been using the following definition, originally given by the German mathematician Georg Cantor in 1898:

> *"By a set we shall understand any collection into a whole of definite distinguishable objects of our intuition or thought."*

Similarly we can think of a set as any **collection** of objects that we can imagine. However, this simple definition actually starts to create a lot of problems.

Question 58. □

Define T *to be the* ***collection*** *of all sets that contain at least three elements:*

$$\mathrm{T} = \{\mathrm{X} : |\mathrm{X}| \geq 3\}.$$

Assumming T *is a set, is* T *an element of* T*?*

Question 59. □

Let $\mathrm{B} = \{\{\{\ldots\}\}\}$*? The '…' corresponds to an 'infinite' number of opening braces followed by an equal number of closing braces!*

(a) Is B *a set? Let's assume it is.*

(b) How many elements does B *have?*

(c) Is $\mathrm{B} \in \mathrm{B}$*?*

We will define a 'collection' to be **ordinary** if it does not contain itself. Most collections are ordinary, but as we saw in the last two example, some aren't. Here are some more examples:

- The collection of abstract ideas is an abstract idea.
- The collection of mathematical objects is a mathematical object.
- The collection of all collections is a collection.

Question 60. Russell's Paradox

Let R *be the collection of all ordinary sets:*

$$\mathrm{R} = \{\mathrm{X} \mid \mathrm{X} \notin \mathrm{X}\}.$$

Does R *contain itself? In other words , is* $\mathrm{R} \in \mathrm{R}$*?*

Question 60 is an example of a **paradox**. A paradox is a statement that can be shown to be both true and false, using a given set of rules and definitions. The term paradox is also used informally to describe a surprising or counterintuitive result that follows from a given set of rules.

The following is an analogy of Russell's Paradox (1902) that was given by Russell in 1918. Try using it on your roommate next time you want to purposefully confuse them!

> **Suppose there is a hairstylist in a village. She cuts the hair of only those people in the village who do not cut their own hair. Who cuts the hairstylist's hair?**

Our naïve approach to set theory (i.e., using natural language as opposed to formal logic) unfortunately allows for the possibility of defining a "set of all sets." As you can see, this leads to a paradox--precisely as the sentence "**this sentence is false**" did. Russell's paradox shows that we need to be very careful about the precise meaning of the word "contains" or "is in" (i.e. $\in$).

To avoid these sorts of paradoxes, people who study **set theory** have come up with a set of rules, called "axioms" that *basically forbid weird sets* like the ones above. This is good, because it means all of the mathematics that we build rests on solid theoretical foundations. Although you are unlikely to ever encounter these weird paradoxes when doing 'usual' mathematics, it is comforting to know that such pathological cases can be avoided by rigorously defining what a set is!

Definition 1.11.35

A set S is an object for which the question "Is x in S?" has an unambiguous answer. We write $x \in S$ (read "x is an element of S") if the answer is yes and $x \notin S$ if the answer is no.

Note: A great deal of research went into developing consistent axioms (i.e., free of contradictions) for set theory in the early 20th century. In 1908, Ernst Zermelo proposed a collection of axioms for set theory that avoided the inconsistencies of naive set theory. In the 1920s, adjustments to Zermelo's axioms were made by Abraham Fraenkel, Thoralf Skolem, and Zermelo that resulted in a collection of nine axioms, called **ZFC**, where ZF stands for *Zermelo* and *Fraenkel* and C stands for the *Axiom of Choice*, which is one of the nine axioms. There was a period of time in mathematics when the Axiom of Choice was controversial, but nowadays it is generally accepted. There is a fascinating history concerning the Axiom of Choice, including its controversy, that I encourage you to read up on. The Wikipedia link below is a good place to start. There are several competing axiomatic approaches to set theory, but ZFC is considered the canonical collection of axioms by most mathematicians.

Exploration Activity

See also:

- Zermelo-Fraenkel Axioms (https://en.wikipedia.org/wiki/Zermelo-Fraenkel_set_theory)
- Axiom of Choice (https://en.wikipedia.org/wiki/Axiom_of_choice)
- Zeno's paradox (https://en.wikipedia.org/wiki/Zeno's_paradoxes)

The next chapter will start by focusing more on Axioms, Definitions, and Theorems.

Chapter 2 | Proof Techniques

§2.1 Theorems, Axioms, and Definitions

Definition 2.1.36

A **theorem** is a statement that it true and can be verified as true.

A **proof** is a written verification, a justification of the truth of a theorem.

Below are some examples of Theorems that you have likely seen in Calculus or Geometry class.

Theorem 2.1.37: The Fundamental Theorem of Calculus

Let f be a continuous function on $[a,b]$. Then for any antiderivative F *of f on $[a,b]$,*

$$\int_a^b f(x)\,\mathrm{d}x = \mathrm{F}(b) - \mathrm{F}(a).$$

Theorem 2.1.38: The Pythagorean Theorem

Let c denote the length of the hypotenuse of a right triangle and let a and b denote the lengths of the other two sides. Then $a^2 + b^2 = c^2$.

Mathematics is the most rigorous scientific field. We accept statements like the Pythagorean Theorem or the Fundamental Theorem of Calculus because we can **prove** them. In fact, a lot of our time in this class is going to be spent learning how to prove such statements! However, even in mathematics, if you ask the question ''But why?'' enough times you arrive at a question without an answer. An axiom is the frustrated parent of the mathematical world's way of saying ''Because I said so.'' In reality, **an axiom is just something so fundamental that we assume it to be true without any proof that it is true.**

Here's a good example we mentioned in the last chapter. A **choice function** (also called selector or selection) is a function f, defined on a collection X of nonempty sets, such that for every set A in X, $f(\mathrm{A})$ is an element of A.

Axiom 2.1.39: The Axiom of Choice

For any set X *of nonempty sets, there exists a choice function f defined on* X.

Another way to think of this - the AoC says that given a collection of perhaps infinitely many sets, you can choose one element from each of them. Seems pretty obvious, right? But can you explain why such a choice should exist? In fact, there is no way to prove [i] it!

[i] To be clear, what we are saying that this statement doesn't follow from simpler assumptions about properties of sets. The axiom can be 'verified to be true' -- a 'proof' of the axiom is that it is true by assumption; all we are saying that it doesn't need a proof.

Most theorems in mathematics are of the form "**if** P**, then** Q." This is by far the most common form, but not all theorems will appear this way. For instance, here is a theorem:

Theorem 2.1.40

$\sqrt{2}$ is not a rational number.

However, we can re-write this theorem so that it is in a form of P $\implies$ Q:

Theorem 2.1.41

If $x^2 = 2$, then x cannot be a rational number.

We will prove the above theorem in claim 80.

You will also see a few other terms such as lemma, proposition, corollary, conjecture etc. See appendix B for a list.

Exploration Activity

Watch this youtube video to learn about the history and the surprises in axiomatic Mathematics and how it led to the discovery of computers.

Before we begin proving theorems, we also need to talk about definitions. Definitions are the cornerstone of advanced mathematics. We work from axioms and definitions to build new ideas. As the semester progress, you'll learn to work with a lot of new and interesting definitions. Some will be somewhat familiar, while others will be very new.

Two important things to keep in mind about mathematical definitions:

- Mathematical definitions are **prescriptive**, not **descriptive**. You only know a definition if you can restate it **verbatim**. Paraphrasing isn't good enough.

  Read appendix A carefully before reading ahead.

- Mathematical definitions change between textbooks and mathematical works. Often, in a textbook or paper, you will have to refer back to find the specific definition the author is using.

§2.2 Divisibility

We will make use of the following definitions from elementary number theory throughout the semester. Although you are likely already familiar with these math concepts, we need to have an agreement on their definition to properly communicate proofs to one another.

Definition 2.2.42

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

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

So for example, $22 = 2 \cdot 11$, so 22 is even. But 22 is not odd, because there are no integers a such that $22 = 2a + 1$.

Warning: Notice that we did not define "even" as being divisible by 2. That's partly because we haven't really clarified what 'divisible' means. In fact we are going to define what it means to be divisible by 2 in the next page.

Note: Mathematical definitions are always biconditional statements but are often presented as conditional statements, like above. They are understood to be biconditional from context.

Definition 2.2.43

Two integers are said to have the same **parity** if they are both even or they are both odd. Otherwise they have **opposite parity**.

Question 61.

Answer whether the following statements are true or false and explain your reasoning.

(a) *6 is not even since for $a = 5$, $6 \neq 2a$.*

(b) *The integer 0 is both even and odd.*

(c) *For all integers a, the two numbers $7a + 1$ and $2a + 1$ have **opposite** parity.*

Definition 2.2.44

Let a and b be integers. If $b = ac$ for some $c \in \mathbb{Z}$, then we say a **divides** b. We denote this by writing

$$a \mid b.$$

In that case, we also say that b is a **multiple** of a and that a is a **divisor** of b.

Note: The expression "$a \mid b$" is a mathematical **statement** that is either true or false. This is not to be confused with the expression "a/b" (with a slanted slash) which is the rational **number** $\frac{a}{b}$.

Question 62.

Answer the following questions. Look very carefully at the definitions!

(a) List all divisors of 12.

(b) List 3 *multiples of* 17.

(c) Consider the statement $a \mid 0$. *What integers* a *make this statement true?*

(d) Is $-4 \mid 20$ *true or false?*

(e) Is $16 \nmid 2$ *true or false (that symbol means "does not divide")?*

(f) What two integers divide every integer?

Definition 2.2.45

Let a and b be integers, not both zero. We say the integer d is the **greatest common divisor (gcd)** of a and b, and write $d = \gcd(a, b)$, if d is the largest integer that divides both a and b. The **least common multiple**, denoted $\operatorname{lcm}(a, b)$, is the smallest positive integer that is a multiple of both a and b.

Question 63.

What does the expression "a ***and*** b ***integers, not both zero****" mean? Can you rewrite it using symbolic logic?*

Suppose we did not have the stipulation in definition 45. Then what would be the value of $\gcd(0, 0)$*? Explain.*

Question 64.

Determine the greatest common divisor or least common multiple:

(a) lcm(15, 21)

(b) lcm(−8, 20)

(c) lcm(−24, −9)

(d) gcd(15, 21)

(e) gcd(−8, 20)

(f) gcd(−24, −9)

Definition 2.2.46

A natural number n is **prime** if it has exactly two *positive* divisors, 1 and n. Also, n is **composite** if it factors as $n = ab$ where $a, b > 1$.

Definition 2.2.47

We say that nonzero integers a and b are **relatively prime**, or **coprime**, if $\gcd(a, b) = 1$.

Question 65.

Are the following pairs of integers coprime? Why or why not?

(a) *15 and 28.*

(b) *42 and -9.*

Some things are so basic that we do not need to prove them in this course, e.g., properties of addition and multiplication of real numbers. We are treating them as axioms (although most are proven using set theory). One fact we will eventually prove, but can take as a fact for now, is something you have probably seen in middle school - **The Division Algorithm**.

Theorem 2.2.48: The Division Algorithm

Given integers a and b with $b > 0$, there exist unique integers q and r for which $a = bq + r$ and $0 \leq r < b$.

Another theorem you have probably seen before, but will be proved later is the following.

Theorem 2.2.49: The Fundamental Theorem of Arithmetic

Every natural number $n > 1$ can be represented in exactly one way as

$$n = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k},$$

where $p_1 < p_2 < \dots < p_k$ are distinct prime numbers and $a_1, a_2, \dots, a_k \in \mathbb{N}$.

Question 66.

Write the unique prime factorization of the following numbers:

(a) 28 *(b)* 120 *(c)* 15400

The next section spells out, in great detail, how we go about proving things in mathematics. However, after several classes thinking about sets and logic, all of you are used to making arguments about mathematics. So let us try to prove some things preemptively, just to try it out, using some of the definitions above.

Question 67.

Try to write up a "proof" for each of the following propositions. Simply write up a brief argument explaining why you think the statement is true.

(a) The sum of any two consecutive integers is odd.

(b) If n is an even integer, then n^2 is an even integer.

(c) Let n, m and a be integers. If $a \mid n$ and $a \mid m$, then $a \mid (n + m)$.

§2.3 Direct Proof

In order to learn to write proofs, we will start by proving statements that you already know are true. You might sometimes think to yourself "Isn't that obvious?" Yes. It probably is--but we want to focus on **the proof**, not just the statement!

Most theorems in mathematics can be written in the form $P \implies Q$. For example,

If a function is differentiable at $x = a$ then it is continuous at $x = a$.

Therefore, will start by learning a simple method of proving statements of the form $P \implies Q$.

2.3.1 Direct Proof of $P \implies Q$

$P \implies Q$ is false only when P is true and Q is false. Therefore, to prove $P \implies Q$ is true by direct proof, we assume P is true, and then show that Q must be true. Here is a rough outline of a direct proof that $P \implies Q$.

Proposition: If P, then Q.

Proof. Assume P is true.
⋮
Therefore, Q is true.
Thus $P \implies Q$. ■

The difficulty here is, of course, in those $\cdots$. It is in these $\cdots$ that we use previous definitions and known results to lead us from assuming P is true, to arriving and the validity of Q. Sometimes the details of the logical path will be a straightforward matter of successive application of the definitions. Often, however, your own creativity and ingenuity will be necessary. This is the art of proof and it is what we are learning in this class.

Read the textbook and fill in the steps below.

Proposition 2.3.50

If n is odd, then n^2 is odd.

Proof of proposition 50.

■

Things to notice about this proof.

- First, we identify the two statements P and Q. Then we start by assumming P is true (''Suppose n is odd'').
- We use the definition of odd to decide exactly what we need to show.
- We use words (not just symbols) so that it is clear and easy to read.
- We end with a happy little proof box ■.

■ Question 68. □

*What's **wrong** with the following ''proof''?*

Proposition 2.3.51

If x is odd, then x^2 is odd.

Proof. Suppose x is odd. Then because an odd times an odd has to be odd, x^2 has to be odd. ■

For each of the following claims, answer the questions to figure out **how** to prove the claim. Then prove the claim in the box. You should write a **real** proof in the box (meaning, don't just sketch a proof or write ''True'', but try to write a something you could show to a friend and they would understand it without your help).

■ Question 69. □

Consider the following proposition.

Proposition 2.3.52

For any integers a, b, and c, if $a \mid b$ and $a \mid c$, then $a \mid (b+c)$.

(a) *It's best to go in steps. First, we have the key word **any**, which means this starts with a universal quantifier. In fact there are three of them: one for each of the variables a, b, and c. Then we've got an **and** and an **if... then.** So first let's translate above proposition to symbolic logic.*

This is not part of the final ''proof''. Instead, the reason for above exercise is that each bit of logic that makes up a statement (quantifiers and connectives) has a corresponding move in writing the proof!

*So let's think about how to start our proof. We want to prove something about **all** possible triples of integers a, b, c. But how would we handle all numbers at once? The answer is that we don't. Instead we start as follows:*

Let a, b, and c be integers.

This allows us to focus on the qualitative property of a, b, c being integer instead of their actual values. We never ever EVER want to assume exact values for a, b and c.

(b) *Ok, the next logical symbol to tackle is* $\implies$ [ii]. *As we mentioned early, here we will start by assumming the antecedent to be true.*

According to Definition 44, what does it mean to say that $a \mid b$*?*

(c) *According to Definition 44, what does it mean to say that* $a \mid c$*?*

Make sure to use different letters for the quotients, because they might be different! Always err on the side of using more variables.

(d) *Now what does it mean to prove* $a \mid (b+c)$*? The statement is equivalenbt to* $(\exists m \in \mathbb{Z})(b+c=am)$*. It's an existential claim! So we have to propose some* m *and verify that it satisfies* $b+c=am$*. That is, we need to solve the equation* $b+c=am$*. Now we could just write* $m=\dfrac{b+c}{a}$*, but that's no good because we need* m *to be an integer, and* ***there's no guarantee that any random fraction is going to be an integer.***

So how can we show that a suitable integer m *exists using the assumption that the antecedent is true?*

Proof of proposition 52.

Let $a, b,$ and c be integers.

■

[ii] The ' $\implies$ ' has precendence over the 'and'. Why?

2.3.2 How to Start a Proof

The best way to learn how to write proofs is to start writing proofs! You can use the proofs from Chapter 4 in the textbook to serve as a model. However, before you even start trying to write a proof, you must first figure out

- What do I **know**?
- What do I need to **show**?

This might involve generating a lot of scratch work, pictures, and ideas that don't work out. The process can involve hunches, speculation, memory, intuition, cleverness, surprises, luck, and assorted psychological and intellectual skills. But, the final written proof is unlikely to exhibit these elements of mental drama, it is more like the final draft of a paper. You hide all of the difficult work and just present a clear, logical, beautiful proof.

> [iii] *...The discoverer of a proof is under no moral or scientific obligation to display to the reader the false starts, aimless meanderings, fruitless speculations, and outright blunders experienced while searching for a proof. It's the final argument that matters. An unfortunate consequence of all this is that the reader studying a proof may think, "This complicated argument flows along so smoothly and so cleverly. I could never do something like this." But actually the theorem prover, like the theorem reader, is (or was) a human being, probably with the standard number of anxieties and complexes. It's just that the argument has been organized, cleaned up, and manicured before going to the printer...*

The next proof is a good example of this. You'll probably have to think for a while about how to prove it before you start writing.

Important Note. The answers to the questions ''What do I **know**?" and ''What do I need to **show**?" are almost always found by going back to **definitions!**

This is a good time to read appendix C for a list of practices in Mathematical writing. Make sure you actually read through the list as we will refer to specific violation of these rules as 'bad' proof writing techniques.

[iii] Larry J. Gerstein. **Introduction to mathematical structures and proofs**. Springer-Verlag New York, 2016.

2.3.3 Direct Proof of $(\forall x \in \mathscr{U})\mathrm{P}(x)$

Every universally quantified statement can be expressed as a conditional statement.

Theorem 2.3.53: (Fact 2.2, pg. 58).

Suppose S *is a set and* $\mathrm{Q}(x)$ *is a statement about* x *for each* $x \in \mathrm{S}$. *Then the following mean the same thing:*

$$(\forall x \in \mathrm{S})\mathrm{Q}(x) \text{ and } (x \in \mathrm{S}) \implies \mathrm{Q}(x).$$

So proving a statement of the form $(\forall x \in \mathscr{U})\mathrm{P}(x)$ goes something like this:

Proposition: Every x in $\mathscr{U}$ satisfies $\mathrm{P}(x)$.

Proof. Let x be an arbitrary object in the universe $\mathscr{U}$.
⋮
Use the definition of $\mathscr{U}$ to find the defining properties of x.
⋮
Use these properites to show $\mathrm{P}(x)$ is true.
Since the choice of x was arbitrary, this implies $(\forall x)\mathrm{P}(x)$ is true. ■

■ **Question 70.** □

Consider the following proposition.

Proposition 2.3.54

Every odd integer is the difference of two squares. (Example: $7 = 4^2 - 3^2$*)*

(a) First of all, note that we could rewrite this in $(\forall n \in \mathscr{U})\mathrm{P}(n)$ *form where* $\mathscr{U} = \{2k+1 \mid n \in \mathbb{Z}\}$ *and*

$$\mathrm{P}(n) : n \text{ can be written as the difference of two squares}$$

(b) Usually to figure out how to prove something, we start by finding some examples. Find two integers a *and* b *such that* $5 = a^2 - b^2$*, then do the same for* 9 *and* 11.

(c) What do you notice about the relationship between a *and* b*?*

Proof of proposition 54.

Let n be an odd integer.

■

2.3.4 Counterexamples

So far in this section, our focus has been on proving statements that involve either explicit or hidden universal quantifiers. However, another important skill for mathematicians is to be able to recognize when a statement is false and then to be able to prove that it is false. For example, suppose we want to know if the following claim is true or false.

Claim 2.3.55

For each integer n, if $5 \mid n^2 - 1$, then $5 \mid (n-1)$.

If you try to prove this claim using direct proof, an outline would look like

Proof. Let n be an integer such that $5 \mid (n^2 - 1)$.
Then $n^2 - 1 = 5k$ or $n^2 = 5k + 1$ for some integer k.
⋮
Then $n - 1 = 5l$ or $n = 5l + 1$ for some integer l.
Hence $5 \mid (n-1)$. ■

The problem is that we can't seem to find any straightforward way to bridge the gap here. At this point, it would be a good idea to try some examples for n and try to find situations in which the hypothesis of the proposition is true. (In fact, this should have been done before we started trying to prove the proposition.)

We quickly find that the claim is in fact not true! Indeed for $n = 4$, the number $n^2 - 1$ is divisible by 5, but $n - 1$ is not.

Definition 2.3.56

A **counterexample** for a statement of the form $(\forall x \in \mathscr{U})(\mathrm{P}(x))$ is an element a in the universal set for which $\mathrm{P}(a)$ is false.

Thus we have in fact proved that the negation of claim 55 is true, i.e. the original claim is false.

A Word of Caution. Finding a counterexample is not a 'proof'. Do not format it as if you are proving a claim; unless the question asks you to prove that the claim is false, in which case you are not really finding a counterexample!

2.3.5 Using Cases

Sometimes it is easier to prove something if we examine different scenarios separately. To do this, we split our proof up into multiple **cases**. Consider the following proposition.

Proposition 2.3.57

$n^2 + 7n + 6$ is even for all integers n.

First write it in P $\implies$ Q *form. The claim would be much easier to prove if we knew something else about n, like whether it was even or odd. So let's treat each case separately!*

Proof of proposition 57.

Let n be an integer.

Case 1.

Case 2.

These two cases show that if n is an integer, then $n^2 + 7n + 6$ is even. ■

Note: Using cases can be helpful because it allows us to assume extra information for writing the proof. Some important things to keep in mind.

- It is common (especially in this class) to choose cases based on sign or parity.
- We have to exhaust every possible case in our proof.

  For example, if you want to show something for every real number, it wouldn't be enough to just show it for $x < 0$ and $x > 0$. You would need a third case where $x = 0$.

- Logically, the proof technique can be justified using the following equivalencies

$$[(P \vee Q) \implies R] = [(P \implies R) \wedge (Q \implies R)]$$

Consider the following proposition.

Proposition 2.3.58

The sum of two integers with the same parity is even.

(a) Write this claim as a statement of the form "If P then Q".

(b) What two cases do you need to consider to prove this statement?

(c) Write a proof of the statement below.

Proof of proposition 58.

Case 1.

Case 2.

■

Using proof by cases can be very tempting, even when it isn't necessary. Often times we'll initially write a proof by cases because the added assumption we get to make helps us see things more clearly. Consider the following claim.

Proposition 2.3.59

If n is an integer, then $(2n+3)+(-1)^n(2n+1)$ is even.

We show two proofs of this claim. First, we show a proof by cases, then we show a direct proof.

Proof of proposition 59.

Proof By Cases.

First we consider the case where n is even. By definition, $n = 2a$ for some integer a. Then

$$\begin{aligned} 2n+3+(-1)^n(2n+1) &= 4a+3+(-1)^{2a}(4a+1) \\ &= 4a+3+4a+1 \\ &= 8a+4 \\ &= 2(4a+2). \end{aligned}$$

Hence, we see that $2n+3+(-1)^n(2n+1)$ is even.

Now we consider the case where n is odd. Then $n = 2b+1$ for some integer b. As in the last case, we plug-in $2b+1$ for n:

$$\begin{aligned} 2n+3+(-1)^n(2n+1) &= (4b+2)+3+(-1)^{2b+1}(4b+2+1) \\ &= 4b+5-(4b+3) \\ &= 2. \end{aligned}$$

Hence, we see again that $2n+3+(-1)^n(2n+1)$ is even. Because every integer is either even or odd, this completes the proof. ■

And now here is a direct proof of the same claim.

Proof of proposition 59.

Direct Proof

Suppose n is an integer. Let us consider the parity of the integers $2n+3$ and $2n+1$. We know that an even integer plus an odd integer is an odd integer. Hence, both $2n+3$ and $2n+1$ are odd integers.

Now $(-1)^n$ is equal to either 1 or -1. Regardless, $(-1)^n(2n+1)$ is still an odd integer. Then the expression $2n+3+(-1)^n(2n+1)$ is simply a sum of two odd integers, which we know results in an even integer. This proves the claim. ■

2.3.6 Treating Similar Cases

What two cases would you need to consider to prove the following proposition?

Proposition 2.3.60

If m and n are integers with opposite parity, then $m+n$ is odd.

The two cases in this proof are exactly alike, except for what we call m and n. In situations where there are multiple cases like this, we usually just do one, and indicate that the other cases are nearly identical by using **"Without loss of generality."**

That statement "Without loss of generality..." means that we are treating one of several nearly identical cases (sometimes, you'll see it written WLOG).

Proof of proposition 60.

Let m and n be integers with opposite parity. Without loss of generality, suppose m is even and n is odd.

■

Warning: Often, we will need to treat cases separately and using **"without loss of generality"** is not correct.

As you are learning to write proofs, you may want to just write out all of the cases until you have enough practice to identify situations where **"without loss of generality"** is appropriate.

2.3.7 Other Examples of Direct Proofs

Consider the following proposition:

Proposition 2.3.61

Suppose $a, b \in \mathbb{N}$. If $\gcd(a,b) > 1$, then $b|a$ or b is not prime.

This claim is of the form $P \implies (Q \vee R)$. We can prove a statement like this using two cases, as follows:

- **Case 1:** Q is true.
- **Case 2:** Q is not true.

Clearly, these claims exhaust all possibilities since Q is either true or not true. In the first case, we have nothing to prove because $P \implies Q$ is true. In the second case, we have to show that if P is true then R is true.

Note: Logically, the following are equivalent

$$[P \implies (Q \vee R)] = [Q \vee (\sim Q \wedge (P \implies R))] = [(P \wedge \sim Q) \implies R]$$

You can check this using a truth table.

■ **Question 71.** □

Prove proposition 61 using cases as described above.

Prove the following proposition by considering two cases.

Proposition 2.3.62

For all real numbers a and b, if $ab = 0$, then $a = 0$ or $b = 0$.

Try more exercises on using direct proof and proof by cases. Several of these questions are taken from the end of Chapter 4 in your textbook. The odd exercises all have proofs in the back of the text. You are more than welcome to look at those for any problems, but you should always try your hand at something first!

Question 72.

□

If $x > 0$, then prove that $x + \frac{1}{x} \geq 2$.

Question 73.

□

If a is an integer and $a^2 \mid a$, then prove that $a \in \{-1, 0, 1\}$.

2.3.8 Reading Proofs

Before we move on to the next section, let us take a moment to discuss reading and checking proofs. One aspect of writing proofs is learning to read and critique them. In later classes you will read and try to understand proofs of concepts with which you are not particularly familiar. Here, our goal is to learn to read proofs with an eye for critiquing them. This will help you to find problems with your own proofs!

Goals.

- Learn to read proofs using examples
- Read and interpret proofs written by others
- Find mistakes in proofs

Reading a mathematical proof is not like reading a passage in a novel or an article online. Reading a proof is an activity in which the reader must take an active role in the process. Fortunately, a well-written proof usually tells you exactly what you should be doing.

Question 74. □

Consider the following claim with the proof taken from the textbook. Answer the questions as you go.

Claim 2.3.63

If x is an even integer, then $x^2 - 6x + 5$ is odd.

Proof. Suppose x is an even integer.

1. Test an example. Do as the first sentence tells you to do. Choose an even integer value to assign to the variable x. Write your choice here and confirm that the claim is true for your choice.

Then $x = 2a$ for some $a \in \mathbb{Z}$, by definition of an even integer.

2. If this sentence is true, then you should be able to choose the value of a for your choice of x. Write that value here.

So

$$\begin{aligned} x^2 - 6x + 5 &= (2a)^2 - 6(2a) + 5 \\ &= 4a^2 - 12a + 5 \\ &= 4a^2 - 12a + 4 + 1 \\ &= 2(2a^2 - 6a + 2) + 1. \end{aligned}$$

Therefore we have $x^2 - 6x + 5 = 2b + 1$, where $b = 2a^2 - 6a + 2 \in \mathbb{Z}$ by closure.

3. This is probably overkill, but double check that b is in fact an integer for your a value. What do we mean by the phrase "by closure"?

Consequently $x^2 - 6x + 5$ is odd, by definition of an odd number. ■

Of course, examples aren't enough to prove general statements. However, reading along with a proof using examples not only helps us find potential mathematical errors, but it can also serve as a guide for clear proof *writing*. As you read your own proofs and the proofs of others this semester, if you find doing so is tedious, then there's a good chance the proof could use some rewriting.

Question 75.

□

Stop and give this one some thought on your own first. What strategies can we use? Then see the proof on the next page and see if it makes sense.

Proposition 2.3.64

Let $a, b, q, r \in \mathbb{Z}$ with $b > 0$ and $a = bq + r$. Then $\gcd(a, b) = \gcd(b, r)$.

This proposition is very similar in spirit to an example in the textbook involving least common multiples. Maybe start by setting $m = \gcd(a, b)$ and $n = \gcd(b, r)$. You want to show that $m \leq n$ and $n \leq m$.

Here is a proof of proposition 64.

Proof of proposition 64.

We are given that $a = bq + r$ where $a, b, q, r \in \mathbb{Z}$ and $b > 0$. Let $m = \gcd(a, b)$ and $n = \gcd(b, r)$. We want to show that $m = n$. One way to do this is to show that $m \leq n$ and $n \leq m$.

First we will show that $m \leq n$. By the definition of **greatest common divisor** (definition 45), we know that $m \mid a$ and $m \mid b$. This means, for some integers k and l, $a = mk$ and $b = ml$. If we substitute these expressions into the equation $a = bq + r$, we get:

$$\begin{aligned} & a && = bq + r \\ \implies & mk && = ml + r \\ \implies & mk - ml && = r \\ \implies & m(k - l) && = r. \end{aligned}$$

By definition of divides, we have that $m \mid r$. Hence, m is a common divisor of both b and r. Thus, we must have $m \leq n$ as $n = \gcd(b, r)$, the greatest common divisor of b and r.

In a similar fashion, we can show that $n \leq m$. Since $n = \gcd(b, r)$, we know that $n \mid b$ and $n \mid r$. Hence, there exist integers x and y such that $b = nx$ and $r = ny$. Substituting into $a = bq + r$ gives us:

$$\begin{aligned} & a = bq + r \\ \implies & a = (nx)q + ny \\ \implies & a = n(xq + y). \end{aligned}$$

Hence, $n \mid a$. Because $n \mid a$ and $n \mid b$, it follows from the definition of GCD that $n \leq m$. ■

Question 76. □

To help you in reading and understanding the above proof of proposition 64, here are some follow-up questions to try and answer.

(a) *Make up an example and follow the steps of the proof for your example. That is, pick integers a and b and find q and r so that $a = bq + r$. Then find $\gcd(a, b)$ and $\gcd(b, r)$ and follow along in the proof with these numbers. Does the proof make sense with these numbers plugged in?*

(b) *What previous definitions from Section 4.2 did we need to utilize here?*

(c) *Why does $m \leq n$ and $n \leq m$ give us that $m = n$?*

(d) *Does it matter that $b > 0$? Why is this part of the hypothesis?*

2.3.9 Evaluating Proofs

One of the ways to figure out whether a proof is correct or not, is to start with the proof and see if you can figure out what is the original proposition! Here's an example:

Proof of some claim. Assume that n is an odd integer. Then $n = 2k+1$ for some integer k. Then

$$3n - 5 = 3(2k+1) - 5 = 6k + 3 - 5 = 6k - 2 = 2(3k-1)$$

Since $3k-1$ is an integer, $3n-5$ is even. ■

Question 77. □

Give two different claims that are being proved by above argument.

Question 78. □

Read the claim and the proposed proofs below and determine whether, in your opinion, it is, in fact, a proof. If you don't believe that the given argument provides a proof of the result, then you should point out the mistake(s). Refer to appendix C to point out the specific issues.

Claim 2.3.65

If x and y are integers of the same parity, then $x-y$ is even.

Proof of claim 65.

Let x and y be two integers of the same parity. We consider two cases, according to whether x and y are both even or are both odd.

Case 1. x and y are both even. Let $x = 6$ and $y = 2$, which are both even. Then $x - y = 4$, which is even.

Case 2. x and y are both odd. Let $x = 7$ and $y = 1$, which are both odd. Then $x - y = 6$, which is even. ■

Question 79. □

Same as above.

Claim 2.3.66

If m is an even integer and n is an odd integer, then $3m+5n$ is odd.

Proof of claim 66.

Let m be an even integer and n an odd integer. Then $m = 2k$ and $n = 2k+1$, for some $k \in \mathbb{Z}$. Therefore,

$$3m + 5n = 3(2k) + 5(2k+1) = 6k + 10k + 5 = 16k + 5 = 2(8k+2) + 1.$$

Since $8k+2$ is an integer, $3m+5n$ is odd. ■

Question 80.

The following proofs come from assignments of previous students. Each proof contains at least one error and most contain several. However, none of these proofs is totally wrong. They just need some adjusting. For each proof, find any errors that you can and suggest a correction.

Claim 2.3.67

Suppose $a, b, c, d \in \mathbb{Z}$. If $a \mid b$ and $c \mid d$, then $ac \mid bd$.

Proof of claim 67.

Suppose $a, b, c, d \in \mathbb{Z}$ so that $a \mid b$ and $c \mid d$. For a to divide b, we need an integer k so that $ak = b$. For c to divide d, we need an integer l so that $cl = d$. We can multiple each of these sides to give us $bd = akcl$ which can be rewritten as $bd = (ac)(kl)$. We can make kl some integer m giving us $bd = (ac)(m)$. Showing that ac divides bd. Therefore, if $a \mid b$ and $c \mid d$, then $ac \mid bd$. ■

Proof of claim 67.

By definition, a divides b if $ak = b$ for $k \in \mathbb{Z}$. That applies to c dividing d, so we have $cl = d$. Therefore, $bd = (ak)(cl)$ or $bd = (ac)(kl)$ which shows that ac is a multiple of bd. ■

Question 81.

Same as above.

Claim 2.3.68

Suppose $x, y \in \mathbb{R}$. If $x < y$, then $x < \frac{x+y}{2} < y$.

Proof of claim 68.

Suppose $x, y \in \mathbb{R}$, then $x < \frac{x+y}{2}$ where $x = \frac{2x}{x} = \frac{x+x}{2}$. By substituting, $\frac{x+x}{2} < \frac{x+y}{2}$ is equivalent to $\frac{2x}{2} < \frac{x+y}{2}$ in which, $x < \frac{x+y}{2}$. If $\frac{x+y}{2} < y$ and $y = \frac{2y}{2} = \frac{y+y}{2}$, then $\frac{x+y}{2} < \frac{y+y}{2}$. After multiplying both sides by 2 we get $x + y < y + y$. Then, by subtracting y we can see that $x < y$. Therefore, $x < \frac{x+y}{2} < y$. ■

Proof of claim 68.

Let $x, y \in \mathbb{R}$ and suppose $x < y$. Multiplying each side by 2, $x < y = 2x < 2y$ and subtracting an x and y from both sides we have $-x - y < -y - x$. Adding $2x$ to the left side, and $2y$ to the right side of the inequality, $2x - x - y < 2y - y - x$ which can be rewritten as $2x < x + y < 2y$. Dividing each expression by 2 we see that when $x < y$ then $x < \frac{x+y}{2} < y$. ■

§2.4 Proof by Contrapositive

Proof by contrapositive is a very powerful proof technique. Any statement that can be proven with a direct proof can be proven with a contrapositive proof and vice versa. However, often one of these proofs will be significantly easier to write. Since $P \implies Q$ is equivalent to $(\sim Q) \implies (\sim P)$, in a proof by contrapositive we give a proof of $(\sim Q) \implies (\sim P)$ and then conclude that $P \implies Q$.

Proposition: If P, then Q.

Proof.

Assume $\sim Q$.

$\vdots$

Therefore, $\sim P$.

Thus, $\sim Q \implies \sim P$.

Therefore, $P \implies Q$.

■

Let the reader know it's a contrapositive proof. Keep in mind that our proof reader is either someone who is skeptical of our claim or someone who doesn't fully understand our claim. If we decide to write a contrapositive proof rather than a direct proof, then our reader could quickly become very confused. For that reason, we always inform the reader at the start of the proof that we are writing a proof by contrapositive.

For this reason, we will always start a proof by contrapositive as follows:

"Contrary to what we have to prove, suppose $\sim Q$."

or

"We proceed via a proof by contrapositive. So let's assume $\sim Q$.

Example 2.4.69

Consider the claim "Let n be an integer. If n^2 is even, then n is even."

P : $\sim P$:

Q : $\sim Q$:

Rewrite the given statement as $P \implies Q$ and write down the contrapositive of the statement:

Contrapositive:

Now let's complete the proof of the claim above using contrapositive proof.

Proof of example 69.

We proceed using a proof by contrapositive, so suppose n is not even.

■

Question 82.

□

Prove the following proposition.

Proposition 2.4.70

Suppose x and y are integers. If $x^2(y+3)$ is even, then x is even or y is odd.

(a) In the claim above, what are the statements P and Q?

P :

Q :

(b) What are the statements $\sim$ P and $\sim$ Q?

$\sim$ P :

$\sim$ Q :

(c) Write the contrapositive of the statement.

(d) Prove the claim using proof by contrapositive.

Proof of proposition 70.

■

Question 83.

□

Prove the following claim using proof by contrapositive.

Claim 2.4.71

Suppose $x, y, z \in \mathbb{Z}$ and $x \neq 0$. If $x \nmid yz$, then $x \nmid y$ and $x \nmid z$.

Question 84.

□

Prove the following claim using proof by contrapositive.

Claim 2.4.72

Suppose that x and y are real numbers such that $x < 2y$. Prove that if $7xy \leq 3x^2 + 2y^2$, then $3x \leq y$.

§2.5 Congruence of Integers

The mathematical relation **congruence** appears frequently in advanced mathematics, especially if you take a course like Abstract Algebra.

First, recall the very fundamental theorem regarding division of integers (theorem 48):

Theorem 2.5.73: The Division Algorithm

For all integers a and b, with $b > 0$, there exist unique integers q and r such that $a = bq + r$ and $0 \leq r < b$.

Question 85.

Use the division algorithm for $b = 17$ and $a = 5$.

□

Definition 2.5.74

Let n be a fixed positive integer. For $x, y \in \mathbb{Z}$, we say x is **congruent to** y **modulo** n if and only if $n \mid (x - y)$. We usually write this as $x \equiv_n y$ or $x \equiv y \pmod{n}$.

If x and y are not congruent modulo n, we write this as $x \not\equiv y \pmod{n}$. The number n is called the **modulus** of the congruence.

Example 2.5.75

What is the truth set of the following open sentence P(y)?

$$4 \equiv y \pmod{3}$$

Question 86.

□

Below, you are given expressions of the form $x \equiv y \pmod{n}$, where x has been provided and y is left blank. Determine a value of y (not equal to x that makes the expression true. Note that there is more than one (in fact, infinitely many) answer for all of these.

$72 \equiv$ (mod 67); $6 \equiv$ (mod 2)

$-6 \equiv$ (mod 8); $-2 \equiv$ (mod 3)

Question 87.

If $a = bq + r$, fill in the blanks below appropriately with a, b, and r.

$$\_\_\_\_\_ \equiv \_\_\_\_\_ \pmod{\_\_\_\_\_}$$

Question 88.

Prove the following theorem.

Theorem 2.5.76

Let $a, b, c \in \mathbb{Z}$ and $n \in \mathbb{N}$. If $a \equiv b \pmod{n}$ and $a \equiv c \pmod{n}$, then $b \equiv c \pmod{n}$.

Question 89.

Prove or provide a counterexample to the following claim.

Claim 2.5.77

If $a, b \in \mathbb{Z}$, then $(a+b)^3 \equiv a^3 + b^3 \pmod 3$.

Question 90.

Consider the following theorem.

Theorem 2.5.78

Let $a, b \in \mathbb{Z}$ and $n \in \mathbb{N}$. If $a \equiv b \pmod n$, then $a^2 \equiv b^2 \pmod n$.

Your textbook contains a proof of Theorem 78 on pg. 132 (it might be helpful to read through that proof). Is the converse of Theorem 78 true? If it is, give a proof, if not, find a counterexample.

§2.6 Proving Statements with Contradiction

The logic behind **proof by contradiction** is as follows. To prove that the statement P is true, we first temporarily assume P is false and then see what happens in that hypothetical scenario. If what happens is mathematically impossible, i.e. it results in a contradiction, then we know P must not have been true to start with!

This method uses the equivalence between P and $((\sim \mathrm{P}) \implies (\mathrm{C} \wedge \sim \mathrm{C}))$.

Proposition: P.

Proof. Suppose $\sim$ P.
⋮
Therefore, C.
⋮
Therefore, $\sim$ C.
Hence, C$\wedge \sim$ C, a contradiction.
Thus, P. ■

We need to recall the following definition before our first example.

Definition 2.6.79

A real number x is **rational** if $x = \frac{a}{b}$ for some $a, b \in \mathbb{Z}$ with $b \neq 0$. A real number is called **irrational** if it is not rational.

One of the oldest examples of proof by contradiction comes from the Pythagoreans. The ancient Greeks had a mathematical philosophy that all numbers were rational numbers. The (likely apocryphal) story is that they murdered the person who first discovered that $\sqrt{2}$ is **irrational**.

Claim 2.6.80

$\sqrt{2}$ is irrational.

Proof of claim 80.

We will use proof by contradiction. Assume that $\sqrt{2}$ is rational, and so there exists $a, b \in \mathbb{Z}$ with $b \neq 0$, such that

$$\sqrt{2} = \frac{a}{b}.$$

In particular, we may choose a and b so that this fraction is in lowest terms (a and b have no common factors).

Squaring both sides and multiplying through by b^2, we get

$$2b^2 = a^2,$$

by which it follows that a^2 is even. We have already proven that if a^2 is even, then a must be even. Because a is even, we may write $a = 2c$ for some $c \in \mathbb{Z}$ and thus, $a^2 = 4c^2$. Therefore,

$$2b^2 = 4c^2 \implies b^2 = 2c^2.$$

Therefore, b^2 is even, and so again, b is even.

But, since a is even if b is even then they share a common factor of 2 and $\frac{a}{b}$ is not be in lowest terms. Therefore, b can not be even. Thus, we have the contradiction: b is even and b is not even. Therefore, it must be the case that $\sqrt{2}$ is in fact irrational, which completes our proof. ■

Note:

- Proofs by contradiction are often helpful to prove 'there does not exist...' statements, because you get to assume something **does** exist.
- It is not always clear what exactly your contradiction C$\wedge \sim$ C will be when you start, so you might have to do a lot of scratch work first to discover one.

Question 91. □

Prove by contradiction that there do not exist integers a and b such that $21a + 30b = 1$.

Another classic theorem that can be proven via contradiction is due to the ancient Greek mathematician Euclid. There is a proof of this theorem in the textbook. Read it carefully. Below we will consider an alternate way of writing the same proof using modular arithmetic notations.

Theorem 2.6.81

There are infinitely many prime numbers.

Proof of theorem 81.

For the sake of contradiction, suppose there are only finitely many prime numbers. Then we can list all the prime numbers as $p_1, p_2, p_3, \dots p_n$, where $p_1 = 2, p_2 = 3, p_3 = 5, p_4 = 7$ and so on. Thus p_n is the n th and largest prime number. Now consider the number

$$a = (p_1 p_2 p_3 \cdots p_n) + 1,$$

that is, a is the product of all prime numbers, plus 1. Now a, like any natural number greater than 1 , has at least one prime divisor, and that means $p_k \mid a$ for at least one of our n prime numbers p_k. Then,

$$a \equiv 0 \pmod{p_k} \implies 1 \equiv 0 \pmod{p_k}$$

In other words $p_k \mid 1$, which is clearly false. So our initial assumption must have been false, i.e. there must be infinitely many prime numbers. ■

Question 92.

□

There are a few subtleties in this proof (and the textbook proof) that are worth discussing.

(a) The proof claims that there must be a prime p_k that divides a. How do we know that this is true?

(b) Will the proof still work if we define a to be $a = (p_1 p_2 \dots p_n) + 3$? Explain. If you say no, exactly which step is no longer valid?

(c) Notice that $2 \cdot 3 + 1 = 7$ is prime, $2 \cdot 3 \cdot 5 + 1 = 31$ is prime, and $2 \cdot 3 \cdot 5 \cdot 7 + 1 = 211$. Do you think this process of multiplying consecutive primes together and then adding 1 will always generate a prime number?

2.6.1 Proof of $(\forall x)P(x)$ by Contradiction

Proposition: $(\forall x)P(x)$.

Proof. Suppose $\sim (\forall x)P(x)$.
Then $(\exists x)(\sim P(x))$.
Let t be an object such that $\sim P(t)$.
$\vdots$
Therefore $Q \wedge \sim Q$.
Thus $(\exists x)(\sim P(x))$ is false, so $(\forall x)P(x)$ is true. ■

Question 93. □

Prove that for every integer n, $4 \nmid (n^2+2)$.

Question 94. □

Prove that for every real number x with $\frac{\pi}{2} \leq x \leq \pi$, we have $\sin x - \cos x \geq 1$.

2.6.2 Proving Conditional Statements by Contradiction

To prove a conditional statement $P \implies Q$ via contradiction we start by assuming $\sim(P \implies Q)$, which is equivalent to $P \wedge \sim Q$. We then proceed logically until we reach a contradiction. This uses the logical equivalence between $P \implies Q$ and $(P \wedge (\sim Q)) \implies (C \wedge \sim C)$.

Proposition: $P \implies Q$.

Proof.

Suppose $\sim(P \implies Q)$.
Thus $P \wedge \sim Q$.
$\vdots$
Therefore, C.
$\vdots$
Therefore, $\sim C$.
Hence, $C \wedge \sim C$, a contradiction.
Thus, $P \implies Q$.

■

Prove the following claims using contradiction.

■ **Question 95.** □

If $a, b \in \mathbb{Z}$, then $a^2 - 4b - 3 \neq 0$.

Question 96.

Suppose $a, b \in \mathbb{R}$. If a is rational and ab is irrational, then b is irrational.

□

Exploration Activity

You should take some time to read through **§6.4: Some words of Advice** from the textbook. Essentially, the advice the book gives, (which I think most mathematicians would agree with), is to only use proof by contradiction when you have to. That is, when you can not see how to prove a theorem using direct proof or proof by contrapositive.

One reason not to use proof by contradiction is that it is usually not **constructive**. Consider your proof of the claim **"Every odd integer is a difference of two squares"**. The proof is **constructive**, because you not only show that the claim is true, but you also show exactly how to write every odd integer as a difference of squares. This is much better than assuming that the claim isn't true and then just showing that something would have to go wrong.

§2.7 Proving Bi-conditional Statements

2.7.1 If-and-Only-If Proof

Proofs of biconditional sentences $P \iff Q$ depend on the use of the equivalence of

$$(P \iff Q) \text{ and } (P \implies Q) \wedge (Q \implies P).$$

We present this here as a new method, but it's really just combining two proofs of the kind you've already been doing into one.

Proposition: $P \iff Q$.

Proof. We prove $P \iff Q$ by proving two implications.

- (Forward Implication) Assume P, then show $P \implies Q$ (using some proof method).
- (Backward Implication) Assume Q, then show $Q \implies P$ (using some proof method).

Therefore, $P \iff Q$. ■

Note: Notice that $P \implies Q$ and $Q \implies P$ in a biconditional proof might use different proof techniques. For example, it is very common that $P \implies Q$ requires direct proof, but $Q \implies P$ requires a contradiction or contrapositive proof.

■ **Question 97.** □

Suppose a and b are positive integers. Prove that $a+1$ divides b and b divides $b+3$ if and only if $a = 2$ and $b = 3$.

Question 98.

Let $a, b \in \mathbb{Z}$. Then prove that $3 \mid (5a + 8b)$ if and only if $3 \mid (a + b)$.

In some cases it is possible to prove a biconditional sentence P $\iff$ Q that uses the 'iff' connective throughout the proof. Start with P and replace it with a sequence of equivalent statements, the last one being Q.

Proof.

$$\begin{aligned} &\text{P iff } R_1 \\ &\text{iff } R_2 \\ &\vdots \\ &\text{iff } R_n \\ &\text{iff Q.} \end{aligned}$$

■

Question 99.

Suppose $a, b \in \mathbb{Z}$. Prove that $a \equiv b \pmod{10}$ if and only if $a \equiv b \pmod{2}$ and $a \equiv b \pmod{5}$.

2.7.2 Equivalent Statements

If the statement "P if and only if Q" holds, then we refer to P and Q as **equivalent statements**. Many very important theorems in mathematics show that several statements are equivalent. As an example, consider the following claim. We have already shown that a few of these are equivalent.

Claim 2.7.82

Let n be an integer. Then the following statements are equivalent.

(a) n *is even.*

(b) n^2 *is even.*

(c) There exists an odd integer m such that $n = m - 5$.

(d) n^2 *is divisible by 4.*

Since these statement are all equivalent, any one of them implies **all** of the others. The diagram in Figure 2.1 shows the relationships between the statements.

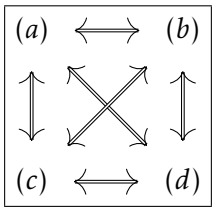
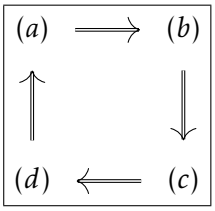


Figure 2.1: All equivalences in claim 82

If we want to prove such a claim, we need to establish all twelve implications in the diagram above (i.e., $a \implies b, b \implies a, a \implies c, c \implies a$, etc.). However, suppose that we just establish the implications in the diagram below.



■ **Question 100.** □

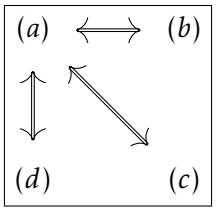
If we prove all of the implications in this diagram, have we shown $(a) \iff (c)$?

Exploration Activity

If you are taking or have taken Linear Algebra, you have probably seen a lot of equivalent statements. For example, check out this version of the ‘‘Invertible Matrix Theorem" which lists 23 statements equivalent to a matrix being invertible!!

mathworld.wolfram.com/InvertibleMatrixTheorem.html

There are many different ways to prove statements are equivalent. For example, if you found it particularly difficult to prove $(b) \implies (c)$, you might instead show all of the following:



§2.8 Existence and Uniqueness Proofs

Last chapter, we proved statements of the form $(\forall x)\mathrm{P}(x)$. Now we will see how to prove a statement of the form $(\exists x)\mathrm{P}(x)$. The strategy is very straightforward, just give an example of the thing that's supposed to exist! Of course, our proof should also include an explanation of why our example fits the requirements of the claim. Below is a general outline for this method.

2.8.1 Direct Proof of $(\exists x)\mathrm{P}(x)$

Proposition: $(\exists x)\mathrm{P}(x)$.

Proof.
⋮
Therefore there must exist an object a such that $\mathrm{P}(a)$ is true.
Therefore, $(\exists x)\mathrm{P}(x)$ is true. ■

Now prove the following two claims using the method above. Make sure to explain why your example actually works.

■ **Question 101.** □

Prove that there exists a positive real number x for which $x^2 < \sqrt{x}$.

We can also prove an existence statement via contradiction.

2.8.2 Proof of $(\exists x)\mathrm{P}(x)$ by Contradiction

Proposition: $(\exists x)\mathrm{P}(x)$.

Proof. Suppose $\sim(\exists x)\mathrm{P}(x)$.
Then $(\forall x)(\sim \mathrm{P}(x))$.
⋮
Therefore, $\sim \mathrm{Q} \wedge \mathrm{Q}$, a contradiction.
Thus $\sim(\exists x)\mathrm{P}(x)$ is false.
Therefore $(\exists x)\mathrm{P}(x)$ is true. ■

Question 102.

□

There are n students present in a classroom. Assume that if student A is friends with student B, then student B is friends with student A. Prove that there exists (at least) a pair of students who have the same number of friends in the room.

Note:

First of all, note that the problem does not ask you find which two students have same no. of acquaintances. It doesn't ask you to find the actual number of acquaintances either. It only asks you show that such two people can be found if we wanted to. It is also entirely possible that the two students have different sets of friends.

Exploration Activity

The proof technique we used above has a name, it's called the Pigeonhole Principle or PHP for short. Here's the more general version of the statement.

The Pigeonhole Principle: If $(nk+1)$ pigeons are put into n pigeon-holes, then at least one hole has more than k pigeons.

In our Proof of above question, notice that we did not actually determine which pair of people had the same number of friends. As we discussed earlier when doing proof by contradiction, this type of proof is a **non-constructive** proof. This is different from the proofs of questions in the last page, where you actually provided an example to prove the claim. As you might have guessed, these types of proofs are called **constructive** proofs.

Again, both constructive and non-constructive proofs are generally acceptable, though constructive proofs are often preferred when possible. You can read more about these two types of proofs in Section 7.4 of your textbook.

Question 103.

□

If a, b, and c are real numbers with $a \neq 0$, then prove that the linear equation $ax + b = c$ has a real solution.

Question 104.

□

Prove that the equation $x^5 + 2x - 5 = 0$ has a real number solution between $x = 1$ and $x = 2$.

Proposition 7.1 on page 152 of your textbook is very important, and actually has a special name:

Proposition 2.8.83: Bézout's Identity

If $a, b \in \mathbb{N}$, then there exist integers j and k for which $\gcd(a,b) = aj + bk$.

You will notice that the proof is **non-constructive**.

Question 105.

*What **axiom** of $\mathbb{N}$ does the proof of Bézout's Identity use to show existence?*

□

Use Bézout's Identity to prove the next two questions.

Question 106.

Prove: If $a \mid bc$ and $\gcd(a,b) = 1$, then $a \mid c$.

□

Question 107.

Euclid's Lemma

Suppose $a, b, p \in \mathbb{Z}$ and p is a prime. Prove that if $p \mid ab$, then $p \mid a$ or $p \mid b$.

This problem is in your homework assignment.

2.8.3 Uniqueness

Many important theorems in mathematics state the existence of some object, and then state that said object is **unique**.

Note: When we want to say that an object x exists **and is unique** using logic symbols, we use the notation $\exists!x$. The existential symbol tells us the object x exists, and the exclamation point is used to denote uniqueness.

Here is a proof scheme for proving existence plus uniqueness.

Proposition: $(\exists!x)\mathrm{P}(x)$.

Proof.

(i) [Prove that $(\exists x)\mathrm{P}(x)$ is true. Use any method here.]

(ii) [Prove that $(\forall y)(\forall z)[(\mathrm{P}(y) \wedge \mathrm{P}(z)) \implies (y = z)]$.]

Assume that y and z are objects in the universe such that $\mathrm{P}(y)$ and $\mathrm{P}(z)$ are true.
⋮
Therefore, $y = z$.

From (i) and (ii) conclude that $(\exists!x)\mathrm{P}(x)$ is true. ■

We will prove a stronger version of **The Divison Algorithm** (theorem 48) below to showcase an existence and uniqueness proof.

Theorem 2.8.84: The Divison Algorithm

Given integers a and b with $b \neq 0$, there exist unique integers q and r for which $a = bq + r$ and $0 \leq r < |b|$.

The existence part of the proof depends on the Well-Ordering Principle of Natural numbers. We will state it here but will not prove it. The statement below might seem "obvious", and it might seem like an axiom to you. I will not elaborate on this issue right now, but you are welcome to read appendix D after you finish this chapter for an interesting discussion on this topic!

Theorem 2.8.85: Well-Ordering Principle of Natural numbers

Any non-empty set of natural numbers contains a smallest element.

■ **Question 108.** □

*Here's a way to prove the **existence** part of the Division Algorithm. Consider the set*

$$\mathrm{S} = \{x : (\exists q \in \mathbb{Z})(x = a - bq), x \geq 0)\}$$

(a) Why is $\mathrm{S} \subseteq \mathbb{N}$?

(b) How do you know that S is non-empty?

(c) *Theorem 85 proves that* S *has a smallest element, call it* r. *Prove that* $r < |b|$.[iv]

Question 109.

Prove the ***uniqueness*** *part of the Division Algorithm.*

To help you in setting this up: start by assuming that, for the integers a and b, you have integers q_1, q_2, r_1, and r_2 satisfying

$$a = bq_1 + r_1 \quad \text{and} \quad 0 \leq r_1 < |b|$$

and

$$a = bq_2 + r_2 \quad \text{and} \quad 0 \leq r_2 < |b|.$$

Your goal is to show that $q_1 = q_2$ and $r_1 = r_2$.

[iv] HINT: if $r \geq |b|$, consider the number $s = r - |b|$. Check that $s < r$ and $s \in$ S. What's the issue here?

Question 110.

□

Prove that the equation $x^5 + 2x - 5 = 0$ *has a* ***unique*** *real number solution between* $x = 1$ *and* $x = 2$.

Question 111.

□

For an irrational number r*, let*

$$S = \{sr + t \mid s, t \in \mathbb{Q}\}.$$

Prove that for every $x \in S$*, there exist unique rational numbers* a *and* b *such that* $x = ar + b$.

§2.9 The Principle of Mathematical Induction

Many statements in mathematics are true **for all natural number**. For example.

- **Fundamental Theorem of Arithmetic:** Every natural number has a unique prime decomposition.
- **Parity of Natural Numbers:** Every natural number is either even or odd.
- **Power Rule for Differentiation:** For any natural number n, we have $\frac{\mathrm{d}}{\mathrm{d}x}[x^n] = nx^{n-1}$.

Each of the above can be thought of as an open sentence $\mathrm{S}(n)$ whose truth value depends on n. So a proof of the claim would be to show that the truth set of $\mathrm{S}(n)$ is all natural numbers. In such scenarios, where we are required to show $(\forall n \in \mathbb{N})\mathrm{S}(n)$, where each $\mathrm{S}(n)$ is a statement depending on n, we can use a proof technique called Proof by Induction.

Here's another type of example. Suppose we need to show $f(n) = g(n)$ for all natural numbers n. Here f and g are some functions of n. In such a situation, $\mathrm{S}(n)$ is the open sentence that $f(n) = g(n)$. So a proof by induction can be used.

We're going to consider the universe for everything to be $\mathbb{N}$ until the end of this ection. The formal statement of the induction principle is as follows:

Theorem 2.9.86: Principle of Mathematical Induction

For each natural number $n \geq 1$, let $\mathrm{S}(n)$ be a mathematical statement. If

(a) $\mathrm{S}(1)$ *is true, and*

(b) the implication

$$\text{if } \mathrm{S}(k) \text{ for some natural number } k, \text{ then } \mathrm{S}(k+1)$$

is true,

then $\mathrm{S}(n)$ is true for all natural number $n \geq 1$.

Note: The Principle of Mathematical Induction is in fact an axiom! In 1889, an Italian mathematician named Giuseppe Peano put together a list of *axioms* that rigorously defined the set of natural numbers based on the notion of successors. We will talk about this in more details in **??**. The fifth defining axiom of the set $\mathbb{N}$ can be roughly stated as:

> *"If a property is possessed by 1 and possessed by the successor of every natural number that possesses it, then the property is possessed by all natural numbers."*

This is essentially the Induction principle in a different form. The key takeaway for now is that the PMI depends on the idea and uniqueness of the 'successor' function and doesn't work for sets that do not have a notion of successor.

2.9.1 Proof by Induction

The utility of induction principle is that it allows us to prove that an infinite number of statements are true by only showing two steps. We outline this in the proof method below.

Proposition: $(\forall n \in \mathbb{N})S(n)$

Proof.

(a) Base step: Verify that $S(1)$ 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.]

(b) Induction Step:

[Your goal is to prove "For all $k \in \mathbb{N}$, if $S(k)$ is true, then $S(k+1)$ is true."]

Let $k \in \mathbb{N}$ and assume that $S(k)$ is true.

$\vdots$ [Do something to derive that $S(k+1)$ is true.]

Therefore, $S(k+1)$ is true.

Therefore, by the principle of mathematical induction, $S(n)$ is true for all $n \in \mathbb{N}$. ■

Note:

- When proving (b), you can alternately use a proof by contradiction or contrapositive.
- The step where you assume that $S(k)$ is true is called the **induction hypothesis** or **induction assumption**. Using the assumption, we prove that then $S(k+1)$ must be true, this is the **Induction Step**.
- When proving step (b), you will **always** utilize the inductive hypothesis in some way in your proof. If you write a proof by induction and do not use the induction hypothesis, then either your proof was wrong, or you didn't actually need induction to begin with.

You should see a great first example in the textbook on page 182 where it is shown that the sum of consecutive odd integers forms a perfect square.[v] Problems like these, involving sums, are good first examples to try out Induction on. We will work out an example here by proving claim 87.

Claim 2.9.87

The sum of the first n natural numbers is equal to $\frac{n(n+1)}{2}$. *That is,*

$$1 + 2 + 3 + \ldots + (n-1) + n = \frac{n(n+1)}{2}.$$

Proof of claim 87.

We will prove the identity by inducting on n.

Base Case: When $n = 1$, the left hand side is 1 and the right hand side is $\frac{n(n+1)}{2} = \frac{1(1+1)}{2} = 1$. Hence the identity is true for $n = 1$.

Induction Hypothesis: Assume that the identity is true for some natural number k.

[v] That is, $1 + 3 + 5 + \cdots + (2n-1) = n^2$ for all $n \geq 1$.

Induction Step: By our induction hypothesis we have,

$$1+2+3+\ldots+k=\frac{k(k+1)}{2}$$

Adding $(k+1)$ to both sides we get,

$$\begin{aligned}1+2+3+\ldots+k+(k+1) &= \frac{k(k+1)}{2}+(k+1)\\ &= (k+1)\left(\frac{k}{2}+1\right)\\ &= \frac{(k+1)(k+2)}{2}\\ &= \frac{(k+1)((k+1)+1)}{2}\end{aligned}$$

Thus the identity holds when $n=k+1$.

Hence by PMI, the identity is true for all natural number n. ■

■ Question 112. □

Prove that for every natural number n,

$$1^2+2^2+3^2+4^2+\cdots+n^2=\frac{n(n+1)(2n+1)}{6}.$$

We can also prove statements involving divisibility using Induction.

Question 113.

Prove that, for all $n \in \mathbb{N}$, 6 *divides* $n^3 - n$.

□

Question 114.

Prove that $3 \mid (5^{2n} - 1)$ *for every integer* $n \geq 0$.

□

We know that we can add equal quantities to both sides of an equation without violating equality, but we can also add *unequal* quantities to both sides of an inequality, as long as the quantity you add to the bigger side is bigger than the quantity that you add to the smaller side.

For example, if $x \leq y$ and $a \leq b$, then $x + a \leq y + b$. Similarly, if $x \leq y$ and b is positive, then $x < y + b$.

Question 115.

□

Prove: For each $n \in \mathbb{N}$,

$$n + 3 < 5n^2.$$

Note: From your textbook (page 183): In induction proofs it is usually the case that the first statement S(1) is indexed by the natural number 1, but this need not always be so. Depending on the problem, we could have our statements begin at S(50) for example. The point is, the base case does not have to be "$n = 1$," but there must always be some **starting point** for induction.

Question 116.

□

Prove: $n^2 - n - 20 > 0$ *for all natural numbers* $n > 5$.

Sometimes it isn't very clear what exactly the induction variable is.

Question 117.

Archimedean Property of $\mathbb{N}$

Prove: For all natural numbers a and b, there exists a natural number s such that $sb > a$.

Question 118.

□

Prove: Every finite set of real numbers has a least element.

Here are some unusual places induction proofs can show up.

Question 119.

Prove that for $n \geq 4$, the number of diagonals in a (non-degenerate convex) n-gon is $\frac{n(n-3)}{2}$.

□

Question 120.

Prove or disprove: $n^2 + n + 41$ is prime for all natural numbers n.

□

Warning: One of the most common mistake in trying a proof via Induction is to fail to utilize the inductive hypothesis. Often, people assume what they are trying to prove is true, when it might not be the case. Another more sinister error can arise when induction cannot even be applied, and this involves examining more closely the base case.

Question 121.

Consider the following "proof" of the false statement that for all natural numbers n, we have $7 \mid 10^n$. Can you find the fallacy?

"Proof". We will use induction, so assume that the statement is true for some $k \in \mathbb{N}$. Then by definition, there exists an $x \in \mathbb{Z}$ such that

$$7x = 10^k.$$

Therefore, multiplying both sides by 10, we have $7x(10) = 7(10x) = (10^k)(10) = 10^{k+1}$. Thus, $7 \mid 10^{k+1}$, and so by mathematical induction, the statement is true for all $n \in \mathbb{N}$. ■

Question 122.

Consider the following "proof" of the false claim. Explain what is wrong with it!

Claim 2.9.88

All real numbers are equal.

"Proof". To prove the claim, we will prove by induction that the following statement holds:

For every set of n real numbers $S = \{a_1, a_2, a_3, \ldots, a_n\}$, we have $a_1 = a_2 = a_3 = \ldots = a_n$.

Base step: When $n = 1$, we have a set of 1 element which is definitely equal to itself. Hence the base case is trivially true.

Induction Hypothesis: Suppose above statement is true for some $k \in \mathbb{N}$.

Induction Step: By induction assumption, any set of k real numbers are equal to each other. Now start with a set of $(k+1)$ real numbers $a_1, a_2, \ldots, a_{k+1}$. Applying the Induction hypothesis to the first k numbers we get

$$a_1 = a_2 = \cdots = a_k$$

Next, applying the Induction hypothesis to the last k numbers we get

$$a_2 = a_3 = \cdots = a_{k+1}$$

Combining above two, we get that

$$a_1 = a_2 = a_3 = \cdots = a_k = a_{k+1}$$

Thus we have show that the statement holds for $n = k+1$ and the induction step is complete.

Hence by the Induction Principle, all real numbers are equal. ■

Exploration Activity

See this StackExchange link for more fake induction proofs.

2.9.2 Proof by Strong Induction

There are some questions where the inductive step $S(k) \implies S(k+1)$ is difficult to prove. Try a proof of the **Fundamental Theorem of Arithmetic**, which we previously called the **Unique Prime Factorization** theorem. We will ignore the 'unique' part for the moment.

Claim 2.9.89

Let n be a natural number. If $n > 1$, then either n is prime or n can be written as a product of prime numbers.

■ **Question 123.** □

Where do we run into trouble in our inductive step? What is the issue?

Be sure to read the proof of the **Fundamental Theorem of Arithmetic** on page 192 of your textbook. The above issue is resolved by using an alternative method of induction called **Strong Induction**.

Theorem 2.9.90: Principle of Strong Mathematical Induction

Suppose $S(n)$ is a mathematical statement for each natural number $n \geq m$. Suppose that

(a) *$S(m)$ is true, and*

(b) *the implication*

$$\text{If } S(i) \text{ for every integer } i \text{ with } m \leq i \leq k, \text{ then } S(k+1).$$

is true for every integer $k \geq m$,

Then $S(n)$ is true for all $n \geq m$.

Notice here how the second part of this Strong Induction Theorem is phrased compared to theorem 86 (which we can just refer to as regular induction). Instead of having the statement $S(k+1)$ follow from just one statement $S(k)$, Strong Induction requires all of the assumptions $S(1), S(2), \ldots, S(k)$ to imply the statement $S(k+1)$. Hence, Strong Induction is used when just one base case is not enough.

Note: In other words, the **Induction Hypothesis** for a strong induction proof assumes $(S_1 \wedge S_2 \wedge \cdots \wedge S_k)$ is true. The **induction step** is to show that S_{k+1} is true when the induction hypothesis holds.

Be sure to read the examples in the text as there is one example very much like the next exercise.

■ **Question 124.** □

Show that any amount of postage of at least 12 cents can be formed using just 4-cent and 5-cent stamps.

A more mathematical way to state the question statement would be.

Proposition 2.9.91

For any $n \in \mathbb{N}$ with $n > 12$, there exists $x, y \in \mathbb{N} \cup \{0\}$, such that $4x + 5y = n$.

Question 125.

Recall from Homework 1, the Chicken Mcnugget Monoid,

$$\mathscr{M} = \{6a + 9b + 20c : \ a, b, c \in \mathbb{N} \cup \{0\}\}.$$

How many base cases would you need to show by strong induction that $\mathscr{M}$ contains all natural numbers $m > 43$?

The Principle of Strong Mathematical Induction is commonly the appropriate proof technique for questions involving recursively defined sequences. Suppose that we are considering a sequence $a_1, a_2, a_3, \ldots$ of numbers, also expressed as $\{a_n\}$. In a recursively-defined sequence $\{a_n\}$, only the first term or perhaps the first few terms are defined specifically, say $a_1, a_2, \ldots, a_k$ for some fixed $k \in \mathbf{N}$. These are called the initial values. Then a_{k+1} is expressed in terms of $a_1, a_2, \ldots, a_k$ and, more generally, for $n > k, a_n$ is expressed in terms of $a_1, a_2, \ldots, a_{n-1}$. This is called the recurrence relation.

Question 126.

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

Question 127.

□

The ***Fibonacci sequence***

$$1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233, 377, \ldots$$

is defined as

$$F_1 = 1, F_2 = 1, \text{ and } F_n = F_{n-1} + F_{n-2} \text{ for all } n \geq 3.$$

Prove that for all natural numbers n,

$$F_1 + F_2 + F_3 + \cdots + F_n = F_{n+2} - 1.$$

Question 128.

□

If r is a nonzero real number such that $r + \frac{1}{r}$ *is an integer, then prove that* $r^n + \frac{1}{r^n}$ *is an integer for every positive integer n.*

Chapter 3 | Set Theory

§3.1 The Cartesian Product

Definition 3.1.92

The ordered pair formed from two elements a and b is the object (a, b).

It's called **ordered** because the order of the **coordinates** a and b is important. The object (a, b) and the object (b, a) are not the same.

Two ordered pairs (a, b) and (c, d) are **equal** if and only if the corresponding coordinates are equal, that is, $a = c$ and $b = d$.

If A and B are sets, the **Cartesian product** of A and B is defined as

$$\mathrm{A} \times \mathrm{B} = \{(a, b) : a \in \mathrm{A} \text{ and } b \in \mathrm{B}\}.$$

We read this as ''A cross B".

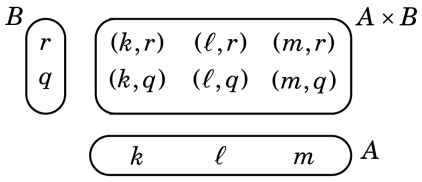


Figure 3.1: Picture of a Cartesian Product, taken from *Book of Proof*

■ **Question 129.** □

Let $\mathrm{A} = \{1, 2\}$ *and* $\mathrm{B} = \{3, 4, 5\}$.

(a) Determine $\mathrm{A} \times \mathrm{B}$.

(b) Is $\mathrm{B} \times \mathrm{A} = \mathrm{A} \times \mathrm{B}$? *Explain why or why not.*

We can take the Cartesian product of an arbitrary number of sets.

Definition 3.1.93

We define $\mathrm{A}^n := \{(a_1, a_2, \ldots, a_n) : a_i \in \mathrm{A} \text{ for } 1 \leq i \leq n\}$

and

$$\mathrm{A}_1 \times \mathrm{A}_2 \times \cdots \times \mathrm{A}_n := \{(x_1, x_2, \ldots, x_n) : x_i \in \mathrm{A}_i \text{ for } 1 \leq i \leq n\}.$$

Note: The ':=' notation stands for ''defined as''. It is used when the right hand side is the definition of the object on the left hand side.

You actually work with Cartesian products all the time in courses like Calculus and Linear Algebra, since $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$ and $\mathbb{R}^3 = \mathbb{R} \times \mathbb{R} \times \mathbb{R}$.

The elements of $A_1 \times A_2 \times \cdots \times A_n$ are called **ordered n–tuples**. Two n–tuples $(a_1, \ldots, a_n)$ and $(b_1, \ldots, b_n)$ are equal if and only if $a_i = b_i$ for every integer $1 \leq i \leq n$.

If we want to be precise about how we are performing our Cartesian products, we can use parentheses. For example, $(A \times B) \times C$ is a Cartesian product where the first set is itself a Cartesian product. Elements in this set would be ordered pairs $((x, y), w)$, where the first coordinate is itself an ordered pair.

Question 130.

□

Let $A = \{1, 2\}$ *and* $B = \{3, 4, 5\}$. *Determine the following sets by listing their elements between braces.*

(a) A^2

(b) $(A \times B) \times A$

(c) $A \times (B \times A)$

(d) $A \times \emptyset$

Question 131.

□

Sketch these Cartesian products on the xy-plane or in $\mathbb{R}^3$ *(3-dimensional space) for the last two.*

(a) $[0, 1] \times \mathbb{R}$.

(b) $\mathbb{N} \times \mathbb{Z}$.

(c) $[0, 1] \times [0, 1] \times [0, 1]$.

(d) $\{(x, y) \in \mathbb{R}^2 : x^2 + y^2 \leq 1\} \times [0, 1]$.

Question 132.

□

If A *and* B *are finite sets, how many elements does* $A \times B$ *have? In other words, can you find a formula for* $|A \times B|$*?*

§3.2 How to Prove $a \in A$

In linear algebra you must show that vectors are contained in vector spaces. In abstract algebra you must show that elements are contained in groups. In real analysis you must show that functions are contained in functional spaces. All of these structures are sets, so the proof boils down to showing that the object in question is in the set in question.

Given a set A, how do we show that $a \in A$? If a set is finite then there should be no issue with showing that a given element is contained in the set. Infinite sets, on the other hand, are usually defined using set builder notation, that is $A = \{x : P(x)\}$. Recall that $P(x)$ is an open sentence, and if $P(x)$ is true then $x \in A$. Otherwise $x \notin A$.

If we wanted to be more precise with our set-builder notation, we might write $A = \{x \in S : P(x)\}$. Then $x \in A$ is true if and only if $x \in S$ and $P(x)$ is true; if either is false, then $x \notin A$.

Question 133. □

Let $B = \{(x, y) \in \mathbb{N} \times \mathbb{N} : x \equiv 3 \pmod{y}\}$.

(a) *Is* $(23, 5) \in C$*?*

(b) *Is* $(16, 4) \in C$*?*

(c) *Let* $z \in \mathbb{N}$*. Is* $(4z + 3, z) \in B$*?*

Question 134.

□

Let $C = \{(x, y) \in \mathbb{Z} \times \mathbb{Z} : x \equiv y \pmod 7\}$.

(a) Give two examples of pairs (x, y) *such that* $(x, y) \in C$.

(b) Give two examples of pairs (a, b) *such that* $(a, b) \notin C$.

(c) Suppose $z \in \mathbb{Z}$. *Is* $(8z + 1, z + 15) \in C$*?*

(d) Let $D = \{(8z + 1, z + 15) : z \in \mathbb{Z}\}$. *Is it true that* $C = D$*?*

§3.3 Subsets and Power Sets

Definition 3.3.94

Suppose A and B are sets. If every element of A is also an element of B, then we say A is a **subset** of B and write $A \subseteq B$. We write $A \nsubseteq B$ if A is not a subset of B.

Question 135.

Rewrite the definition of '$A \subseteq B$*' using logical symbols.*

Note: We sometimes replace $A \subseteq B$ with $A \subset B$ (read as "A is a **proper** subset of B") if there is at one element in B that is not in A.

Question 136.

Determine if we should write $\subseteq$ *or* $\nsubseteq$ *between the two sets (reading left to right). As an example, the first one has been filled in for you! Recall that you learned the definition of* $\mathbb{Q}$ *earlier and promised never to forget it.*

(a) $\{1,2,3\} \subseteq \{0,1,2,3,4\}$

(b) $\{1,2,5\} \quad \{0,1,2,3,4\}$

(c) $\{x \in \mathbb{R} : x > 0\} \quad \{x \in \mathbb{R} : x \geq 0\}$

(d) $\mathbb{N} \quad \mathbb{Z}$

(e) $\mathbb{Z} \quad \mathbb{Q}$

(f) $\mathbb{N} \quad \mathbb{Q}$

(g) For any set A, A A

(h) For any set A, $\emptyset$ A.

Question 137.

Are the following True or False?

(a) $\{x \in \mathbb{R} : x - 2 = 0\} \subseteq \{x \in \mathbb{R} : x^2 - 2x = 0\}$

(b) $\{x \in \mathbb{R} : x^2 - 2x = 0\} \subseteq \{x \in \mathbb{R} : x - 2 = 0\}$

Question 138.

Consider two sets, $A = \{x : P(x)\}$ *and* $B = \{x : Q(x)\}$*. What can we say about the open sentences* P *and* Q *if we know that* $A \subseteq B$*?*

Question 139.

Let $A = \{a, b\}$, $S = \{1, \triangle, \{a, b\}\}$.

(a) List all the subsets of A.

(b) List all of the subsets of S.

Warning: Pay attention ahead, there is a distinction between '$\in$' and '$\subseteq$'.

Question 140.

Decide whether the following are True or False. If it is False, please give a brief justification.

(a) $\mathbb{N} \in \{\mathbb{N}, \mathbb{R}\}$

(b) $2 \in \{\mathbb{N}, \mathbb{R}\}$

(c) $2 \subseteq \{1, 2, 3\}$

(d) $\mathbb{N} \subseteq \{\mathbb{N}, \mathbb{R}\}$

Definition 3.3.95

Let A be a set. The **power set** of A is the set whose elements are all the possible subsets of A. It is denoted $\mathscr{P}(A)$, so

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

Question 141.

Compute the following power sets.

(a) $\mathscr{P}(\{3, 5\})$

(b) $\mathscr{P}(\{0, 1, b\})$

(c) $\mathscr{P}(\emptyset)$

(d) $\mathscr{P}(\{\emptyset\})$

(e) $\mathscr{P}(\{1, \emptyset\})$

Note: If A is finite, it is possible (though maybe not practical) to list out all of the elements of $\mathscr{P}(A)$ between braces. That is not possible if A is infinite.

Question 142.

Find $\mathscr{P}(\{a, b\}) \times \mathscr{P}(\{0, 1\})$ *and* $\mathscr{P}(\{a, b\} \times \{0, 1\})$. *Are these two sets the same? Note that you might not need to list every element of each set to answer this question.*

Theorem 3.3.96

If A *is a set with* n *elements, then* $\mathscr{P}(A)$ *is a set with* 2^n *elements.*

Can you explain why? Read the explanation on page 13 in the textbook first. See if you can understand the idea. Here's a sketch of a combinatorial proof.

Proof of theorem 96.

If $n = 0$, or if A is the empty set, then $\mathscr{P}(A) = \{\emptyset\}$ which is a set with $2^0 = 1$ element. Thus the theorem is true for $n = 0$.

Suppose A has n elements, for $n \geq 1$. We can write A as

$$A = \{x_1, x_2, \ldots, x_n\}.$$

To describe any subset B of A, we need to know for each $x_i \in A$ whether the element is in B. For each x_i, there are exactly two possibilities (either $x_i \in B$ or $x_i \notin B$), so there are $\underbrace{2 \cdot 2 \cdot 2 \cdots 2}_{n \text{ factors}}$ different ways of making a subset of A.

Therefore $\mathscr{P}(A)$ has 2^n elements. ■

Question 143.

Prove theorem 96 by induction on n.

Question 144.

Suppose A *and* B *are sets of cardinality* $|A| = n$ *and* $|B| = m$. *Determine the cardinality of the given sets.*

(a) $|\mathscr{P}(A \times B)| =$

(b) $|\mathscr{P}(\mathscr{P}(A))| =$

(c) $|\{X \in \mathscr{P}(B) : |X| \leq 1\}| =$

(d) $|\mathscr{P}(A \times \mathscr{P}(B))| =$

Question 145.

Let $A = \{X \in \mathscr{P}(\mathbb{Z}) : |X| = 2\}$. *Are the following sets in* A*?*

(a) Is $\{-3, 7\} \in A$?

(b) Is $\{\pi, 7\} \in A$?

(c) Is $\{-3, 7, 12\} \in A$?

Exploration Activity

Discuss what the elements of the set $\mathscr{P}(\mathbb{R}^2)$ look like.

§3.4 Union, Intersection, Difference

A **binary operation** for sets is an operation that takes two ('bi') sets and produces one set. For example, the Cartesian product is a binary operation.

Definition 3.4.97

Let A and B be sets.

- The **union** of A and B is the set $A \cup B = \{x : x \in A \textbf{ or } x \in B\}$.
- The **intersection** of A and B is the set $A \cap B = \{x : x \in A \textbf{ and } x \in B\}$.
- The **difference** of A and B is the set $A \setminus B = \{x : x \in A \textbf{ and } x \notin B\}$.
- Sets A and B are said to be **disjoint** if $A \cap B = \emptyset$.

Note: In the textbook, the difference of A and B is denoted as $A - B$. We are going to use the $A \setminus B$ notation instead to avoid any ambiguity with the regular arithmetic operation.

Question 146.

Consider the following sets for this question:

$$A = \{1, 2, 3, 4, 5\}, \quad B = \{4, 5, 6\},$$

Perform the indicated set operation to obtain a new set.

(a) $A \cup B =$

(b) $A \cap B =$

(c) $A \setminus B =$

(d) $B \setminus A =$

(e) $(A \setminus B) \cup (B \setminus A) =$

(f) $(A \setminus B) \cap (B \setminus A) =$

Question 147.

Determine the elements contained in these intervals in $\mathbb{R}$. It might help to draw the intervals to aid in your understanding.

(a) $[0, 3] \cup [2, 5]$ *(b)* $[0, 3] \cap [2, 5]$ *(c)* $[0, 3] \setminus [2, 5]$

Question 148.

*Write the open interval $(1, 3)$ as the union of two **disjoint** subsets of $\mathbb{R}$.*

Question 149.

Let A *be an arbitrary set. determine the following:*

(a) $A \cup \emptyset$ *(b)* $A \cap \emptyset$ *(c)* $A \setminus \emptyset$

Question 150.

Suppose $A = \{0, 1\}$ *and* $B = \{1, 2\}$. *Find the following:*

(a) $(A \cap B) \times A$ *(b)* $(A \times B) \cap B$

This is a fun one. If you believe it is "False" then you should be able to produce an element that is in one of the sets but not the other. It might help to try to sketch these sets below.

Question 151.

(a) Is the statement $(\mathbb{R} \times \mathbb{Z}) \cap (\mathbb{Z} \times \mathbb{R}) = \mathbb{Z} \times \mathbb{Z}$ *true or false?*

(b) What about the statement $(\mathbb{R} \times \mathbb{Z}) \cup (\mathbb{Z} \times \mathbb{R}) = \mathbb{R} \times \mathbb{R}$*?*

Question 152.

Does there exist a set X *for which* $\mathbb{N} \in X$ *and* $\mathbb{N} \subseteq X$*?*

§3.5 Complement

When considering sets, they often naturally live inside some larger **universal set**. From now on, we will assume that, whenever we are discussing sets, there is some universal set U (which is often made clear from the context).

Definition 3.5.98

Let A be a subset of the universal set U. The **complement** of A is the set $\overline{A} = U \setminus A$.

Note: Our textbook uses the bar notation for complement but other texts and authors use different notation. One of the most common is to use a superscript c like so: A^c. In a future math class, this notation might change! (sorry)

Question 153.

□

(a) *If* $U = \{1,2,3,4,5\}$ *and* $A = \{1,3\}$, *then* $\overline{A} =$

(b) *If* $U = \mathbb{Z}$, *then* $\overline{\mathbb{N}} =$

(c) *If* U *is the universe, then what is* $\overline{U}$*?*

And what about $\overline{\emptyset}$*?*

Question 154.

□

Let $U = \{0,1,2,\ldots,10\}$ *and consider the sets* $A = \{0,2,7\}$, $B = \{1,3,6\}$, $C = \{0,2,4,6,8,10\}$. *Calculate the set operations below for these sets.*

(a) $A \cup B$

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

(c) $A \setminus C$

(d) $B \setminus C$

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

(f) $(A \cap B)$

(g) $C \cap \emptyset$

(h) $\overline{B} \cup B$

(i) $\overline{B} \cap B$

(j) $A \cap \overline{C}$

(k) $\overline{(A \cup B)}$

(l) $\overline{A} \cap \overline{B}$

Question 155.

□

In the previous exercise, some of the sets are the same, possibly due to coincidence and possibly because they are the same for any sets A, B, *and* C*!* ***Write down at least one conjecture you have based on these results.***

§3.6 Venn Diagrams

We sometimes use circular diagrams called Venn diagrams to represent sets. I'm guessing you've seen these before, but maybe haven't thought about how the regions or their overlaps represent intersections, unions, and complements.

Question 156. □

*How many **different** ways can you draw a Venn diagram involving two sets* A *and* B*?*

Question 157. □

Draw four two-circle Venn diagrams for A *and* B*. Then shade* $A \cup B$, $A \cap B$, A, *and* $B \setminus A$.

Question 158. □

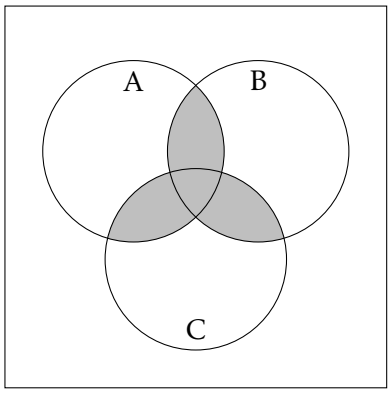
Suppose $|A| = 5$, $|B| = 7$, *and* $|A \cup B| = 9$*. What can you say about* $|A \cap B|$*?*

Question 159.

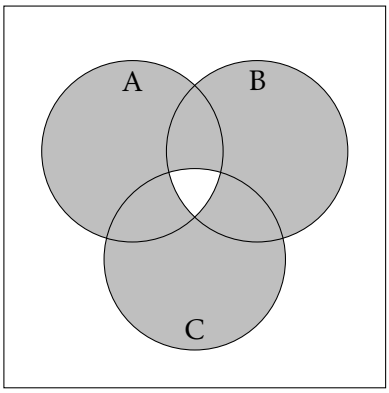
Draw a three-circle Venn diagram (like the ones depicted below) for A, B, *and* C. *Then shade* $(A \setminus B) \cap C$.

Question 160.

Write a corresponding expression for the shaded region of the given Venn Diagrams.



(a)



(b)

Fun fact: It is impossible to draw a Venn diagram for four sets in the plane using circles, but it can be done with ellipses. Try it out!

§3.7 How to Prove $A \subseteq B$

We have two (or three) main methods to prove that $A \subseteq B$. They all revolve around the fact that proving $A \subseteq B$ means proving the conditional statement "If $x \in A$, then $x \in B$." In other words, every element of A is also an element of B.

- **Proving $A \subseteq B$ with a direct proof (Pick-a-point Method)**

> *Proof.* Suppose $x \in A$.
> ⋮
> Thus $x \in B$.
> Therefore $A \subseteq B$. ■

- **Proving $A \subseteq B$ with a contrapositive proof**

> *Proof.* Suppose $x \notin B$.
> ⋮
> Thus $x \notin A$.
> Therefore $A \subseteq B$. ■

- Finally, you could also use **proof by contradiction** (assume $x \in A$ and $x \notin B$, then get some contradiction).

Remember that we want to practice and refine our proof writing capabilities, so some of these may have very simple proofs, but focus on practicing writing out details in a logical and rigorous way. That is, **write down your given/hypothesis** and **state what you are trying to prove**. Clearly state if something follows from a definition or a prior result.

Theorem 3.7.99

(a) *For every set* A, $\emptyset \subseteq A$.

(b) *For every set* A, $A \subseteq A$.

(c) *Transitivity Property: For all sets* A, B, *and* C, *if* $A \subseteq B$ *and* $B \subseteq C$, *then* $A \subseteq C$.

Theorem 3.7.100

For all sets A, B, *and* C:

(a) $A \subseteq A \cup B$

(b) $A \cap B \subseteq A$

(c) *If* $A \subseteq B$, *then* $A \cup C \subseteq B \cup C$.

(d) *If* $A \subseteq B$, *then* $\overline{B} \subseteq \overline{A}$.

(e) *If* $A \subseteq B$, *then* $A \cap C \subseteq B \cap C$.

(f) *If* $A \subseteq B$, *then* $A \setminus C \subseteq B \setminus C$.

Let's prove one of these claims as an example.

■ **Question 161.** □

Prove the following claim.

Claim 3.7.101

If $A \subseteq B$, *then* $A \cap C \subseteq B \cap C$.

Proof of claim 101.

Suppose that $A \subseteq B$ and let $x \in A \cap C$. Since $x \in A \cap C$, $x \in A$ and $x \in C$. Therefore, to show that $x \in B \cap C$, it remains only to show that $x \in B$. Since $A \subseteq B$ and $x \in A$, it follows that $x \in B$, and thus that $x \in B \cap C$. Therefore, we have shown that if $A \subseteq B$, then $A \cap C \subseteq B \cap C$. ■

■ Question 162. □

If A *and* B *are sets with* $\mathscr{P}(A) \subseteq \mathscr{P}(B)$, *then prove that* $A \subseteq B$.

■ Question 163. □

Let $A = 4\mathbb{Z} = \{n \in \mathbb{Z} : n \text{ is a multiple of } 4\}$ *and* $B = 2\mathbb{Z} = \{n \in \mathbb{Z} : n \text{ is even}\}$. *Prove* $A \subseteq B$.

■ Question 164. □

Prove or provide a counterexample to each of the following:

(a) $(A \times B) \cup (C \times D) \subseteq (A \cup C) \times (B \cup D)$

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

§3.8 How to Prove A = B

Definition 3.8.102

Two sets A and B are **equal** if and only if they have exactly the same elements:

$$A = B \iff A \subseteq B \text{ and } B \subseteq A.$$

As such, the most common way to show that A = B is the following two part method.

Proof.

(a) Prove that $A \subseteq B$ (by any method).

(b) Prove that $B \subseteq A$ (by any method).

Therefore A = B. ■

Question 165. □

Let $A = \{2k+1 : k \in \mathbb{Z}\}$ *and* $B = \{2k-1 : k \in \mathbb{Z}\}$. *Prove that* A = B.

This shows that we could also use $x = 2k - 1$ for some $k \in \mathbb{Z}$ as our definition of odd.

Question 166. □

Let $C = \{x \in \mathbb{Z} : 15 \mid x\}$ *and* $D = \{x \in \mathbb{Z} : 3 \mid x\} \cap \{x \in \mathbb{Z} : 5 \mid x\}$. *Prove that* C = D.

For this next theorem, sketch a Venn diagram of sets A and B with $A \subseteq B$ to give you a visual. This might help you see why each statement is equivalent to $A \subseteq B$. Having a visual can also prove helpful in crafting a **pick-a-point** proof method of proof. But note: a picture, by itself, never constitutes a complete proof when working with sets.

Theorem 3.8.103

Suppose A *and* B *are sets contained in a universal set* $\mathscr{U}$*. The following are equivalent:*

(a) $A \subseteq B$

(b) $\overline{B} \subseteq \overline{A}$

(c) $\overline{A} \cup B = \mathscr{U}$

(d) $A \cap \overline{B} = \emptyset$

(e) $A \cup B = B$

(f) $A \cap B = A$

Sketch of Proof. Recall we saw how to prove statements of this form in the last chapter. The shortest proof would be to show $(a) \implies (b) \implies (c) \implies (d) \implies (e) \implies (f) \implies (a)$. ■

Example 3.8.104

Here is one part of a possible proof for theorem 103 above. Suppose we wanted to prove that (b) implies (c). That is, we want to assume that $\overline{B} \subseteq \overline{A}$ is true and prove that $\overline{A} \cup B = \mathscr{U}$.

Proof. Suppose (b) holds, meaning $\overline{B} \subseteq \overline{A}$. We want to show that $\overline{A} \cup B = \mathscr{U}$, which we can do by showing two inclusions.

The inclusion $\overline{A} \cup B \subseteq \mathscr{U}$ is always true, because our universe is $\mathscr{U}$.

Now we show that $\mathscr{U} \subseteq \overline{A} \cup B$. Let $x \in \mathscr{U}$. We know that $\mathscr{U} = B \cup \overline{B}$, so there are two possibilities for where x lives.

If $x \in B$, then $x \in \overline{A} \cup B$ by definition of the union of two sets. Otherwise, $x \in \overline{B}$. Hence, by (b), $x \in \overline{A}$. Thus, $x \in \overline{A} \cup B$ and we get $\mathscr{U} \subseteq \overline{A} \cup B$. Therefore, $\overline{A} \cup B = \mathscr{U}$ and we have that (b) implies (c). ■

■ **Question 167.** □

Prove the following statement (which is one of DeMorgan's Laws). If A *and* B *are sets in a universal set* $\mathscr{U}$*, then:*

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

Proof. Left as homework. ■

Usually, when we prove if an only if proofs, we first prove one direction and then the other. However, sometimes, the two directions are so similar our proof can basically be read "backwards" to prove the other direction. In these cases, you can write "if and only if" at each step. Consider the following example.

Proposition 3.8.105

Let A *and* B *be sets, then* $(A \setminus B) \cup (B \setminus A) = (A \cup B) \setminus (A \cap B)$.

Proof.

■

Warning: That's so useful! Why don't we always do that? Because there is a dark force that tempts students to throw $\iff$ in front of every line whether it makes sense to or not. Consider the following "proof." Is it correct?

Proposition 3.8.106: Questionable Statement

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

"Proof".

$$\begin{aligned} & (x,y) \in (A \times B) \cup (C \times D) \\ \iff & (x,y) \in A \times B \text{ or } (x,y) \in C \times D \\ \iff & (x \in A \text{ or } x \in C) \text{ and } (y \in B \text{ or } y \in D) \\ \iff & x \in (A \cup C) \text{ and } y \in (B \cup D) \\ \iff & (x,y) \in (A \cup C) \times (B \cup D) \end{aligned}$$

■

Question 168.

□

Hopefully, you provided a counterexample to one direction of this proof in the last section . Therefore, there must be at least one flaw in this proof. Which implication is not correct?

Compare this to the theorem and proof below, which are entirely correct!

Theorem 3.8.107

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

Proof of theorem 107.

We will prove $(A \times B) \cap (C \times D) = (A \cap C) \times (B \cap D)$ using a biconditional proof.

$$\begin{aligned} & (x,y) \in (A \times B) \cap (C \times D) \\ \iff & (x,y) \in A \times B \text{ and } (x,y) \in C \times D \\ \iff & (x \in A \text{ and } x \in C) \text{ and } (y \in B \text{ and } y \in D) \\ \iff & x \in (A \cap C) \text{ and } y \in (B \cap D) \\ \iff & (x,y) \in (A \cap C) \times (B \cap D) \end{aligned}$$

Therefore $(A \times B) \cap (C \times D) = (A \cap C) \times (B \cap D)$. ■

Question 169. □

Is it true that $(\mathbb{R} \setminus \mathbb{Z}) \times \mathbb{N} = (\mathbb{R} \times \mathbb{N}) \setminus (\mathbb{Z} \times \mathbb{N})$*? Prove these sets are equal by proving the more general claim:*

Claim 3.8.108

For any sets A, B, *and* C *in a universal set* $\mathcal{U}$*,*

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

Here are some more theorems involving sets. You should try proving these on your own to get some practice.

Theorem 3.8.109

For all sets A, B, *and* C*:*

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

Theorem 3.8.110

If A *and* B *are sets with no elements, then* A = B.

Proof. Since A has no elements, the sentence $(\forall x)(x \in A \Rightarrow x \in B)$ is true. Therefore, $A \subseteq B$. Similarly, $(\forall x)(x \in B \Rightarrow x \in A)$ is true, so then $B \subseteq A$. Therefore, by definition of set equality, A = B. ■

Theorem 3.8.111

For any sets A *and* B*, if* $A \subseteq B$*, and* $A \neq \emptyset$*, then* $B \neq \emptyset$.

Proof. Suppose $A \subseteq B$ and $A \neq \emptyset$. Since A is nonempty, there is an object x such that $x \in A$. Since $x \in A$, then $x \in B$. Therefore $B \neq \emptyset$. ■

Theorem 3.8.112

If A, B, *and* C *are sets, then*

(a) $A \times (B \cup C) = (A \times B) \cup (A \times C)$.

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

Recall the following question from the end of Chapter 1 concerning Russell's Paradox. See if you have better luck now!

■ **Question 170.** □

Assuming that we have a universal set $\mathscr{U}$*, the set* R *in Russell's paradox would have to be stated as:*

$$R = \{X : X \in \mathscr{U} \text{ and } X \notin X\}.$$

Show that $R \notin R$ *and* $R \notin \mathscr{U}$*. Does this resolve the paradox?*

§3.9 Indexed Sets

We can extend the ideas of unions and intersections to larger numbers of sets. To write these more compactly, we usually index the sets (so we write $A_1 \cup A_2 \cup A_3 \cup \cdots$ instead of $A \cup B \cup C \cup \cdots$). We also use some notation similar to the Σ-notation you used to write sums in Calculus.

Definition 3.9.113

Suppose $A_1, A_2, \ldots, A_n$ are sets. Then

$$A_1 \cup A_2 \cup \cdots \cup A_n = \bigcup_{i=1}^{n} A_i = \{x : x \in A_i \text{ for at least one set } A_i, \text{ for } 1 \leq i \leq n\}$$

$$A_1 \cap A_2 \cap \cdots \cap A_n = \bigcap_{i=1}^{n} A_i = \{x : x \in A_i \text{ for every set } A_i, \text{ for } 1 \leq i \leq n\}$$

Question 171. □

Rewrite the definitions using logical symbols for universal quantifiers.

Question 172. □

Suppose $A_1 = \{a, 1, 3, 5\}$, $A_2 = \{a, b, 1\}$, $A_3 = \{a, -2, 1\}$. *Determine the following union and intersection:*

(a) $\bigcup_{i=1}^{3} A_i =$

(b) $\bigcap_{i=1}^{3} A_i =$

These same ideas and notation work for **infinite** unions and intersections.

Question 173. □

Let $A_1 = \{1\}, A_2 = \{1, 2\}, A_3 = \{1, 2, 3\}, \ldots, A_i = \{1, 2, \ldots, i\}, \ldots$.

(a) $\bigcup_{i=1}^{\infty} A_i$

(b) $\bigcap_{i=1}^{\infty} A_i$

In the last two questions, we counted off our sets using the natural numbers as indices. If you wanted to talk about the 145th set in the list for the previous problem, you know to denote this set by A_{145}. For the full collection of sets, instead of saying "i goes from 1 to ∞", we can say $i \in \mathbb{N}$. For example, we can write

$$A_1 \cup A_2 \cup A_3 \cup \cdots = \bigcup_{i=1}^{\infty} A_i = \bigcup_{i \in \mathbb{N}} A_i, \qquad A_1 \cap A_2 \cap A_3 \cap \cdots = \bigcap_{i=1}^{\infty} A_i = \bigcap_{i \in \mathbb{N}} A_i.$$

In this case, the sets are **indexed** by the set $\mathbb{N}$. We call $\mathbb{N}$ the **index set**. 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.

Example 3.9.114

Suppose we wanted to think about open intervals of the form $(-\alpha, \alpha)$, where α is any real number. Such a family of open intervals would include intervals like

$$(-\sqrt{2}, \sqrt{2}), (-100, 100), (-6\ln(17), 6\ln(17)), \ldots$$

and so on. How can we **index** each of these sets? The way we described them tells us exactly - we want to think about sets of the form $(-\alpha, \alpha)$ for each $\alpha \in \mathbb{R}$. Hence, we could denote each such interval by

$$A_\alpha = (-\alpha, \alpha), \text{ for } \alpha \in \mathbb{R}.$$

In this case, our indexing set is $\mathbb{R}$.

Any set (finite or infinite) can be used as an indexing set. In our text, the letter I is often used for arbitrary indexing sets, and small Greek letters are used to represent elements of these sets. Of course, these are merely conventions, not rules. You can really use any symbols you want.

Note:

- If I is a set and we have a collection of sets indexed by I, then we may write $\{A_\alpha\}_{\alpha \in I}$ to refer to this collection. We read this as ''the set of A-alphas over alpha in I."
- If a collection of sets is indexed by $\mathbb{N}$, then we usually will write $\{A_i\}_{i \in \mathbb{N}}$ or $\{A_i\}_{i=1}^{\infty}$ to refer to this collection.

Question 174.

Describe the set of all circles in xy-plane with integer radius and centered at the origin, as an indexed set.

Definition 3.9.115

Given a collection of set $\mathscr{A} = \{A_\alpha : \alpha \in I\}$ where I is some index set not equal to $\emptyset$, we define

$$\bigcup_{\alpha \in I} A_\alpha = \{x : (\exists \alpha \in I)(x \in A_\alpha)\} \quad \text{and} \quad \bigcap_{\alpha \in I} A_\alpha = \{x : (\forall \alpha \in I)(x \in A_\alpha)\}$$

We call these **generalized unions** and **generalized intersections**.

Question 175.

For each $n \in \mathbb{N}$, let $\mathrm{B}_n = \{na : a \in \mathbb{Z}\}$. Determine the following sets.

(a) $\displaystyle\bigcup_{i\in\mathbb{N}} \mathrm{B}_i$

(b) $\displaystyle\bigcap_{i\in\mathbb{N}} \mathrm{B}_i$

Question 176.

Determine the following sets.

(a) $\displaystyle\bigcup_{i\in\mathbb{N}} \left[0, \frac{i}{i+1}\right]$

(b) $\displaystyle\bigcup_{i\in\mathbb{N}} \left[0, 1 - \frac{1}{i}\right]$

(c) $\displaystyle\bigcap_{i\in\mathbb{N}} [0, i+1]$

(d) $\displaystyle\bigcap_{i\in\mathbb{N}} \left[0, 1 + \frac{1}{i}\right]$

Question 177.

Let $\mathrm{A}_\alpha = (\alpha, \infty)$. Determine the following sets.

(a) $\displaystyle\bigcap_{\alpha\in\mathbb{R}} \mathrm{A}_\alpha$

(b) $\displaystyle\bigcup_{\alpha\in\mathbb{R}} \mathrm{A}_\alpha$

3.9.1 Proofs involving Indexed Sets

Try to formally prove a few questions from last section using the methods we have learned so far.

Question 178. □

For each $n \in \mathbb{N}$, let $A_n = [0, n+1] = \{x \in \mathbb{R} : 0 \leq x \leq n+1\}$. Prove:

(a) $\bigcup_{n\in\mathbb{N}} A_n = [0, \infty)$

(b) $\bigcap_{n\in\mathbb{N}} A_n = [0, 2]$

To prove (b) in the next question, consider an indirect approach, such as contrapositive or contradiction. This is often the technique we use when trying to show that a set is empty.

Question 179. □

For each $\alpha \in \mathbb{R}$, let $A_\alpha = (\alpha, \infty) = \{x \in \mathbb{R} : \alpha < x\}$. Prove:

(a) $\bigcup_{\alpha\in\mathbb{R}} A_\alpha = \mathbb{R}$

(b) $\bigcap_{\alpha\in\mathbb{R}} A_\alpha = \emptyset$

Question 180.

For each $\alpha \in \mathbb{R}$, *let* $A_\alpha = \{(x, \alpha(x^2-1)) \in \mathbb{R}^2 : x \in \mathbb{R}\}$.

Prove that $\bigcap_{\alpha\in\mathbb{R}} A_\alpha = \{(-1,0),(1,0)\}$.

Question 181.

See if you can prove the following theorem.

Theorem 3.9.116: DeMorgan's Laws for Generalized Union and Intersection

Let $\mathscr{A} = \{A_\alpha : \alpha \in I\}$ *be an indexed collection of sets. Then*

(a) $\overline{\left(\bigcap_{\alpha\in I} A_\alpha\right)} = \bigcup_{\alpha\in I} \overline{A_\alpha}$

(b) $\overline{\left(\bigcup_{\alpha\in I} A_\alpha\right)} = \bigcap_{\alpha\in I} \overline{A_\alpha}$

Question 182.

Prove that

(a) $B \cup \left(\bigcap_{\alpha \in I} A_\alpha \right) = \bigcap_{\alpha \in I} (B \cup A_\alpha).$

(b) $B \setminus \left(\bigcap_{\alpha \in I} A_\alpha \right) = \bigcup_{\alpha \in I} (B \setminus A_\alpha).$

Chapter 4 | Relations and Functions

We'll now a make a change in the focus of the course. Up to this point, our focus has been on learning techniques to write proofs. Along the way we've had to learn a few new concepts to have something new to write proofs about. The remainder of our time will be devoted to learning new math concepts, but these are still fundamental to all of mathematics. In this chapter, we focus on **Relations** and **functions**. You may be already familiar with some or both of these notions, but we will explore them in a more abstract and more rigorous way than you have (likely) ever done before. All the while we will, of course, write proofs and continue to focus on improving our writing.

§4.1 Relation on a Set

We first seek to motivate our upcoming definition for a **relation** by means of an example.

Question 183. □

(a) Let's pretend that you're teaching an elementary school class and you need to teach the students how to properly use the less than symbol "<." To keep things simple, we'll focus entirely on the integers in the set $A = \{1, 5, 7, 10\}$*. The students need to see some examples, so write down every possible correct use of the "<" symbol for elements in the set* A *(e.g.,* $5 < 7$ *is one example).*

(b) Repeat the same process for the "=" symbol.

In the question above, there's nothing particularly special about the "<" and "=" symbols. That is, the symbols themselves don't really have any meaning. It's the elements that we put the symbols between that really matter. To sum up: the only way to distinguish between two relations on a given set is to know an **ordered pair** that belongs to one of the relations but not to the other. Hence, when we talk of **relations**, we are really talking about Cartesian product of **sets**.

Definition 4.1.117

Let A be a set. Then a relation R on the set A is a collection of ordered pairs of elements of A; that is, a subset $R \subseteq A \times A$. If $(a, b) \in R$ we write aRb and say aloud "a is related to b". If $(a, b) \notin R$, then we write $a \not R b$.

Question 184. □

Let $A = \{0, 1, 2, 3\}$ *and consider a relation* $R \subseteq A \times A$ *defined by congruence modulo 3:*

$$xRy \iff x \equiv y \pmod 3.$$

Write out the relation R *as a set of ordered pairs.*

Here's a less numerical example.

Example 4.1.118

- Let P denote the set of all people with accounts on Facebook. Define a relation via $x \; y \iff x$ is friends with y. Then is a relation on P .
- Compare this to the set Q of all people with accounts on Instagram. Define via $x \; y \iff x$ follows y. Then is a relation on Q.

There is an interesting distinction between the two relations above. Observe that $x \; y$ automatically implies $y \; x$. But $x \; y$ does not necessarily imply $y \; x$.

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

Example 4.1.119

Figure 4.1 depicts a digraph that represents a relation R given by

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

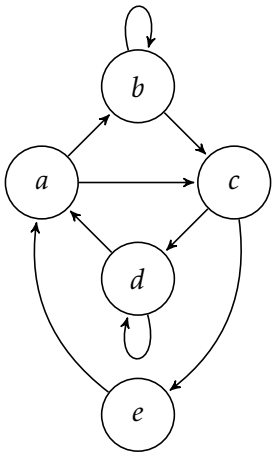


Figure 4.1: An example of a digraph for a relation R

Question 185.

Consider the digraph in fig. 4.2 below. Write the sets A *and* R.

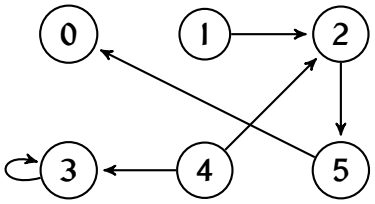


Figure 4.2: Digraph for Question 3

Example 4.1.120

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:

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

A picture depicting this relation (a set) in $\mathbb{R}^2$ is the standard unit circle.

Example 4.1.121

The ‘‘less than" relation $<$ on $A = \mathbb{Z}$ can be written in set-builder notation as:

$$\{(x, y) \in \mathbb{Z} \times \mathbb{Z} : y - x \in \mathbb{N}\}.$$

Note how we write the relation without referencing the symbol ‘$<$’ or ‘$>$’. We know from our algebra of numbers that, if $x < y$, then $0 < y - x$. Hence, we define the relation using only sets and arithmetic here.

■ **Question 186.** □

Consider the relation $R = (\mathbb{R} \times \mathbb{R}) \setminus \{(x, x) : x \in \mathbb{R}\} \subseteq \mathbb{R} \times \mathbb{R}$. *What familiar relation on* $\mathbb{R}$ *is this? Explain.*

4.1.1 Properties of Relations

Definition 4.1.122

Let A be a set and R be a relation on A.

- R is **reflexive** if and only if for all $x \in A$, xRx.
- R is **symmetric** if and only if for all $x, y \in A$, if xRy then yRx.
- R is **transitive** if and only if for all $x, y, z \in A$, if xRy and yRz, then xRz.

Example 4.1.123

We can see that several familiar relations satisfy two or more of the reflexive, symmetric, and transitive properties.

(a) The relation $\leq$ on $\mathbb{R}$ satisfies the reflexive and transitive properties. Can you think of an example to show why $\leq$ is not symmetric?

(b) Give a set X, we can make the subset relation $\subseteq$ on $\mathscr{P}(X)$. Then $\subseteq$ is reflexive and transitive, but not symmetric.

(c) The relation $=$ on $\mathbb{R}$ satisfies all three properties in definition 122.

Question 187. □

Define a relation R *on* $\mathbb{Z}$ *as* xRy *if* $|x-y|<1$. *Is* R *reflexive? Symmetric? Transitive? If a property does not hold, say why. What familiar relation on* $\mathbb{Z}$ *is this?*

Question 188. □

Consider $R = \{(a,b) \in \mathbb{Z} \times \mathbb{Z} \ : \ b = na \text{ for some } n \in \mathbb{Z}\}$ *on* $\mathbb{Z}$.

(a) What familiar relation on $\mathbb{Z}$ *is* R *describing?*

(b) Determine if R *is reflexive, symmetric, or transitive.*

Question 189. □

Consider the relation $R = \{(1,1),(1,2),(2,1),(2,2),(3,3)\}$ *on the set* $\{1,2,3\}$. *Is* R *reflexive? Symmetric? Transitive?*

Question 190. □

True or False: *If a relation is symmetric and transitive, then it is also reflexive.*

Definition 4.1.124

A relation R on a set A is an **equivalence relation on** A if and only if R is reflexive, symmetric, and transitive on A.

Example 4.1.125: Some examples of equivalence relations.

(a) Given any set A, **equality** is an equivalence relation. That is, the relation

$$\mathrm{R} = \{(a, a) \in \mathrm{A} \times \mathrm{A} : a \in \mathrm{A}\}$$

is always an equivalence relation for any set A.

(b) The book shows, in Example 11.8 on page 208, that **congruence modulo** n is an equivalence relation on $\mathbb{Z}$. That is, for any integer $n > 1$, the relation R defined by $a\mathrm{R}b \iff a \equiv b \pmod{n}$ is an equivalence relation on $\mathbb{Z}$.

(c) On the set $\mathscr{T}$ of all triangles in a given plane, the relations of congruence and similarity are both equivalence relations.

Question 191.

Consider the relation $\mathrm{R} = \{(a, b) \in \mathbb{Z} \times \mathbb{Z} : 3a - 5b \text{ is even}\}$. *Prove that* R *is an equivalence relation.*

□

Question 192.

Prove that the relation T *on* $\mathbb{R} \times \mathbb{R}$ *given by* $(x, y)\mathrm{T}(a, b)$ *if and only if* $x^2 + y^2 = a^2 + b^2$ *is an equivalence relation.*

□

4.1.2 Equivalence Class and Partitions

Definition 4.1.126: Equivalence Class

Let $\sim$ be an equivalence relation on a set A. For $a \in A$, the **equivalence class** of a determined by $\sim$ is the set:

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

The set

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

of all equivalence classes is called A mod $\sim$, and sometimes referred to as the quotient set of A by $\sim$.

Note: Notice that $A/\sim$ is a **set of sets**. In particular, an element of $A/\sim$ is a subset of A.

Question 193. □

Let $A = \{1,2,3,4,5,6\}$ *and define an equivalence (check) relation* $\sim$ *by*

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

Determine the equivalence classes $[a]$ *for each* $a \in A = \{1,2,3,4,5,6\}$.

Question 194. □

Compute the equivalence classes $[(1,2)],[(4,0)]$, *and* $[(0,0)]$ *for the realtion in question 192. Draw a geometric picture in* $\mathbb{R}^2$ *representing these classes.*

Question 195.

Describe the equivalence classes for the equivalence relation in question 191. [i]

In all of the above examples, you might notice that equivalence classes that are not equal have empty intersection. This is in fact true for any equivalence relation.

Theorem 4.1.127

Let $\sim$ be an equivalence relation on a nonempty set A. For all $x, y \in A$,

(a) $[x] \subseteq A$ *and* $x \in [x]$*, i.e. every equivalence class is a nonempty subset of* A.

(b) $x \sim y$ *if and only if* $[x] = [y]$*, i.e. elements of* A *are related if and only if their equivalence classes are identical.*

(c) $x \nsim y$ *if and only if* $[x] \cap [y] = \emptyset$*, i.e. elements of* A *are unrelated if and only if their equivalence classes are disjoint.*

Question 196.

Consider the relation '$\equiv \pmod 4$ on $\mathbb{Z}$'. In example 125(b), you computed all of the equivalence classes for this relation. These can be written as $[0], [1], [2]$, and $[3]$. Given any integer x, explain how you would determine which of these four equivalence classes x belongs to. Explain why this shows that $\mathbb{Z} = [0] \cup [1] \cup [2] \cup [3]$.

Theorem 127 tells us that the set of equivalence classes, A/R, forms a **partition** of the set A.

Definition 4.1.128

Let A be a nonempty set. Then Ω is a **partition of** A if Ω is a set of subsets of A such that

(a) If $X \in \Omega$, then $X \neq \emptyset$.

(b) Given $X, Y \in \Omega$, either $X = Y$ or $X \cap Y = \emptyset$.

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

[i] If you get stuck, see the solution in the back of the book for Exercise 7 in Section 11.3 of the textbook.

Example 4.1.129

The following are all examples of partitions of the given set.

(a) freshman, sophomore, junior, senior (set of college students)

(b) evens, odds (set of integers)

(c) rationals, irrationals (set of real numbers)

Question 197.

Let $A = \{1,2,3,4,5,6,7,8\}$. *One possible partition of* A *is*

$$\Omega = \{\{1,2,8\},\{3,5,6,7\},\{4\}\}.$$

(a) Describe ***three more partitions*** *for* A.

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

Question 198.

(a) There are five different equivalence relations on the set $\{a,b,c\}$. *Describe them all (diagrams will suffice).*

(b) List all partitions for the set $A = \{a,b,c\}$. *Compare your answer to above. What do you notice?*

§4.2 Functions

Definition 4.2.130

Let A and B be sets. Then we define R to be a **relation from** A **to** B if and only if R is a subset of $A \times B$ ($R \subseteq A \times B$).

If $(a,b) \in R$ we write aRb and say a is R-**related** (or **related**) to b. If $(a,b) \notin R$, then we write $a \not R b$.

Hence, when we discussed **relations** on a set A throughout last section, we were really thinking of relations from a set A to itself.

This should line up with your grade school introduction to relations. You saw these as ordered pairs of numbers. From here, it was a quick step over to thinking about functions as special relations. You probably remember plotting points in the plane $\mathbb{R}^2$ and being asked, "**is this the graph of a function**?" All of that thinking still holds true in general, but now you can see that relations and functions from your algebra and Calculus days were secretly about **sets** - specifically, subsets of $\mathbb{R} \times \mathbb{R}$.

Functions are relations between two sets that satisfy certain properties. They make up our final fundamental tool of mathematics. Functions are used in all branches of mathematics to model diverse situations and pull together ideas that at first seem unrelated. As such, functions are as vital as numbers in mathematics.

4.2.1 A specific type of Relation

Definition 4.2.131

Suppose A and B are sets. A **function** (or mapping) from A to B is a relation $f \subseteq A \times B$, satisfying the property that for each $a \in A$, the relation f contains exactly one ordered pair of the form (a,b). We write $f : A \to B$ and read it as "f is a function from A to B" or "f maps A to B."

A function is only a **single-valued correspondence.** Meaning, for every $x \in A$, there corresponds only one unique value in B. This condition allows us to refer to *the* image of x, instead of *an* image. You visualized this in prior math classes, when studying functions $f : \mathbb{R} \to \mathbb{R}$, by means of the **vertical line test**. If the graph of a relation in $\mathbb{R}^2$ didn't pass the vertical line test, then it couldn't be a function, precisely because there would be some input a that shows up more than once in an ordered pair of f.

Question 199. □

Let $A = \{1,6,12\}$, $B = \{0,2,12\}$. *The following are all relations from* A *to* B, *but which are functions? Explain why or why not?*

(a) $f_1 = \{(1,2),(6,0),(12,12)\}$

(b) $f_2 = \{(1,0),(1,2),(6,12),(12,0)\}$

(c) $f_3 = \{(1,12),(6,0)\}$

(d) $f_4 = \{(1,0),(6,0),(12,0)\}$

Question 200.

Consider the set $C = \{(x,y) \in \mathbb{N} \times \mathbb{N} : x \equiv 5 \pmod{y}\} \subset \mathbb{N} \times \mathbb{N}$. *Is* C *a function?*

Definition 4.2.132

Let $f : A \to B$. We write $y = f(x)$ when $(x,y) \in f$. We say that y is the **value** of f at x (or the **image** of f at x) and that x is the **pre-image** of y under f.

Definition 4.2.133

Consider a function $f : A \to B$. The set A is called the **domain** of f and is denoted $\mathrm{Dom}(f)$. The set B is called the **codomain** of f and is denoted $\mathrm{Codom}(f)$. The **range** of f is the set $\{f(a) : a \in A\}$. We denote the range by $\mathrm{Rng}(f)$.

The **range** is the set of objects that are actually used as second coordinates. It follows immediately from the definition that $\mathrm{Rng}(f) \subseteq \mathrm{Codom}(f)$. However, it is possibly that the range of f is a proper subset of the codomain.

Question 201.

Let $X = \{a,b,c,x,y,z\}$ *and* $Y = \{1,2,3,4,5,6,7,8,9\}$. *Define a function* $f : X \to Y$ *to be:*

$$f = \{(a,2),(b,3),(c,7),(x,9),(y,4),(z,8)\}.$$

Define a function $g : Y \to X$ *to be:*

$$g = \{(1,b),(2,c),(3,b),(4,a),(5,z),(6,z),(7,b),(8,x),(9,y)\}.$$

Determine the following:

(a) The range of f.

(b) The range of g.

Question 202.

Consider $f = \{(x,y) : x \in \mathbb{N}$ *and* $x + y = 5\}$. *Write out some elements of* f. *What are the domain and range of* f*?*

Question 203.

Consider the relation $C = \{(x,y) \in \mathbb{R} \times \mathbb{R} : x^2 + y^2 = 1\}$. *Is* C *also a function?*

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

Example 4.2.134

Figure 4.3 depicts a bubble diagram for a function from domain $X = \{a, b, c, d\}$ to codomain $Y = \{1, 2, 3, 4\}$. In this case, the range is equal to $\{1, 2, 4\}$.

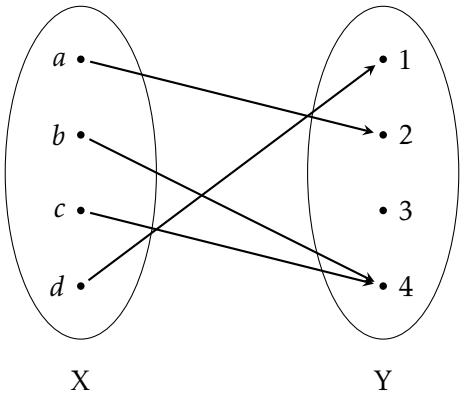


Figure 4.3: An example of a bubble diagram for a function.

■ **Question 204.** □

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

■ **Question 205.** □

There are eight different functions $f : \{a, b, c\} \to \{0, 1\}$. List them all by drawing bubble diagrams.

Functions whose domains and codomains are subsets of $\mathbb{R}$ are often called *real functions*. The domain of a real function is understood to be the largest possible subset of $\mathbb{R}$.

■ **Question 206.** □

What is the domain of the real function $f(x) = \sqrt{3 - x}$?

Because functions are also sets of ordered pairs (like relations), we can say that f and g are **equal** if and only if $f \subseteq g$ and $g \subseteq f$.

Definition 4.2.135

Two functions $f : A \to B$ and $g : A \to D$ are **equal** if $f = g$ (as sets).

Notice also that the **domains** of two equal functions must be the same. We characterize equality in an equivalent manner below:

Theorem 4.2.136

Two functions f and g are equal if and only if

(a) $\mathrm{Dom}(f) = \mathrm{Dom}(g)$ *and*

(b) *for all* $x \in \mathrm{Dom}(f)$, $f(x) = g(x)$

■ **Question 207.** □

Consider the real functions:

$$f(x) = \frac{x^2 - 4}{x - 2}; \quad g(x) = x + 2.$$

Are these functions equal?

4.2.2 Injective and Surjective Functions

Definition 4.2.137

A function $f : A \to B$ is a **surjection** (or is **surjective**, or is **onto** B) if and only if for every $b \in B$ there exists an $a \in A$ such that $f(a) = b$.

In other words, a function $f : A \to B$ is said to be **onto** its codomain when $\mathrm{Rng}(f) = B$.

■ **Question 208.** □

*Re-write the definition of **surjective** using quantifier symbols (the $\forall$ and $\exists$ symbols).*

You are likely familiar with the words **one-to-one** from Calculus when discussing invertible functions. Here we give a formal definition.

Definition 4.2.138

A function $f : A \to B$ is an **injection** (or is **injective**, or is **one-to-one**) if and only if whenever $x \neq y$ then $f(x) \neq f(y)$.

Note: When trying to show a function is one-to-one, we typically prove the contrapositive: if $f(x) = f(y)$, then $x = y$.

Question 209.

*Re-write the definition of **injective** using quantifier symbols.*

Question 210.

Determine if the following functions are injective and/or surjective.

(a) $f : \mathbb{Z} \to \mathbb{Z}$, $f(x) = x^2$

(b) $g : \mathbb{N} \to \mathbb{N} \times \mathbb{N}$, $g(n) = (n+1, 2n)$

(c) $\mathrm{F} : \mathscr{P}(\mathbb{Z}) \to \mathscr{P}(\mathbb{Z})$, $\mathrm{F}(\mathrm{X}) = \overline{\mathrm{X}}$

(d) $h : \mathbb{Z} \to \{0, 1\}$, $h(x) = \begin{cases} 0 & x \text{ is even} \\ 1 & x \text{ is odd} \end{cases}$

Functions that satisfy being both injective and surjective have a special name.

Definition 4.2.139

A function $f : A \to B$ is a **bijection** if it is both injective and surjective.

Question 211.

For each item below, describe a function $f : X \to Y$ satisfying the given requirements. You can use pictures, write out the ordered pairs, give a formula, etc. to describe your functions. Assume the sets X and Y are finite sets (and of course, you can change what X and Y are for each item!).

(a) $f : X \to Y$ *is surjective, but not injective.*

(b) $f : X \to Y$ *is one-to-one, but not onto.*

(c) $f : X \to Y$ *is bijective.*

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

Question 212.

Consider $f : \mathbb{R} - \{2\} \to \mathbb{R} - \{5\}$ *defined by* $f(x) = \dfrac{5x+1}{x-2}$. *Prove that* f *is a bijection, i.e., show that* f *is both injective and surjective. See the example proofs given in Section 12.2 for assistance!*

Question 213. □

Is $g : \mathbb{R}^2 \to \mathbb{R}^2$ defined by $g(x,y) = (xy, x^3)$ surjective? Is it injective? Prove or give a counter-example.

4.2.3 Composition

You likely recall function composition from algebra and Calculus. Composing is an operation unique to functions (over just regular ol' numbers) and is the process of applying one function after another. That is, taking the output of one function and treating it as the input to another function. Notice that this necessarily requires the codomain of the first function to equal the domain of the second.

Definition 4.2.140

Suppose $f : A \to B$ and $g : B \to C$ are functions. The **composition** of f with g is another function, denoted as $g \circ f$ and defined as follows: If $x \in A$, then $g \circ f(x) = g(f(x))$. Therefore, $g \circ f$ sends elements of A to elements of C, so $g \circ f : A \to C$.

Question 214. □

In each case, give examples of finite sets X, Y, and Z, and functions $f : X \to Y$ and $g : Y \to Z$ that satisfy the given conditions. Drawing bubble diagrams is sufficient.

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

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

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

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

Theorem 4.2.141

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

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.

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

Question 215. □

Consider the functions $f : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ defined as $f(m,n) = m + n$ and $g : \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}$ defined as $g(m) = (m,m)$.

(a) Find the formulas for $g \circ f$ and $f \circ g$.

(b) Is the function f surjective? Injective? Provide counter-examples or give a proof.

(c) Is the function g surjective? Injective? Provide counter-examples or give a proof. [ii]

4.2.4 Inverse Functions

Definition 4.2.142

If R is a relation from A to B, then the **inverse** of R is the relation

$$R^{-1} = \{(y,x) \ : \ (x,y) \in R\}.$$

Since R is a relation from A to B, then R^{-1} is a relation from B to A. If we have a function $f : A \to B$, then the relation f^{-1} may or may not be a function.

Question 216. □

Let $A = \{1,6,12\}$, $B = \{0,2,4\}$. *Define* $f : A \to B$ *by:*

$$f = \{(1,2),(6,0),(12,4)\}.$$

Then compute f^{-1}.

[ii] Recall: two ordered pairs (a,b) and (x,y) in $\mathbb{Z} \times \mathbb{Z}$ are equal if and only if $a = x$ and $b = y$.

Question 217.

Define $g : \mathrm{A} \to \mathrm{B}$ *as:*

$$g = \{(1,0),(6,0),(12,0)\}.$$

Then compute g^{-1}.

Question 218.

Provide another example of a function $f : \mathrm{A} \to \mathrm{B}$ *such that* f^{-1} *is not a function (a bubble diagram will suffice).*

Question 219.

Provide another example of a function $f : \mathrm{A} \to \mathrm{B}$ *such that* f^{-1} *is a function (a bubble diagram will suffice).*

Theorem 4.2.143

Let $f : \mathrm{A} \to \mathrm{B}$ *be a function. Then the inverse relation* f^{-1} *is a function from* B *to* A *if and only if* f *is bijective.*

Given any set A, we can define an **identity function** $i_{\mathrm{A}} : \mathrm{A} \to \mathrm{A}$ that sends each element of A to itself: $i_{\mathrm{A}}(a) = a$ for all $a \in \mathrm{A}$. You can check that i_{A} is always a bijective function.

These identity functions act like the additive or multiplicative identities of 0 and 1 in our standard arithmetic of integers and real numbers. That is, in $\mathbb{R}$, you know that 2 and $\frac{1}{2}$ are inverses to each other because $2 \cdot \frac{1}{2} = 1$. A similar result holds for bijective functions f via composition and the aptly named inverse function f^{-1}.

Definition 4.2.144

If $f : \mathrm{A} \to \mathrm{B}$ is bijective then its **inverse** is the function $f^{-1} : \mathrm{B} \to \mathrm{A}$. Functions f and f^{-1} satisfy both $f^{-1} \circ f = i_{\mathrm{A}}$ and $f \circ f^{-1} = i_{\mathrm{B}}$.

Let's break down what the above definition says. If $f : \mathrm{A} \to \mathrm{B}$ is a bijective function, then the inverse relation $f^{-1} : \mathrm{B} \to \mathrm{A}$ is a function, and we call it the **inverse** of f. Moreover, the defining property of this inverse function is that composition on either side of f should result in an identity function. That is, for all $a \in \mathrm{A}$, $(f^{-1} \circ f)(a) = a$ and for all $b \in \mathrm{B}$, $(f \circ f^{-1})(b) = b$.

Question 220.

Why do we need to check the composition in both directions?

Let

$$f(x) = 2x \qquad \text{and} \qquad g(x) = \left\lfloor \frac{x}{2} \right\rfloor.$$

Consider both to be functions from $\mathbb{Z}$ to $\mathbb{Z}$. Are f and g inverse functions?

Question 221.

The function $f : \mathbb{R} \to (0, \infty)$ defined as $f(x) = e^{x^3+1}$ is bijective. Find its inverse.

Question 222.

Consider the function $f : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}$ defined by $f(m, n) = (5m + 4n, 4m + 3n)$.

(a) Prove that f is bijective.

(b) Determine f^{-1}.

Chapter 5 | Cardinalities

§5.1 Sets with Equal Cardinalities

We begin with a discussion of what it means for two sets to have the same cardinality. If both sets are finite, this is just a simple matter of counting up all the elements. But what if both sets are infinite? In that case, we need a new approach to define what it means to have the same cardinality.

Definition 5.1.145

Let A and B be sets (finite or infinite). We say that the set A and B have the same cardinality, if either A and B are both empty or there exists a bijection from the set A onto the set B. We denote this by writing $|A| = |B|$.

Two sets having the same cardinality are also referred to as **equinumerous** sets and the property is called **equinumerosity**.

Warning: The definition does not tell us how to define cardinality of a set A. It only defines an equivalence relation as we will see below.

We now define what it means to be a finite set using the notion of equinumerosity. If we use the notation $\mathbb{N}_k$ to denote the set

$$\mathbb{N}_k = \{1, 2, 3, \ldots, k\}$$

then we can define a set to be **finite** iff either $A = \emptyset$ or $|A| = |\mathbb{N}_k|$. In the second case, we write $|A| = k$. If a set A is not finite, we say that it is **infinite**.

Question 223.

*Which of the following pair of sets have equal cardinality? When answering this question, make sure you can either **prove** the existence of a bijection or **prove** that one cannot be found.*

(a) $\{a, b, c\}$ *and* $\{0, 1\}$.

(b) $\{1, 2, 3\}$ *and* $\{50, 60, 70\}$.

Question 224.

Let A *and* B *be finite sets and let* $f : A \to B$ *be a function. Justify the following statements.*

(a) If f *is injective, then* $|A| \leq |B|$.

(b) If f *is surjective,* $|A| \geq |B|$.

(c) If f *is bijective, then* $|A| = |B|$.

If f is a bijection from A to B, then by theorem 143, f^{-1} is a bijection from B to A. Either one of these functions can be utilized to prove that $|A| = |B|$. This idea is worth keeping in mind as you tackle problems in this chapter. In particular, you might have an easier time creating a bijection between two sets in one direction over the other. This is often a limitation of the human mind as to opposed to some fundamental mathematical difficulty.

The following example illustrates an important distinction between finite sets and infinite sets, namely infinite sets can be in bijection with proper subsets of themselves!

Example 5.1.146

Define $f : \mathbb{Z} \to 6\mathbb{Z}$ via $f(n) = 6n$. It is easily verified that f is both injective and surjective, and hence $|\mathbb{Z}| = |6\mathbb{Z}|$. We could also utilize the inverse function $f^{-1} : 6\mathbb{Z} \to \mathbb{Z}$ given by $f^{-1}(n) = \frac{1}{6}n$ to show that $\mathbb{Z}$ and $6\mathbb{Z}$ have the same cardinality.

Question 225.

□

Define a function $f : \mathbb{N} \to \mathbb{Z}$ as follows:

$$f(n) = \begin{cases} 0 & \text{if } n = 1 \\ -k & \text{if } n = 2k+1 \\ k & \text{if } n = 2k \end{cases}$$

Check that f is a bijection.

The above exercise proves that $|\mathbb{N}| = |\mathbb{Z}|$. This might seem surprising--or it might be what you thought all along. I mean, after all, isn't infinity the same as infinity? On the other hand, $\mathbb{N} \subset \mathbb{Z}$, so $\mathbb{Z}$ definitely has all the elements of $\mathbb{N}$ and more! Fortunately, the way we have defined equal cardinality settles the issue.

Question 226.

Prove that $f(t) = \dfrac{1}{1+e^{-t}}$ *is a bijection from* $\mathbb{R}$ *to* $(0,1)$.

□

So there are exactly as many real numbers between 0 and 1 as there are on the entire number line!

Question 227.

Given two real number intervals (a,b) *and* (c,d)*, prove that* $|(a,b)| = |(c,d)|$.

□

Question 228.

If A *is a set, do* A *and* $\mathrm{A} \times \{x\}$ *have the same cardinality? Justify your answer.*

□

Our first theorem concerning cardinality will likely not come as a surprise.

Theorem 5.1.147

Let A, B, *and* C *be sets.*

(a) $|A| = |A|$.

(b) *If* $|A| = |B|$, *then* $|B| = |A|$.

(c) *If* $|A| = |B|$ *and* $|B| = |C|$, *then* $|A| = |C|$.

In other words, if $\mathscr{U}$ *is the universal set, then equinumerosity is an equivalence relation on* $\mathscr{P}(\mathscr{U})$.

The examples from the last page might (wrongly) lead you to guess that all infinite sets have equal cardinality. However, this is not true as we will show below. The following argument is due to the famous Mathematician Cantor, and is known as **Cantor's diagonalization argument.**

Theorem 5.1.148

$\mathbb{N}$ *and* $(0,1)$ *are* ***not*** *equinumerous. In other words,* $|\mathbb{N}| \neq |(0,1)|$.

Proof of theorem 148.

We will prove the claim by showing that there does not exists a surjection from $\mathbb{N}$ to $(0,1)$. So let $f : \mathbb{N} \to (0,1)$ be an arbitrary function. Consider the sequence of values $\{f(n)\}_{n\in\mathbb{N}}$ written in their standard[a] decimal forms as follows.

$$\begin{aligned}
f(1) &= 0.a_{11}a_{12}a_{13}a_{14}a_{15}\dots \\
f(2) &= 0.a_{21}a_{22}a_{23}a_{24}a_{25}\dots \\
f(3) &= 0.a_{31}a_{32}a_{33}a_{34}a_{35}\dots \\
f(4) &= 0.a_{41}a_{42}a_{43}a_{44}a_{45}\dots \\
f(5) &= 0.a_{51}a_{52}a_{53}a_{54}a_{55}\dots \\
&\vdots \\
f(n) &= 0.a_{n1}a_{n2}a_{n3}a_{n4}a_{n5}\dots
\end{aligned}$$

here the number a_{ij} is the j-th digit to the right of the decimal point in the decimal representation of $f(i)$. We will now construct a real number $b = 0.b_1b_2b_3b_4b_5\dots$ as follows

$$b_k = \begin{cases} 1 \text{ if } a_{kk} \neq 1 \\ 2 \text{ if } a_{kk} = 1 \end{cases}$$

Now for each $n \in \mathbb{N}$, the number b and $f(n)$ differ in the nth decimal place. Therefore, b is not in $\mathrm{Rng}(f)$ and so f is not a surjection. This proves that any function from $\mathbb{N}$ to $(0,1)$ is not a surjection and hence, there is no bijection from $\mathbb{N}$ to $(0,1)$.

■

[a] i.e. it does not end with an infinite string of 9's. For example, replace 0.4999999… with 0.50000…. It turns out that every real number can be expressed uniquely in standard decimal form. We will take this fact for granted.

As a consequence, $|\mathbb{N}| \neq |\mathbb{R}|$ since $|\mathbb{R}| = |(0,1)|$. So there are at least two different ''types of infinities''.

§5.2 Countable and Uncountable Sets

The cardinalities of $\mathbb{N}$ and $\mathbb{R}$ have special names. Note that these are not real numbers.

Definition 5.2.149

The cardinality of $\mathbb{N}$ is denoted by the symbol $\aleph_0$ (pronounced *aleph null*).

The cardinality of $\mathbb{R}$ is denoted by the symbol $\mathfrak{c}$ (short for *continuum*).

Definition 5.2.150

A set A is called **countably infinite** (or denumerable) iff $|A| = \aleph_0$.

A is called is **countable** iff it is either finite or countably infinite.

If a set A is infinite and $|A| \neq \aleph_0$, then it is called **uncountable**.

Note that if $|A| = |\mathbb{N}|$, then there exists a bijection $f : \mathbb{N} \to A$. That means the elements of A can be "listed" as $f(1), f(2), f(3), \ldots$. Rewriting $f(i)$ as a_i, we get the following observation

Theorem 5.2.151

A set A is countably infinite if and only if its elements can be arranged in an infinite list $a_1, a_2, a_3, a_4, \ldots$.

■ **Question 229.** □

What do you think about $\mathbb{Q}$? Is it countable or uncountable?[i]

Although we will not prove it here, the following proposition is true.

Proposition 5.2.152

*$\mathbb{R}$ and the **power set of** $\mathbb{N}$ have the same cardinality. In other words, $|\mathbb{R}| = |\mathscr{P}(\mathbb{N})|$.*

We sometimes express this by writing $\mathfrak{c} = 2^{\aleph_0}$. For natural numbers k, we can write $k < 2^k$. Can we similarly write $|\mathbb{N}| < |\mathbb{R}|$? For that we must make sure to properly define what it means to say $|A| < |B|$ for two sets.

Definition 5.2.153

Suppose A and B are sets.

- $|A| = |B|$ means there is a bijection $A \to B$.
- $|A| < |B|$ means there is an injection $A \to B$, but no bijection $A \to B$.
- $|A| \leq |B|$ means there is an injection $A \to B$.

[i] **Hint:** Read page 276-278 in the textbook.

The proof of proposition 152 requires the use of an important theorem called the Schröder-Bernstein theorem that says:

Theorem 5.2.154: Schröder-Bernstein theorem

If A *and* B *are sets such that* $|A| \leq |B|$ *and* $|B| \leq |A|$, *then* $|A| = |B|$.

A proof of theorem 154 can be found in your textbook.

One can easily check that there is a trivial injection from $\mathbb{N}$ to $\mathbb{R}$. We have also shown earlier that $|\mathbb{N}| \neq |\mathbb{R}|$. Thus by using definition 153, we can write $\aleph_0 < \mathfrak{c}$. In fact, one can mimic Cantor's Diagonalization Argument to show that for any set A, we have $|A| < |\mathscr{P}(A)|$.

As a consequence, we have,

$$|\mathbb{N}| < |\mathbb{R}| = |\mathscr{P}(\mathbb{N})| < |\mathscr{P}(\mathscr{P}(\mathbb{N}))| < |\mathscr{P}(\mathscr{P}((\mathscr{P}(\mathbb{N})))| < \dots$$

The main takeaway from this is

Theorem 5.2.155

There are (at least) countably infinitely many infinities.

§5.3 Further Musings on Cardinality and the Continuum Hypothesis

We will finish this chapter (and the course) with some fun musing about axioms! The language of chapter 5 can be used to define a new type of numbers called "cardinal numbers", which are cardinalities of sets. These are not real numbers, and have their own rules for arithmetic! In particular the symbols $+, -, *$ etc. need to be redefined. For example,

$$1 + \aleph_0 \neq \aleph_0 + 1$$

Here's another interesting property about cardinal numbers. First recall that given any two real numbers a and b, exactly one of the following occurs: (1) $a = b$, (2) $a < b$, (3) $a > b$.

Is it true for cardinal numbers, with our new definition of $<$ symbol?

Theorem 5.3.156

For any two cardinal numbers a and b, exactly one of the following occurs: (1) $a = b$, (2) $a < b$, (3) $a > b$.

There has never been any evidence that Cantor was able to prove theorem 156. Zermelo was able to prove it in 1904, but he had to use a new axiom formulated by himself to do so! This was the **Axiom of Choice**.

Axiom 5.3.157: The Axiom of Choice.

For every collection of pairwise disjoint nonempty sets, there exists at least one set that contains exactly one element from each of these nonempty sets.

As it turned out, theorem 156 is true if and only if the Axiom of Choice is true.

For nearly a century after Cantor formulated his theories on infinite sets (around 1880s), mathematicians struggled with the question of whether or not there exists a set A for which

$$\aleph_0 = |\mathbb{N}| < |A| < |\mathbb{R}| = \mathfrak{c}$$

It was commonly suspected that no such set exists, but no one was able to prove or disprove this. The assertion that no such A exists came to be called the continuum hypothesis. More specifically, the **continuum hypothesis** says that $\aleph_1$, the smallest infinite cardinal number bigger than $\aleph_0$ is in fact $\mathfrak{c} = 2^{\aleph_0}$, i.e. there is no set whose cardinality is strictly between that of the natural numbers and that of the real numbers.

Before we resolve the issue of the Continuum hypothesis, we need to talk about Gödel. Nowadays, all of modern set theory and mathematics uses the foundation of ZFC axioms (Zermelo-Fraenkel + Axiom of Choice). But note that the axiom of choice is an axiom because we can neither prove nor disprove it from ZF. So naturally, it was then asked around the beginning of twentieth century whether or not ZFC is **complete**. Here, **complete** roughly means that every statement in the axioms' language, is either provable or disprovable. Indeed, if not ZFC, is there a better list of axioms that is complete?

Gödel conclusively showed in 1931, in one of the biggest upsets of mathematical history, that any formal system of axiom is either incomplete or inconsistent. This means for any formal system of axioms, either there is a paradox (a statement which can be proved to be both true and false at the same time) or there exists a statement that can be neither proved nor disproved. This is known as **Gödel's (first) incompleteness theorem**.

At this point, the discussion regarding the Continuum hypothesis changes track, and people started to suspect that it is in fact independent of ZFC. That indeed turned out to be the case! To clarify, Gödel

proved in 1940 that the existence of a set with intermediate cardinality, can not be proved in standard set theory. On the other hand, Paul Cohen proved in 1963 that the nonexistence of an intermediate-sized set can not be proved in standard set theory either.

Taken together, Gödel and Cohens' results mean that the standard axioms of mathematics (ZFC) cannot ''decide'' whether the continuum hypothesis is true or false, and that no logical conflict can arise from either asserting or denying the continuum hypothesis. In fact, you can choose to treat it as a new axiom. We are free to either accept the result as true or accept it as false, and the two choices lead to different—but equally consistent—mathematical universes.

We will however note that most mathematicians are agnostics on this issue, but tend to prefer the version of set theory in which the continuum hypothesis holds (ZFC+CH). But then of course there are again statements that are independent of ZFC+CH.[ii]

> [iii]''The situation with the continuum hypothesis is a testament to the immense complexity of mathematics. It is a reminder of the importance of rigor and careful, systematic methods of reasoning that only **begins** with the ideas introduced in this'' course.

[ii] see https://en.wikipedia.org/wiki/List_of_statements_independent_of_ZFC.
[iii] Richard H. Hammack. **Book of proof**. Richard Hammack, 2018.

Appendices

§A Definitions in Mathematics

It is difficult to overstate the importance of definitions in mathematics. Definitions play a different role in mathematics than they do in everyday life.

Suppose you give your friend a piece of paper containing the definition of the rarely-used word **rodomontade**. According to the Oxford English Dictionary[iv] (OED) it is:

> A vainglorious brag or boast; an extravagantly boastful, arrogant, or bombastic speech or piece of writing; an arrogant act.

Give your friend some time to study the definition. Then take away the paper. Ten minutes later ask her to define rodomontade. Most likely she will be able to give a reasonably accurate definition. Maybe she'd say something like, ''It is a speech or act or piece of writing created by a pompous or egotistical person who wants to show off how great they are.'' It is unlikely that she will have quoted the OED word-for-word. In everyday English that is fine---you would probably agree that your friend knows the meaning of the rodomontade. This is because most definitions are **descriptive**. They describe the common usage of a word.

Let us take a mathematical example. The OED[v] gives this definition of **continuous**.

> Characterized by continuity; extending in space without interruption of substance; having no interstices or breaks; having its parts in immediate connection; connected, unbroken.

Likewise, we often hear calculus students speak of a continuous function as one whose graph can be drawn ''without picking up the pencil.'' This definition is descriptive. However, as we learned in calculus, the picking-up-the-pencil description is not a perfect description of continuous functions. Indeed, being continuous is specific to each value in the domain of the function. So the definition above is largely imprecise, it is not a mathematical definition.

Mathematical definitions are **prescriptive**. The definition must prescribe the exact and correct meaning of a word. Contrast the OED's descriptive definition of continuous with the definition of continuous found in a real analysis textbook.

> A function $f : A \to \mathbb{R}$ is **continuous at a point** $c \in A$ if, for every $\varepsilon > 0$, there exists a $\delta > 0$ such that
>
> $$|f(x) - f(c)| < \varepsilon \qquad \text{whenever } |x - c| < \delta \text{ (and } x \in A).$$
>
> If f is continuous at every point in the domain A, then we say that f is **continuous on** A.[vi]

In mathematics there is very little freedom in definitions. Mathematics is a deductive theory; it is impossible to state and prove theorems without clear definitions of the mathematical terms. The definition of a term must completely, accurately, and unambiguously describe the term. Each word is chosen very carefully and the order of the words is critical. In the definition of continuity changing ''there exists'' to ''for every,'' changing the orders of quantifiers, changing $<$ to $\leq$ or $>$, or changing $\mathbb{R}$ to $\mathbb{Z}$ would completely change the meaning of the definition.

What does this mean for you, the student? Our recommendation is that at this stage you memorize the definitions word-for-word. It is the safest way to guarantee that you have it correct. As you gain confidence and familiarity with the subject you may be ready to modify the wording. You may want to change ''for

[iv] http://www.oed.com/view/Entry/166837, you can get access through the College of Wooster library if needed.

[v] http://www.oed.com/view/Entry/40280

[vi] This definition is taken from page 109 of Stephen Abbott's **Understanding Analysis**, but the definition would be essentially the same in any modern real analysis textbook.

every'' to ''given any'' or you may want to change $|x - c| < \delta$ to $-\delta < x - c < \delta$ or to ''the distance between x and c is less than δ.''

Of course, memorization is not enough; you must have a conceptual understanding of the term, you must see how the formal definition matches up with your conceptual understanding, and you must know how to work with the definition. It is perhaps with the first of these that descriptive definitions are useful. They are useful for building intuition and for painting the ''big picture.'' Only after days (weeks, months, years?) of experience does one get an intuitive feel for the ε, δ-definition of continuity; most mathematicians have the ''picking-up-the-pencil'' definitions in their head. This is fine as long as we know that it is imperfect, and that when we prove theorems about continuous functions in mathematics we use the mathematical definition.

§B Fancy Mathematical Terms

Here are some important mathematical terms that you will encounter in this course and throughout your mathematical career.

- **Definition** - a precise and unambiguous description of the meaning of a mathematical term. It characterizes the meaning of a word by giving all the properties and only those properties that must be true.
- **Theorem** - a mathematical statement that is proved using rigorous mathematical reasoning. In a mathematical paper, the term theorem is often reserved for the most important results.
- **Lemma** - a minor result whose sole purpose is to help in proving a theorem. It is a stepping stone on the path to proving a theorem. Very occasionally lemmas can take on a life of their own (Zorn's Lemma, Urysohn's Lemma, Burnside's Lemma, Sperner's Lemma).
- **Corollary** - a result in which the (usually short) proof relies heavily on a given theorem (we often say that ''this is a corollary of Theorem A'').
- **Proposition** - a proved and often interesting result, but generally less important than a theorem.
- **Conjecture** - a statement that is unproved, but is believed to be true (Collatz Conjecture, Goldbach Conjecture, Twin prime Conjecture).
- **Claim** - an assertion that is then proved. It is often used like an informal lemma.
- **Axiom/Postulate** - a statement that is assumed to be true without proof. These are the basic building blocks from which all theorems are proved (Euclid's five postulates, axioms of ZFC, Peano axioms).
- **Identity** - a mathematical expression giving the equality of two (often variable) quantities (trigonometric identities, Euler's identity).
- **Paradox** - a statement that can be shown, using a given set of axioms and definitions, to be both true and false. Paradoxes are often used to show the inconsistencies in a flawed axiomatic theory (e.g., Russell's Paradox). The term paradox is also used informally to describe a surprising or counterintuitive result that follows from a given set of rules (Banach-Tarski Paradox, Alabama Paradox, Gabriel's Horn).

§C Mathematical Writing Practices

Adapted from: *Writing in Mathematics* by Annalisa Crannell, *Foundations of Mathematics* lecture notes by Dana Earnst

C.1 Why do we care about writing in a Math class?

For most of your life so far, the only kind of writing you've done in math classes has been on homeworks and tests, and for most of your life you've explained your work to people that know more mathematics than you do (that is, to your teachers). But soon, this will change. Now that you are taking a 'Proof' course, you know far more mathematics than the average American has ever learned - indeed, you know more mathematics than most college graduates remember. With each additional mathematics course you take, you further distance yourself from the average person on the street. You may feel like the mathematics you can do is simple and obvious (doesn't everybody know what a function is?), but you can be sure that other people find it bewilderingly complex. It becomes increasingly important, therefore, that you can explain what you're doing to others that might be interested: your parents, your boss, the media.

Nor are mathematics and writing far-removed from one another. Professional mathematicians spend most of their time writing: communicating with colleagues, applying for grants, publishing papers, writing memos and syllabi. Writing well is extremely important to mathematicians, since poor writers have a hard time getting published, getting attention from the Deans, and obtaining funding. It is ironic but true that most mathematicians spend more time writing than they spend doing math.

But most of all, one of the simplest reasons for writing in a math class is that writing helps you to learn mathematics better. By explaining a difficult concept to other people, you end up explaining it to yourself.

C.2 How is Mathematical Writing different from what you've done so far?

A good mathematical essay has a fairly standard format. We tend to start solving a problem by first explaining what the problem is, often trying to convince others that it's an interesting or worthwhile problem to solve. On your homeworks, you've usually just said,''Problem 9(a)'' and then plunged ahead; but in your formal writing, you'll have to take much greater pains.

After stating what the problem is, we usually then state the answer, even before we show how we got it. Sometimes we even state the answer right along with the problem. It's uncommon, although not so uncommon as to be exceptional, to read a math paper in which the answer is left for the very end. Explaining the solution and then the answer is usually reserved for cases where the solution technique is even more interesting than the answer, or when the writers want to leave the readers in suspense. But if the solution is messy or boring, then it's typically best to hook the readers with the answer before they get bogged down in details.

Math is difficult enough that the writing around it should be simple. 'Beautiful' math papers are the ones that are the easiest to read: clear explanations, uncluttered expositions on the page, well-organized presentation. For that reason, mathematical writing is not a creative endeavor the same way that, say, poetry is: you shouldn't be spending a lot of time looking for the perfect word, but rather should be developing the most clear exposition. Unlike humanities students, mathematicians don't have to worry about over-using 'trite' phrases in mathematics. In fact, at the end of this document are a list of trite but useful phrases that you may want to use in your papers, either in this class or in the future.

This guide, together with the checklist, should serve as a reference while you write and will also be referred to when I comment on your writing throughout the semester. If you can master these basic areas, your writing may not be spectacular, but it should be clear and easy to read - which is the goal of mathematical writing, after all.

C.3 Guidelines

(a) **The burden of communication lies on you, not on your reader.** It is your job to explain your thoughts; it is not your reader's job to guess them from a few hints. You are trying to convince a skeptical reader who doesn't believe you, so you need to argue with airtight logic in crystal clear language; otherwise the reader will continue to doubt. If you didn't write something on the paper, then (a) you didn't communicate it, (b) the reader didn't learn it, and (c) the grader has to assume you didn't know it in the first place.

(b) **Tell the reader what you're proving.** The reader doesn't necessarily know or remember what "Theorem 2.13" is. Even a professor grading a stack of papers might lose track from time to time. Therefore, the statement you are proving should be on the same page as the beginning of your proof. For an exam this won't be a problem, of course, but on your homework, recopy the claim you are proving. This has the additional advantage that when you study for exams by reviewing your homework, you won't have to flip back in the notes/textbook to know what you were proving.

(c) **Clearly state the assumptions or hypothesis which underlie the formulas.** Sometimes the formula or theorems are straightforward and don't have any assumptions or hypothesis, but not often. For example, if you are planning to use mean value theorem, you must first demonstrate the continuity and differentiability of the function (not that we will need it for this class).

(d) **Use English words.** Although there will usually be equations or mathematical statements in your proofs, use English sentences to connect them and display their logical relationships. If you look in your notes/textbook, you'll see that each proof consists mostly of English words.

(e) **Use complete sentences.** If you wrote a history essay in sentence fragments, the reader would not understand what you meant; likewise in mathematics you must use complete sentences, with verbs, to convey your logical train of thought.

Some complete sentences can be written purely in mathematical symbols, such as equations (e.g., $a^3 = b^{-1}$), inequalities (e.g., $x < 5$), and other relations (like $5 \mid 10$ or $7 \in \mathbb{Z}$). These statements usually express a relationship between two mathematical **objects**, like numbers or sets.

However, it is considered bad style to begin a sentence with symbols. Some common phrases to use to avoid starting a sentence with mathematical symbols are "We see that..." or "We observe that..." or "It follows that..."

You can also often accomplish this by simple rewording: instead of writing "$3n+7$ is even because n is odd," write "Since n is odd, $3n+7$ is even."

(f) **Show the logical connections among your sentences.** Use phrases like "Therefore" or "because" or "if..., then..." or "if and only if" to connect your sentences.

(g) **Know the difference between statements and objects.** A mathematical object is a **thing**, a noun, such as a group, an element, a vector space, a number, an ordered pair, etc. Objects either exist or don't exist. Statements, on the other hand, are mathematical **sentences**: they can be true or false.

When you see or write a cluster of math symbols, be sure you know whether it's an object (e.g., "$x^2 + 3$") or a statement (e.g., "$x^2 + 3 < 7$"). One way to tell is that every mathematical statement includes a verb, such as $=$, $\leq$, "divides", etc.

(h) **The symbol "=" means "equals".** Don't write A = B unless you mean that A actually equals B. This rule seems obvious, but there is a great temptation to be sloppy. In calculus, for example, some people might write $f(x) = x^2 = 2x$ (which is false), when they really mean that "if $f(x) = x^2$, then $f'(x) = 2x$."

(i) **Don't interchange = and $\Longrightarrow$.** The equals sign connects two **objects**, as in "$x^2 = b$"; the symbol

"$\implies$" is an abbreviation for "implies" and connects two **statements**, as in "$a+b=a \implies b=0$." You should avoid using $\implies$ in your formal write-ups.

(j) **Avoid logical symbols in your proofs.** Similar to $\implies$, you should avoid using the logical symbols $\forall, \exists, \vee, \wedge$, and $\iff$ in your formal write-ups. These symbols are useful for abbreviating in your scratch work.

(k) **Say exactly what you mean.** Just as $=$ is sometimes abused, so too people sometimes write $A \in B$ when they mean $A \subseteq B$, or write $a_{ij} \in A$ when they mean that a_{ij} is an entry in matrix A. Mathematics is a very precise language, and there is a way to say exactly what you mean; find it and use it.

(l) **Don't write anything unproven.** Every statement on your paper should be something you **know** to be true. The reader expects your proof to be a series of statements, each proven by the statements that came before it. If you ever need to write something you don't yet know is true, you **must** preface it with words like "assume," "suppose," or "if" (if you are temporarily assuming it), or with words like "we need to show that" or "we claim that" (if it is your goal). Otherwise the reader will think they have missed part of your proof.

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

(n) **Don't write the proof backwards.** Beginning students often attempt to write "proofs" like the following, which attempts to prove that $\tan^2(x) = \sec^2(x) - 1$:

$$\begin{aligned}
\tan^2(x) &= \sec^2(x) - 1 \\
\left(\frac{\sin(x)}{\cos(x)}\right)^2 &= \frac{1}{\cos^2(x)} - 1 \\
\frac{\sin^2(x)}{\cos^2(x)} &= \frac{1-\cos^2(x)}{\cos^2(x)} \\
\sin^2(x) &= 1 - \cos^2(x) \\
\sin^2(x) + \cos^2(x) &= 1 \\
1 &= 1
\end{aligned}$$

Notice what has happened here: the student **started** with the conclusion, and deduced the true statement "$1 = 1$." In other words, they have proved "If $\tan^2(x) = \sec^2(x) - 1$, then $1 = 1$," which is true but highly uninteresting.

Now this isn't a bad way of **finding** a proof. Working backwards from your goal often is a good strategy **on your scratch paper**, but when it's time to **write** your proof, you have to start with the hypotheses and work to the conclusion.

Here is an example of a suitable proof for the desired result, where each expression follows from the

one immediately proceeding it:

$$\begin{aligned}\sec^2(x) - 1 &= \frac{1}{\cos^2(x)} - 1 \\ &= \frac{1 - \cos^2(x)}{\cos^2(x)} \\ &= \frac{\sin^2(x)}{\cos^2(x)} \\ &= \left(\frac{\sin(x)}{\cos(x)}\right)^2 \\ &= (\tan(x))^2 \\ &= \tan^2(x).\end{aligned}$$

(o) **Write strings of equalities (or inequalities) in the proper order.** When your reader sees something like

$$A = B \leq C = D,$$

they expect to understand easily why $A = B$, why $B \leq C$, and why $C = D$, and they expect the **point** of the entire line to be the more complicated fact that $A \leq D$. For example, if you were computing the distance d of the point $(12, 5)$ from the origin, you could write

$$d = \sqrt{12^2 + 5^2} = 13.$$

In this string of equalities, the first equals sign is true by the Pythagorean theorem, the second is just arithmetic, and the **point** is that the first item equals the last item: $d = 13$.

A common error is to write strings of equations in the wrong order. For example, if you were to write "$\sqrt{12^2 + 5^2} = 13 = d$", your reader would understand the first equals sign, would be baffled as to how we know $d = 13$, and would be utterly perplexed as to why you wanted or needed to go through 13 to prove that $\sqrt{12^2 + 5^2} = d$.

(p) **Be concise.** Most students err by writing their proofs too short, so that the reader can't understand their logic. It is nevertheless quite possible to be too wordy, and if you find yourself writing a full-page essay, it's probably because you don't really have a proof, but just an intuition. When you find a way to turn that intuition into a formal proof, it will be much shorter.

(q) **Introduce every symbol you use.** If you use the letter "k," the reader should know exactly what k is. Good phrases for introducing symbols include "Let $n \in \mathbb{N}$," "Let k be the least integer such that...," "For every real number a...," and "Suppose that X is a counterexample."

(r) **Use appropriate quantifiers (once).** When you introduce a variable $x \in S$, it must be clear to your reader whether you mean "for all $x \in S$" or just "for some $x \in S$." If you just say something like "$y = x^2$ where $x \in S$," the word "where" doesn't indicate whether you mean "for all" or "some".

Phrases indicating the quantifier "for all" include "Let $x \in S$"; "for all $x \in S$"; "for every $x \in S$"; "for each $x \in S$"; etc. Phrases indicating the quantifier "some" (or "there exists") include "for some $x \in S$"; "there exists an $x \in S$"; "for a suitable choice of $x \in S$"; etc.

On the other hand, don't introduce a variable more than once! Once you have said "Let $x \in S$," the letter x has its meaning defined. You don't **need** to say "for all $x \in S$" again, and you definitely should **not** say "let $x \in S$" again.

(s) **Use a symbol to mean only one thing.** Once you use the letter x once, its meaning is fixed for the duration of your proof. You cannot use x to mean anything else.

(t) **Write "Let $x = \ldots$," not "Let $\cdots = x$."** When you have an existing expression, say a^2, and you want to give it a new, simpler name like b, you should write "Let $b = a^2$," which means, "Let the new symbol b mean a^2." This convention makes it clear to the reader that b is the brand-new symbol (i.e. we are defining b) and a^2 is the old expression they already understand.

If you were to write it backwards, saying "Let $a^2 = b$," then your startled reader would ask, "What if $a^2 \neq b$?"

(u) **Don't "prove by example."** Most problems ask you to prove that something is true "for all"---You **cannot** prove this by giving a single example, or even a hundred. Your answer will need to be a logical argument that holds for **every example there possibly could be**.

On the other hand, if the claim that you are trying to prove involves the existence of a mathematical object with a particular property, then providing a specific example is sufficient.

(v) **Make your counterexamples concrete and specific.** Proofs need to be entirely general, but counterexamples should be absolutely concrete. When you provide an example or counterexample, make it as specific as possible. For a set, for example, you must name its elements, and for a function you must give its rule. Do not say things like "a counterexample is $x = 2k$ for some $k \in \mathbb{Z}$"; instead, provide an actual even number, e.g. $x = 8$ that works as your counterexample.

(w) **Don't include examples in proofs.** Including an example very rarely adds anything to your proof. If your logic is sound, then it doesn't need an example to back it up. If your logic is bad, a dozen examples won't help it (see rule u). There are only two valid reasons to include an example in a proof: if it is a **counterexample** disproving something, or if you are performing complicated manipulations in a general setting and the example is just to help the reader understand what you are saying.

(x) **Use whitespace.** Don't cram your answer into a few lines of the paper, filled from left margin to right margin. Let your writing breathe! When you start a new thought, start a new line. Use paragraphs to collect your sentences. This helps the reader understand your thought much better, and it also encourages you to be more clear.

(y) **Use scratch paper.** Finding your proof will be a long, potentially messy process, full of false starts and dead ends. Do all that on scratch paper until you find a real proof, and only then break out your clean paper to write your final proof carefully.

Only sentences that actually contribute to your proof should be part of the proof. Do not just perform a "brain dump," throwing everything you know onto the paper before showing the logical steps that prove the conclusion. **That is what scratch paper is for.**

C.4 Good phrases to Use in Math writing:

- Therefore (thus, so, hence, accordingly, it follows that, we see that, then)
- We assume that (assuming, where M stands for)
- We wish to show (demonstrate, prove, explain why, find)
- if (whenever, provided that, when)
- notice that (note , notice, recall, observe)
- since (because)

§D Natural Numbers and the Well-Ordering Principle

D.1 Natural Numbers

How would you define the set of Natural numbers? Informally, this is the set of numbers that you can ''count''. But what does it mean to count? Is there one (or more) property that mathematically 'defines' what it means to be a natural number?

In 1889, an Italian mathematician named Giuseppe Peano put together a list of *axioms* that rigorously defined the natural numbers based on the notion of successors. It goes as follows.[vii]

Definition 0.4.158

Consider a set N together with a function $S : N \to N$ and a certain object called 1. Assume that the set N has the following properties:

(**P1**) $1 \in N$; that is the object 1 is an element of the set N;

(**P2**) if $n \in N$, then $S(n) \in N$;

(**P3**) $S(n) \neq 1$ for every $n \in N$;

(**P4**) if $S(n) = S(m)$, then $m = n$;

(**P5**) if $M \subseteq N$ such that $1 \in M$ and $S(m) \in M$ for every $m \in M$, then $M = N$.[a]

Then the set N is called the set of Natural numbers and is denoted by $\mathbb{N}$.

[a] This is the Principle of Mathematical Induction!

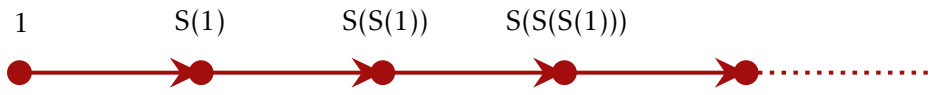
Note: Note that some axioms of Set theory are assumed as prerequisites, at the very least the concept of set itself, the fundamental membership relation '$\in$', and the definition of equality of sets.

The function $S(n)$ is called the successor function. With this language the second Peano axiom says that every natural number has a unique successor $S(n)$ which itself is a natural number.

Question 230. □

Which assumption or axiom gives us the 'unique'-ness of the successor?

We normally represent the natural numbers as dots on a line:[viii]



where each dot is a natural number, and the arrow points from a number to its successor. We also adopt the symbols 2 for S(1), 3 for S(S(1)), 4 for S(S(S(1))), etc.

Each clause of this definition is necessary in order for counting to work. (P1) is obvious, but the others are also necessary. Without the others, we might have ''number lines" that look very different.

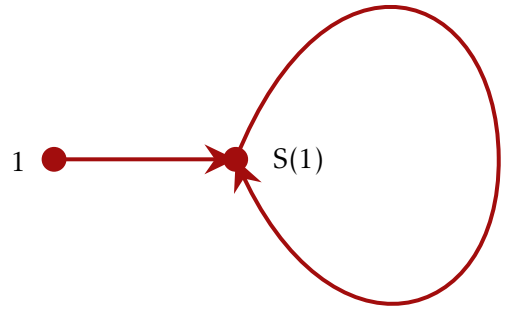
[vii] The original definition includes 0 as a natural number, but now-a-days we do not consider it as such.
[viii] This section taken from lecture notes by Andrew Cooper.

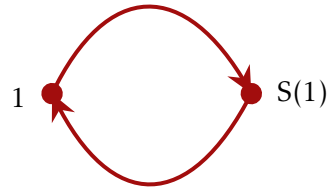
Question 231.

Find a set N *that satisfies axioms* P1, P3, P4, *and* P5 *but not axiom* P2.

Question 232.

Consider two "number line"s that look as follows. Identify which Peano axioms each of the "number lines" above satisfies, and which axioms they do not satisfy.





Question 233.

Challenge Question

Find a set N *that satisfies axioms* P1, P2, P3, *and* P4 *but not axiom* P5.

D.2 The Well-Ordering Principle

The well-ordering principle states the following.

Proposition 0.4.159: The Well-Ordering Principle

Any non-empty set of natural numbers contains a smallest element.

Observe that the WOP is a statement that describes a property of Natural numbers; as such it assumes that the set $\mathbb{N}$ satisfies axioms (P1) through (P5). In this framework, the WOP is a provable theorem that follows from PMI (axiom P5).

Let's see how WOP follows from PMI. We will first need to show that theorem 86 - the Principle of mathematical Induction implies theorem 90 - the Principle of Strong Mathematical Induction (PSMI). However, we will do so from the Peano axioms without any further assumptions about $\mathbb{N}$.

Question 234.

□

Here is an outline for proving that PMI implies PSMI.

(a) First of all, check that proving PSMI is equivalent to proving the following:

$$\begin{aligned} &\text{Given } \mathrm{M} \subseteq \mathbb{N}, \\ &\text{If} \quad (\forall n)[\{k : k < n\} \subseteq \mathrm{M} \implies n \in \mathrm{M}] \\ &\text{Then} \quad \mathrm{M} = \mathbb{N}. \end{aligned}$$

We will try to give a direct proof. What is the antecedent? What is the consequent? Write down the proof structure outline.

(b) Our strategy is as follows: we will prove by PMI that "for every $n \in \mathbb{N}$, the set $\{1, 2, 3, \ldots, n\} \subseteq \mathrm{M}$". This will prove $n \in \mathrm{M}$ for all $n \in \mathbb{N}$.

Check the base case.

(c) What is the induction hypothesis? The induction hyupothesis, along with the antecedent from part (a) should now prove the induction step.

(d) Then by PMI, the claim in part (b) is true. How does the consequent of part (a) follow from this?

Question 235.

□

Next, here is an outline for proving that PSMI implies the WOP. This, together with our above question completes a proof of PMI $\implies$ WOP.

(a) Start off via contradiction: suppose A is a non-empty subset of $\mathbb{N}$ that does not contain a least element. To utilize induction, we define a mathematical statement for each n as follows:

$$\mathrm{S}(n) : n \text{ is not an element of A.}$$

(b) Explain why you know that S(1) is true.

(c) Suppose that you know $\mathrm{S}(1) \wedge \mathrm{S}(2) \wedge \cdots \wedge \mathrm{S}(k)$ is true, for some $k \geq 1$. Explain why you know that $\mathrm{S}(k+1)$ must also be true.

(d) Use Strong Induction to arrive at a contradiction regarding the set A.

Most textbooks claim PMI and WOP to be equivalent axioms. The proof relies on the claim that WOP implies PMI, completing the circular chain. However, there are certain big issues with this claim. We will begin with a correct claim!

Claim 0.4.160

If a set $M \subseteq \mathbb{N}$ *satisfies the WOP, then it satisfies PMI.*

The problem here is that by assumming M to be subset of $\mathbb{N}$, we automatically know that PMI is valid. As such whether or not M satisfies WOP is irrelevant. On the other hand, if you do not assume PMI to be true apriori, how do you define $\mathbb{N}$?

If we are *trying* to show that PMI follows from WOP, we would have to restate WOP as an alternate axiom (P5') in place of (P5):

(P5') Every nonempty subset $M \subseteq N$ has a least element,

and show that PMI can be proved as a theorem starting from these axioms. However, we can easily construct a set N[ix] that satisfies P1, P2, P3, P4, P5' but not P5[x]. This shows that PMI doesn't follow from WOP, if we construct $\mathbb{N}$ using the Peano axioms.

We will conclude this discussion with the comment that this doesn't mean your textbook is wrong! They are simply using some other axiomatic construction of the set $\mathbb{N}$. Indeed in some other axiomatic framework, PMI and WOP are equivalent to each other. See page 31 in your textbook for one such construction.

[ix] Consider $N = \{(0,n) : n \in \mathbb{N}\} \cup \{(1,n) : n \in \mathbb{N}\}$, where the Peano constant 1 is interpreted as the pair $(0,1)$, and the successor function is defined as $S(x,n) := (x, n+1)$ for all $x \in \{0,1\}$ and $n \in \mathbb{N}$. See the Wikipedia page on PMI for a pictorial representation of the 'number line'.

[x] Lars–Daniel Öhman. ''Are Induction and Well-Ordering Equivalent?'' In: **The Mathematical Intelligencer** 41.3 (2019), pp. 33–40. DOI: 10.1007/s00283-019-09898-4.

Exercises

§E Reflection Tasks

E.1 Task 1

Question 1001. □

*Introduce and post something about yourself in the **Social** channel in MS Teams.*

Question 1002. □

Read the syllabus and complete the syllabus quiz.

Question 1003. □

Read the Introduction chapter fully and carefully. Post any question you have to the Teams channel.

E.2 Task 2

Here is a list of blog posts and videos for you read and watch. I am not going to quiz you on them; but I recommend that you go through all of these (takes a total of 30-40 mins excluding the last article) within the first week and before you write about the reflection prompts below.

- The State of Being Stuck | Ben orlin (6 mins read)
- Lessons from My Math Degree That Have Nothing to Do with Math (6 min read)
- Is Mathematics Invented or Discovered? | Roger Penrose (4 mins)
- Videos on Growth Mindset and Productive Failure
  - Grit: the power of passion and perseverance | Angela Lee Duckworth (6 min)
  - What learning looks like (1:46 min)
  - Michael Jordan Failure Commercial (0:32 min)
  - KhanAcademy interview with Carol Dweck about growth mindset (3:06 min)
  - Ira Glass on the Creative Process (1:54 min)
- What is Mathematics? The Most Misunderstood Subject (short article by Dr. Robert H. Lewis, Professor of Mathematics, Fordham University)

Question 1004. □

Answer the following questions.

(a) What are some words you would use to describe mathematics?

(b) What words would you use to describe a typical mathematician?

(c) What do you think it means to be "good at mathematics"?

(d) What does the phrase "doing mathematics" mean to you?

(e) What do you do when you are struggling with a mathematical problem?

(f) When has most of the mathematics we know been developed?

(g) Who are some famous mathematicians? Can you name some contemporary mathematicians? I.e. mathematicians from the 20th or 21st century?

(h) What is your major (if you have declared one already)?

(i) What do you think are the goals for this course?

(j) What concerns, if any, do you have about taking this course?

E.3 Task 3

Note: You are required to type your submission using LaTeX.

Question 1005. □

Read the Foreword, Preface, and any two stories (they aren't too long) from Living Proof (click the link), and then type up responses to the following questions for each story. Be sure to indicate which stories you read.

(a) Did you identify with the author of the story? If so, in what way?

(b) How does the author's experience differ from your own?

(c) What surprised you about the author's story?

(d) Did this story make you think differently about mathematics? I'm expecting more than "yes/no".

(e) What about the story inspires and/or bothers you?

E.4 Task 4

Note: You are required to type your submission using LaTeX.

Question 1006.

We completed chapter 1 last week and our first quiz is coming up soon, so now is a good time to start reviewing your notes, the homework, and the textbook. This task asks you to write a short reflection on your learning so far in the course.

(a) Browsing the textbook, notes, or homework, identify a specific question, example, or exercise that you find or did find confusing. If you can't identify a specific problem, then try to identify a concept or topic that was/is confusing. If you haven't already done so, seek assistance until you better understand the problem.

(b) Write a short essay describing the problem and answering the following questions. What ultimately helped you gain a better understanding of your specific problem? Was it talking to your professor, talking to a peer in class, reading the notes, or something else? How often do you engage in this behavior? Is this something you should do more of? Does this behavior transfer well to your other courses?

Your response should be at least about 250 words in length (about half a page). Full credit will be given to thoughtful, spell-checked responses that follow the standard conventions of English writing and address the questions above.

Question 1007.

*Here's a famous paradox called the **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.

Explain how the above claim is paradoxical in nature and how it can be resolved. Look up the relevant Wikipedia page for an explanation.

E.5 Task 5

> **Note:** You are required to type your submission using LaTeX.

Watch this video by Mike Rugnetta of PBS Idea Channel Five Fallacies.

Rugnetta points out the most common logical fallacies and draws explanations to illustrate how they are committed, why they might seem acceptable, and why they are logical errors.

Question 1008.

Find an advertisement for a product of your choice from YouTube (or any other online source) and write a short (250 words) essay on any logical fallacies you find in it.

You do not have to identify the fallacy by name, since this is not a logic course. Instead, I want to you to identify at least one example of bad faith argument made in the video and write about it. Please be sure to submit a link to the video as well.

§F Weekly Exercises

There are sometimes many valid answers for these problems, so if you are unsure if your solution is correct, you can always ask me or our TA! Please let me know if you notice any errors or typos.

F.1 Chapter 1 Exercises

Question 2001. 2+2+3 points

Write each of the following sets in set-builder notation.

(a) The half open interval of the real line, $[2,4)$.

(b) The set of all multiples of 3*, i.e.* $\{\ldots,-6,-3,0,3,6,9,12,15,\ldots\}$

(c) The Chicken McNugget monoid is a set described as follows. A long time ago, in the UK, chicken nuggets used to only come in packs of 6*,* 9*, or* 20*. We say that a natural number is in the Mcnugget monoid if you can buy exactly that many chicken nuggets by combining different sized packs. For example,* 7 *is not in the Mcnugget monoid because there is no way to buy exactly* 7 *nuggets using a combination of the different pack sizes. Similarly,* 8 *is not in the set, but* 6 *and* 15 *are in the set.*

Write the set using set-builder notation.

Question 2002. 2+2+2+2 points

Write out each of the following sets by listing their elements between braces.

> ***Note:*** $\mathbb{C} := \{a+bi : a,b \in \mathbb{R}\}$ *is the set of* ***complex numbers*** *where* $i := \sqrt{-1}$.

(a) $\{2x : x \in \mathbb{Z} \text{ and } |x| < 4\}$

(b) $\{x \in \mathbb{C} : x^2 + 2 = 0\}$

(c) $\{x \in \mathbb{Z} : |2x| < 4\}$

(d) $\{6a + 2b : a,b \in \mathbb{Z}\}$

Question 2003. 4 points

Given a set X*, a binary operation on the set is a calculation that combines two elements of the set to produce a third object. The set* X *is said to be* ***closed*** *under the binary operation if the resulting object is always an element of the set* X*.*

For example the set $\mathbb{N}$ *is closed under the binary operation of addition* $(+)$ *but not closed under the operation of subtraction* $(-)$*. This is because given two elements* $m,n \in \mathbb{N}$*, the number* $m+n$ *is always a natural number, but* $m-n$ *may not be a natural number.*

Find whether $\mathbb{N},\mathbb{Z},\mathbb{Q}$*, and* $\mathbb{R}$ *are closed under the binary operations of addition, subtraction, multiplication, and division. Make sure to give a counterexample if you think a set is not closed under a certain operation.*

Question 2004. 2+2+3+3 points

Rewrite each of the following statement or open sentence using simple statements or open sentences P*,* Q*,* R *etc. and logical symbols* $\vee, \wedge$*, or* $\sim$*.*

(a) The number x equals zero, but the number y does not.

(b) $x \leq y$.

(c) L_1 and L_2 have the same slope or L_1 and L_2 are vertical lines.

(d) Although 51 divides 153, it is neither a prime nor a divisor of 409.

Question 2005.

3+3+4 points

For (a),(b), and (c) below,

(i) Rewrite the statement in "If P*, then* Q*" form.*

(ii) Write the converse of the statement.

(iii) Write the contrapositive of the statement.

(a) For a function to be integrable, it is necessary that it is continuous.

(b) A geometric series with ratio r converges if $|r| < 1$.

(c) Bakers do not add fat to egg whites, because otherwise the meringue will not form.

Question 2006.

□

Using truth tables, ***prove*** *that the following two compound statements are logically equivalent. You should also explain why your argument counts as a "proof".*

$$(P \Rightarrow Q) \qquad \textit{and} \qquad ((P \wedge \sim Q) \Rightarrow (Q \wedge \sim Q))$$

Please be sure to include some helper columns in your truth tables, as this will help in quickly checking/grading your work.

> **Note:** The logical equivalence above allows us to use a technique of proof known as "proof by contradiction". We will learn more about this in next chapter.

Question 2007.

□

Make two truth tables that prove ***DeMorgan's Laws****:*

$$\sim (P \wedge Q) = (\sim P) \vee (\sim Q)$$

$$\sim (P \vee Q) = (\sim P) \wedge (\sim Q)$$

Be sure to ***give your table(s) a caption*** *of some kind.*

Question 2008.

□

For each of the following statements, either prove that they are logically equivalent or prove that they are not.

(a) $P \Rightarrow (Q \Rightarrow R)$ and $(P \wedge Q) \Rightarrow R$.

(b) $(\sim P) \wedge (P \Rightarrow Q))$ and $\sim (Q \Rightarrow P)$.

Question 2009.

As we have mentioned before, the word 'or' is used in two different ways in English language. In math, 'or' usually means ***inclusive or****, as in "one or the either or both". The* ***exclusive or****, means "one or the either but* ***not*** *both", also has its uses in English, for example, "are you a vegetarian or non-vegetarian?"*[xi]*. We will use the symbol* $\veebar$ *to denote* ***exclusive or****.*

Find a logically equivalent proposition of $P \veebar Q$ *that uses only* $\vee, \wedge$*, and* $\sim$*.*

Question 2010.

For each of the following:

(i) Write it as an English sentence.

(ii) Say whether the sentence is true or false.

(iii) Give a brief explanation for your reasoning in (ii).

(a) $(\forall x \in \mathbb{R})(\exists n \in \mathbb{N})(x^n \geq 3)$

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

(c) $(\exists n, m \in \mathbb{R})(\forall x \in \mathbb{R})(\text{either } x < n \text{ or } x > m)$

Question 2011.

Translate these sentences into symbolic logic. The universe is specified in parentheses if needed.

(a) The cube root of every positive real number is positive. ($\mathscr{U} = \mathbb{R}$)

(b) All that glisters is not gold. ($\mathscr{U}$ = all metals)

(c) For every integer x, there exists an integer y such that $x^2 = y$. ($\mathscr{U} = \mathbb{Z}$)

(d) If the derivative of f is always zero, then f is constant. (choose an appropriate $\mathscr{U}$)

Question 2012.

Negate the given sentence. One possible approach would be to translate the sentence into logic symbols, negate the statement with symbols, then translate back to words.

(a) Every integer can be written as a product of primes.

(b) If $f'(x) = 0$ for all x, then f is a constant function.

(c) There is a real number that is not the root of any nonzero polynomial with integer coefficients.

(d) For every positive number ε, there is a positive number M for which $|f(x) - L| < \varepsilon$ whenever $x > M$.

[xi] If you answered 'Yes' to this question, this is why people think mathematicians are weird.

Question 2013.

Depending on where you took Calculus, you may or may not have seen the formal definition of limit. Regardless, the expression $\lim_{x\to c} f(x) = \mathrm{L}$ *can be written with quantifiers as follows. Here all the numbers are assumed to be real (i.e.* $\mathscr{U} = \mathbb{R}$*).*

$$(\forall \varepsilon > 0)\ (\exists \delta > 0)\ (|x - c| < \delta \Rightarrow |f(x) - \mathrm{L}| < \varepsilon).$$

Write the negation of above statement symbolically and translate that to words. (i.e. what it means to say $\lim_{x\to c} f(x) \neq \mathrm{L}$*).*

Question 2014.

This is an Exploration Activity. You can freely use online or other resources to look up the answers.

(a) Find the five axioms of Euclidean Geometry from Wikipedia (or other sources) and write them down.

(b) We will focus on the fifth axiom, called the 'Parallel Postulate'. Consider the following scenario. Since the axioms can neither be proved or disproved, one can conceivably assume that the fifth postulate is, in fact, incorrect! Indeed there are whole branches of Geometry, called non-Euclidean geometries that assume the 5th postulate to be wrong.

Find at least two different types of non-Euclidean geometry and write down explicitly the alternatives of the 'parallel postulate' used to describe them.

F.2 Chapter 2 Exercises

Question 2015.

Determine the greatest common divisor or least common multiple:

(a) $\gcd(120, 720)$

(b) $\gcd(2^n, 2^{n+1})$

(c) $\gcd(a, 0)$, $(a \in \mathbb{Z}$ and $a \neq 0)$

(d) $\operatorname{lcm}(120, 720)$

(e) $\operatorname{lcm}(2^n, 2^{n+1})$

(f) $\operatorname{lcm}(a, 1)$, $(a \in \mathbb{Z}$ and $a \neq 0)$

Question 2016.

This is an Exploration Activity. You can freely use online or other resources to look up the answers.

***Define** the following objects precisely. Remember that your definition cannot be descriptive, it has to be prescriptive.*

(a) a rectangle,

(b) a circle,

(c) a parabola.

Question 2017.

Prove that if x and y are odd, then xy is odd.

Question 2018.

Prove that if $x \in \mathbb{R}$ *and* $0 < x < 6$*, then* $\dfrac{9}{x(6-x)} \geq 1$.

HINT: Remember, we start by assuming P is true (i.e. x is a real number and $0 < x < 6$) and then show that Q is true (i.e. $\frac{9}{x(6-x)} \geq 1$). But, for your *scratch-work*, it can often be a good idea to work backwards. So try to start with Q and manipulate the expression backwards until you get a 'simple statement' that is obviously true. After you figure out **what** to do, you start with the 'simple statement' and proceed forward like magic, leaving others to wonder, ''how did you know to do that?"

Note: You may use scratch work to find the proof, but you must rewrite the final proof neatly in the correct order. See page 123 in textbook for some advice and a similar problem.

■ Question 2019. □

Directions: *At least one problem similar to question 2019 will appear in every homework from now on, and in your quizzes. Below, there is a proposed proof of a proposition. However, the proposition may be true or may be false.*

- *If the proposition is false, the proposed proof is, of course, incorrect. In this situation, you are to find the error in the proof and then provide a counterexample showing that the proposition is false.*
- *If the proposition is true, the proposed proof may still be incorrect. In this case, you are to determine why the proof is incorrect and then write a correct proof using the writing guidelines that have been presented in the lecture note.*
- *If the proposition is true and the proof is correct, you are to decide if the proof is well written or not. If it is well written, then you simply must indicate that this is an excellent proof and needs no revision. On the other hand, if the proof is not well written, then you must then revise the proof by writing it according to the guidelines of appendix C.*

(a) ***Proposition.*** *If m is an even integer, then $(5m+4)$ is an even integer.*

Proof. *We see that $5m+4 = 10n+4 = 2(5n+2)$. Therefore, $(5m+4)$ is an even integer.*

(b) ***Proposition.*** *For all real numbers x and y, if $x \neq y, x > 0$, and $y > 0$, then $\frac{x}{y} + \frac{y}{x} > 2$.*

Proof. *Since x and y are positive real numbers, xy is positive and we can multiply both sides of the inequality by xy to obtain*

$$\left(\frac{x}{y} + \frac{y}{x}\right) \cdot xy > 2 \cdot xy$$
$$x^2 + y^2 > 2xy$$

By combining all terms on the left side of the inequality, we see that $x^2 - 2xy + y^2 > 0$ and then by factoring the left side, we obtain $(x-y)^2 > 0$. Since $x \neq y, (x-y) \neq 0$ and so $(x-y)^2 > 0$. This proves that if $x \neq y, x > 0$, and $y > 0$, then $\frac{x}{y} + \frac{y}{x} > 2$.

■ Question 2020. □

Suppose a, b, c, and d are natural numbers. If $a \mid (b-c)$ and $a \mid (c-d)$, then prove that $a \mid (b-d)$.

■ Question 2021. □

For $x \in \mathbb{R}$, we define the function $|x|$, called the absolute value of x, by

$$|x| = \begin{cases} x, & \text{if } x \geq 0 \\ -x, & \text{if } x < 0 \end{cases}$$

Prove that if $|x| < a$, then $-a < x < a$.

[HINT: Use proof by cases.]

Question 2022.

Suppose a is an integer. Prove that if $5 \mid 8a$, then $5 \mid a$.

[HINT: There are lot's of ways to prove this. You can use the unique prime factorization theorem or congruence. You can use proof by contrapositive if you wish.]

Question 2023.

Suppose p and q are real numbers. Prove that, if pq is not rational then at least one of p or q is not rational.

[HINT: Use the definition of rational numbers. Use proof by contrapositive.]

Question 2024.

(a) *Prove the following claim.*

Claim. *If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then $ac \equiv bd \pmod{n}$.*

(b) *Using the claim or otherwise, find a number $0 \leq m < 31$ such that $2^{1023} \equiv m \pmod{31}$. In other words, find the remainder when you divide 2^{1023} by 31.*

Question 2025.

Evaluate all the proofs from section 2.3.9 using the instructions from question 2019.

Question 2026.

> ***Hint:*** *Use proposition 64. What should we choose as a, b, q, r?*

Prove that two consecutive odd numbers are always relatively prime to each other.

Question 2027.

(a) *Let n be an integer. Show that either $n^2 \equiv 0 \pmod{4}$ or $n^2 \equiv 1 \pmod{4}$.*

(b) *Using part (a), or otherwise, show that there do not exist integers m and n such that $n^2 + 2 = m^2$.*

Question 2028.

□

Hint. *Be careful with what the hypothesis is and what the conclusion is in this question.*

Suppose n is a natural number. Prove that if $n, n+2$, and $n+4$ are all prime numbers, then $n = 3$.

Question 2029.

□

Note: *Same instructions as question 2019.*

(a) ***Proposition.*** *For all real numbers x and y, if x is irrational and y is rational, then $x+y$ is irrational.*

Proof. *We will use a proof by contradiction. So we assume that the proposition is false, which means that there exist real numbers x and y where $x \notin \mathbb{Q}, y \in \mathbb{Q}$, and $x+y \in \mathbb{Q}$. Since the rational numbers are closed under subtraction and $x+y$ and y are rational, we see that*

$$(x+y)-y \in \mathbb{Q}$$

However, $(x+y)-y = x$, and hence we can conclude that $x \in \mathbb{Q}$. This is a contradiction to the assumption that $x \notin \mathbb{Q}$. Therefore, the proposition is not false, and we have proven that for all real numbers x and y, if x is irrational and y is rational, then $x+y$ is irrational.

(b) ***Proposition.*** *For each real number $x, x(1-x) \leq \frac{1}{4}$.*

Proof. *A proof by contradiction will be used. So we assume the proposition is false. This means that there exists a real number x such that $x(1-x) > \frac{1}{4}$. If we multiply both sides of this inequality by 4, we obtain $4x(1-x) > 1$. However, if we let $x = 3$, we then see that*

$$\begin{aligned} & 4x(1-x) > 1 \\ \implies & 4 \cdot 3(1-3) > 1 \\ \implies & -12 > 1 \end{aligned}$$

The last inequality is clearly a contradiction and so we have proved the proposition.

Question 2030. The Three Prisoner's Problem

Three prisoners have been sentenced to long terms in prison, but due to overcrowded conditions, one prisoner must be released.

The warden devises a scheme to determine which prisoner is to be released. He tells the prisoners that he will blindfold them and then paint a red dot or a blue dot on each forehead. After he paints the dots, he will remove the blindfolds and a prisoner should raise his hand if he sees a red dot on at least one of the other two prisoners. The first prisoner to identify the color of the dot on his own forehead will be released. Of course, the prisoners agree to this. (What do they have to lose?)

The warden blindfolds the prisoners, as promised, and then paints a dot on the foreheads of all three prisoners. In fact, he paints a red dot on the foreheads of all three prisoners. He removes the blindfolds and, since each prisoner sees a red dot (indeed two red dots), each prisoner raises his hand. Some time passes when one of the prisoners exclaims, ''I know what color my dot is! It's red!'' This prisoner is then released.

How did this prisoner correctly identify the color of the dot painted on his forehead?

Question 2031.

Recall the proof of infinitude of prime numbers that we did in class. Will the proof still work if we instead define $a = (p_1 p_2 \dots p_n) - 1$*? What about* $a = (p_1 p_2 \dots p_n) + 31$*?*

Question 2032.

Prove that the number $\log_3 5$ *is irrational.*

Note that the logarithm here is base 3, not logarithm base 10 or the natural logarithm, which has base e.

Question 2033.

Let $a, b \in \mathbb{Z}$*. Prove that the following are equivalent:*

(a) a *is even.*

(b) $a^3 + a^2 + a$ *is even.*

(c) $4 | a^3$*.*

Question 2034.

Let $a, b \in \mathbb{N}$*. Prove that if* $a + b$ *is even, then there exist nonnegative integers* x *and* y *such that* $x^2 - y^2 = ab$*.*

Question 2035.

Evaluate the following claim and proof according to the instructions from question 2019.

> ***Claim:*** *There exists a unique element* $(x, y) \in \mathbb{R} \times \mathbb{R}$ *such that* $xy = 1$*.*
>
> *Proof.* First, notice that $(2, \frac{1}{2}) \in \mathbb{R} \times \mathbb{R}$ and $(2)(\frac{1}{2}) = 1$. Therefore, there exists $(x, y) \in \mathbb{R} \times \mathbb{R}$ such that $xy = 1$.
> Now to show uniqueness, suppose there exists another element $(x', y) \in \mathbb{R} \times \mathbb{R}$ such that $x'y = 1$. Then $x'y = xy$ and since $xy = 1$, we know that y can not equal zero. Therefore, we can divide both sides by y and conclude that $x = x'$.
> Likewise, if (x, y') satisifes the equation, then $xy' = xy$, and since $x \neq 0$, this implies $y = y'$. Thus, there exists a unique $(x, y) \in \mathbb{R} \times \mathbb{R}$ such that $xy = 1$. ■

Question 2036.

See the attached LaTeX file for instructions on how to answer this question.

(a) Prove Euclid's Lemma from question 107.

(b) Using Euclid's lemma or other wise show that $\sqrt{p}$ *is irrational for any prime number* p*.*

Question 2037.

Prove that for all $n \in \mathbb{N}$*,*

$$1 \cdot 2 + 2 \cdot 3 + 3 \cdot 4 + 4 \cdot 5 + \cdots + n(n+1) = \frac{n(n+1)(n+2)}{3}.$$

Question 2038.

Prove that $9 \mid (4^{3n} + 8)$ *for every integer* $n \geq 0$ *using induction.*

Note that we have learned other ways to prove this, but I am asking you to prove it by induction.

Question 2039.

Let s_n *denote the partial sum of the first* n *terms of the harmonic series*

$$\sum \frac{1}{n} = 1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \dots$$

Show that s_{2^n}*, i.e. the sum of the first* 2^n *terms, is greater than or equal to* $1 + \frac{n}{2}$.

Note that this is the proof of the fact that the harmonic series diverges.

Question 2040.

For the Fibonacci sequence, show that $\sum_{i=1}^{n} F_i^2 = F_n F_{n+1}$.

Question 2041.

Define a sequence $\{a_i\}_{i \in \mathbb{N}}$ *as*

$$a_1 = \sqrt{2}, \quad a_{n+1} = \sqrt{2 + a_n} \quad \text{for } n \geq 1$$

Show that

$$a_n = 2 \cos \frac{\pi}{2^{n+1}} \quad \text{for all } n \in \mathbb{N}.$$

Question 2042.

Answer questions 121 and 122 from the lecture notes.

Question 2043.

Prove that for all $n \in \mathbb{N}$*, we can find a polynomial* $P_n(x)$ *with* ***integer*** *coefficients such that*

$$\cos(nx) = P_n(\cos x).$$

These polynomials are known as Chebyshev polynomials. For example,

$$P_2(x) = 2x^2 - 1$$

because $\cos(2x) = 2\cos^2 x - 1$. Similarly,

$$P_3(x) = 4x^3 - 3x$$

because $\cos(3x) = 4\cos^3 x - 3\cos x$.

There are lots of ways to prove the claim, you can check the Wikipedia page on Chebyshev polynomials. I will outline two proof techniques below. The first one is nonconstructive, it proves the existence, but doesn't give a formula. The second one actually finds out the formula. See if you can follow along and fill in the gaps.

Proof 1 (Sketch). We will use the trigonometric identity

$$\cos(a+b) = \cos a \cos b - \sin a \sin b$$

Use it to prove that

$$\cos((k+1)x) + \cos((k-1)x) = 2\cos(kx)\cos(x)$$

So we can write

$$\cos((k+1)x) = 2\cos(kx)\cos(x) - \cos((k-1)x)$$

Now use use **strong** induction to prove the given claim. ■

Exploration Activity

You get full credit for completing the gaps in the first proof. Here's an alternate proof if you are familiar with complex numbers or binomial expansion. If those words mean something to you, or if you are willing to look those up, keep reading.

Proof 2. We will first prove the following identity known as ''de Moivre's Formula'':

$$(\cos x + i \sin x)^n = \cos(nx) + i \sin(nx)$$

for all $n \in \mathbb{N}$. Here i is the square root of -1. You can show this using induction (show it yourself). You would need to use the trigonometric identities

$$\cos(a+b) = \cos a \cos b - \sin a \sin b$$

and

$$\sin(a+b) = \sin a \cos b + \cos a \sin b.$$

Now, we can write

$$\cos(nx) = \frac{1}{2}(\cos(nx) + i\sin(nx) + \cos(nx) - i\sin(nx)) = \frac{1}{2}((\cos x + i \sin x)^n + (\cos x - i \sin x)^n)$$

So all that remains, is to show that when we expand the sums on the last term, all $\sin x$ terms cancel out or can be replaced with $\cos x$.

We will use the following identity that can be proved using the binomial theorem. Look up the theorem and try to prove the following identity using the theorem.

$$(a+b)^n + (a-b)^n = 2\sum_{k=0}^{n} \binom{n}{2k} a^{n-2k} b^{2k}$$

where $\binom{p}{q} = \frac{p!}{q!(p-q)!}$. We can thus conclude that,

$$\begin{aligned}\cos(nx) &= \sum_{k=0}^{n}\binom{n}{2k}(\cos x)^{n-2k}(i\sin x)^{2k}\\ &= \sum_{k=0}^{n}\binom{n}{2k}(\cos x)^{n-2k}(\sin^2 x)^{k}(-1)^{k}\\ &= \sum_{k=0}^{n}\binom{n}{2k}(\cos x)^{n-2k}(1-\cos^2 x)^{k}(-1)^{k}\end{aligned}$$

which is a polynomial of $\cos x$ with integer coefficients! ■

F.3 Chapter 3 Exercises

Question 2044. □

List the elements of $\{\emptyset\}\times\{0,\emptyset\}\times\{0,1\}$.

Question 2045. □

Sketch the following sets of points in $\mathbb{R}^2$.

(a) $\{(x,y) : x<1, y\in[-1,1]\}$

(b) $\{(x,y) : x\in\mathbb{Z}, y\in\mathbb{R},$ *and* $y<x\}$

(c) $\{(x,x+n) : x\in\mathbb{R}, n\in\mathbb{Z}\}$.

Question 2046. □

Is the following statement True or False? Give a brief justification for your answer.

For ***any*** *two sets* A *and* B, $A\times B\neq B\times A$.

Question 2047. □

Answer the following True or False and if it is False, give a brief justification for why.

(a) $\mathbb{Q}\subseteq\mathbb{Z}$

(b) $\{\mathbb{N}\}\subseteq\{\mathbb{N},\mathbb{R}\}$

(c) $\mathbb{N}\in\mathbb{R}$

(d) $\{\mathbb{N}\}\in\{\{\mathbb{N}\},\mathbb{R}\}$

Question 2048. □

List four elements of $\mathscr{P}(\mathbb{N})$, *two of which are finite sets and two of which are infinite sets.*

Question 2049. □

Translate the following statements to English and determine whether they are true or false (give a proof).

(a) $(\exists n\in\mathbb{N})(\forall X\in\mathscr{P}(\mathbb{N}))(|X|<n)$

(b) $(\forall X \in \mathscr{P}(\mathbb{N}))(\exists n \in \mathbb{N})(|X| < n)$

(c) $(\forall n \in \mathbb{N})(\exists X \in \mathscr{P}(\mathbb{N}))(|X| = n)$

Question 2050.

Let $A = \{a, b, c, d\}$, $B = \{b, e\}$, *and* $C = \{a, e, i, o, u\}$. *Perform the indicated set operation to obtain a new set.*

(a) $B \cup C =$

(b) $A \cap C =$

(c) $B \setminus A =$

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

Question 2051.

Suppose $A = \{0, 1\}$ *and* $B = \{1, 2\}$. *Find the following:*

(a) $\mathscr{P}(A) \cap \mathscr{P}(B)$

(b) $\mathscr{P}(A) \setminus \mathscr{P}(B)$

(c) $\mathscr{P}(A \cap B)$

(d) $\mathscr{P}(A \times B)$

Question 2052.

Sketch the sets $X = [-1, 3] \times [0, 2]$ *and* $Y = [0, 3] \times [1, 4]$ *on the plane* $\mathbb{R}^2$. *On separate drawings, shade in the sets* $X \cup Y$, $X \cap Y$, $X \setminus Y$, *and* $Y \setminus X$.

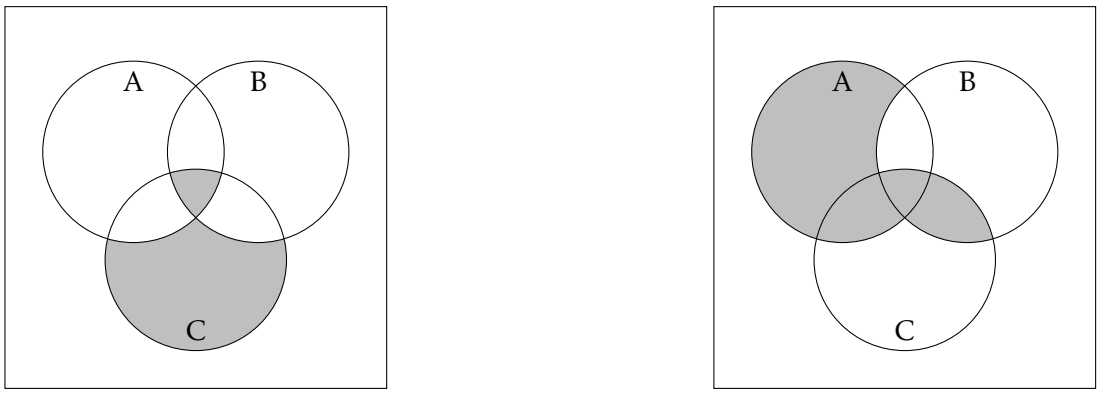
Question 2053.

Prove theorem 96 by induction on n.

Question 2054.

2 + 2 **points**

Write a corresponding expression for the shaded region in the Venn Diagrams in fig. 1 below.



(a) (b)

Figure 1

Question 2055. 2 + 2 points

(a) *Is it true that* $A \cup (B \cap C) = (A \cup B) \cap C$*? Justify your answer by drawing the two corresponding Venn diagrams.*

(b) *Is it true that* $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$*? Justify your answer by drawing the two corresponding Venn diagrams.*

Question 2056. 3 points

Is it true that $(A \cap B) \setminus C = (A \setminus C) \cap B$*? Prove your answer* ***without*** *drawing any Venn diagrams!* [HINT: Write down the definition of the two sets in set-builder notation.]

Question 2057. 3 points

Give example of two nonempty sets A *and* B *such that* $\{A \cup B, A \cap B, A \setminus B, B \setminus A\}$ *is the power set of some set.*

Question 2058. 4 points

Give an example of four sets A_1, A_2, A_3, A_4 *such that* $|A_i \cap A_j| = |i - j|$ *for every two integers* i *and* j *with* $1 \leq i < j \leq 4$.

Question 2059. 3 points

For a set A *with* $|A| = 2$*, what is the largest possible value of* $|A \cap \mathscr{P}(A)|$ *?*

Question 2060. 6 points

Prove or provide a counterexample for each of the following claims.

(a) $\mathscr{P}(A \cap B) = \mathscr{P}(A) \cap \mathscr{P}(B)$.

(b) $\mathscr{P}(A \cup B) = \mathscr{P}(A) \cup \mathscr{P}(B)$.

Question 2061. 4 points

For $a \in \mathbb{N}$*, let* $a\mathbb{Z}$ *denote the set of all integer multiples of* a*. Prove that for all* $a, b \in \mathbb{N}$*,*

$$a = b \text{ if and only if } a\mathbb{Z} = b\mathbb{Z}.$$

Note: The last question is not very trivial. Be careful when arguing the backward implication.

Question 2062. 4 + (2 + 2) points

For each $z \in \mathbb{Z}$*, let* $C_z = [z, z+1) \subseteq \mathbb{R}$.

(a) *Draw a picture representing the sets* C_{-2}, C_0, C_1*, and* C_5.

(b) *Determine* $\bigcup_{z \in \mathbb{Z}} C_z$ *and* $\bigcap_{z \in \mathbb{Z}} C_z$.

Note: Read chapter 1.8 from the textbook before attempting next problem.

Question 2063. 2 + 2 points

Let $I = [0,1]$. *Determine the following:*

(a) $\bigcup_{\alpha \in I} [\alpha, 1] \times [0, \alpha^2]$

(b) $\bigcap_{\alpha \in I} [\alpha, 1] \times [0, \alpha^2]$

Question 2064. 1 + 1 + 2 + 2 points

Let $I = [0,3]$. *For each number* $\alpha \in I$, *let* $A_\alpha = \{(\alpha, x) \in \mathbb{R}^2 : 0 \leq x \leq \alpha\}$. *Draw a picture in* $\mathbb{R}^2$ *depicting the set in each of the following cases.*

(a) A_1

(b) $A_{\sqrt{2}}$

(c) $\bigcap_{\alpha \in I} A_\alpha$

(d) $\bigcup_{\alpha \in I} A_\alpha$

F.4 Chapter 4 and 5 Exercises

Question 2065. 4 points

Draw digraph diagrams for all the different relations on $A = \{a, b, c\}$ *that are both reflexive and symmetric, but* ***not*** *transitive.*

Question 2066. 2 points

Answer question 190.

Question 2067. 6 points

A relation R *is defined on* $\mathbb{Z}$ *by* aRb *if* $3 \mid (a^3 - b)$. *Prove that* R *is an equivalence relation.*

> **Hint:** For symmetric, add $a^3 - b$ and $b^3 - a$. For transitive, add $a^3 - b$ and $b^3 - c$ and use reflexivity.

Question 2068. 4 points

In example 125(b), we established that the relation '$\equiv \pmod n$*', denoted henceforth by* $\equiv_n$, *is an equivalence relation on* $\mathbb{Z}$. *In other words, if* $R = \equiv_n$, *then*

$$R = \{(a, b) \in \mathbb{Z} \times \mathbb{Z} \mid a \equiv b \pmod n\}$$

For this relation, the set of equivalence classes is denoted $\mathbb{Z}_n$. *Formally we will write*

$$\mathbb{Z}_n = \{[0]_n, [1]_n, [2]_n, \ldots, [n-1]_n\}$$

where $[i]_n = \{x \mid x \equiv_n i\}$, *the set of integers that are congruent to* i *modulo* n.

For example, $\mathbb{Z}_4 = \{[0]_4, [1]_4, [2]_4, [3]_4\}$ *where* $[i]_4 = \{4k + i \mid k \in \mathbb{Z}\}$, *the set of numbers that are are congruent to* i *modulo* 4.

Suppose $m, n \geq 2$. *Prove that*

$$\mathbb{Z}_m \cap \mathbb{Z}_n \neq \emptyset \iff m = n.$$

Question 2069. 4 points

Are either of the following sets functions from $\mathbb{Z}$ to $\mathbb{Z}$? If so, what is the domain and range of the function?

(a) $\{(x,y) \in \mathbb{Z}\times\mathbb{Z} : 3x+y=4\}$

(b) $\{(x,y) \in \mathbb{Z}\times\mathbb{Z} : x+3y=4\}$

Question 2070. 2 points

Consider the function $f : \mathbb{Z}\times\mathbb{Z} \to \mathbb{Z}\times\mathbb{Z}$ defined as

$$f((x,y)) = (x+y, x)$$

Find a formula for f^{-1}.

Question 2071. 4 points

Is $g : \mathbb{R}^2 \to \mathbb{R}$ defined by $g(x,y) = -xy + 5y^2$ surjective? Is it injective? Prove each or give a counter-example.

Question 2072. 4 points

Let A, B and C be nonempty sets and let f, g and h be functions such that $f : A \to B, g : B \to C$ and $h : B \to C$. For each of the following, prove or disprove:

(a) *If $g \circ f = h \circ f$, then $g = h$.*

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

Question 2073. 3 points

*A **permutation** of (or on) a nonempty set A is a bijective function from A to A. If $|A| = n$, find the number of permutations on A. Don't forget to justify your answer, a formal proof is unnecessary.*

Question 2074. 4 points

Show that the sets $\{0,1\}\times\mathbb{N}$ and $\mathbb{N}$ are equinumerous.

Question 2075. 3 points

Use one of the P^3 questions to prove that $\mathbb{N}\times\mathbb{N}$ and $\mathbb{N}$ are equinumerous.

> **Note:** Consequently, if $|A| = |\mathbb{N}|$ and $|B| = |\mathbb{N}|$, then $|A \times B| = |\mathbb{N}|$. In other words, this exercise proves that the Cartesian product of two countable sets is countable.

Question 2076. 3 points

Prove that the set of all irrational numbers is uncountable.

> **Hint:** Use theorems 14.4 and 14.6 from the textbook. You may use these without proof.