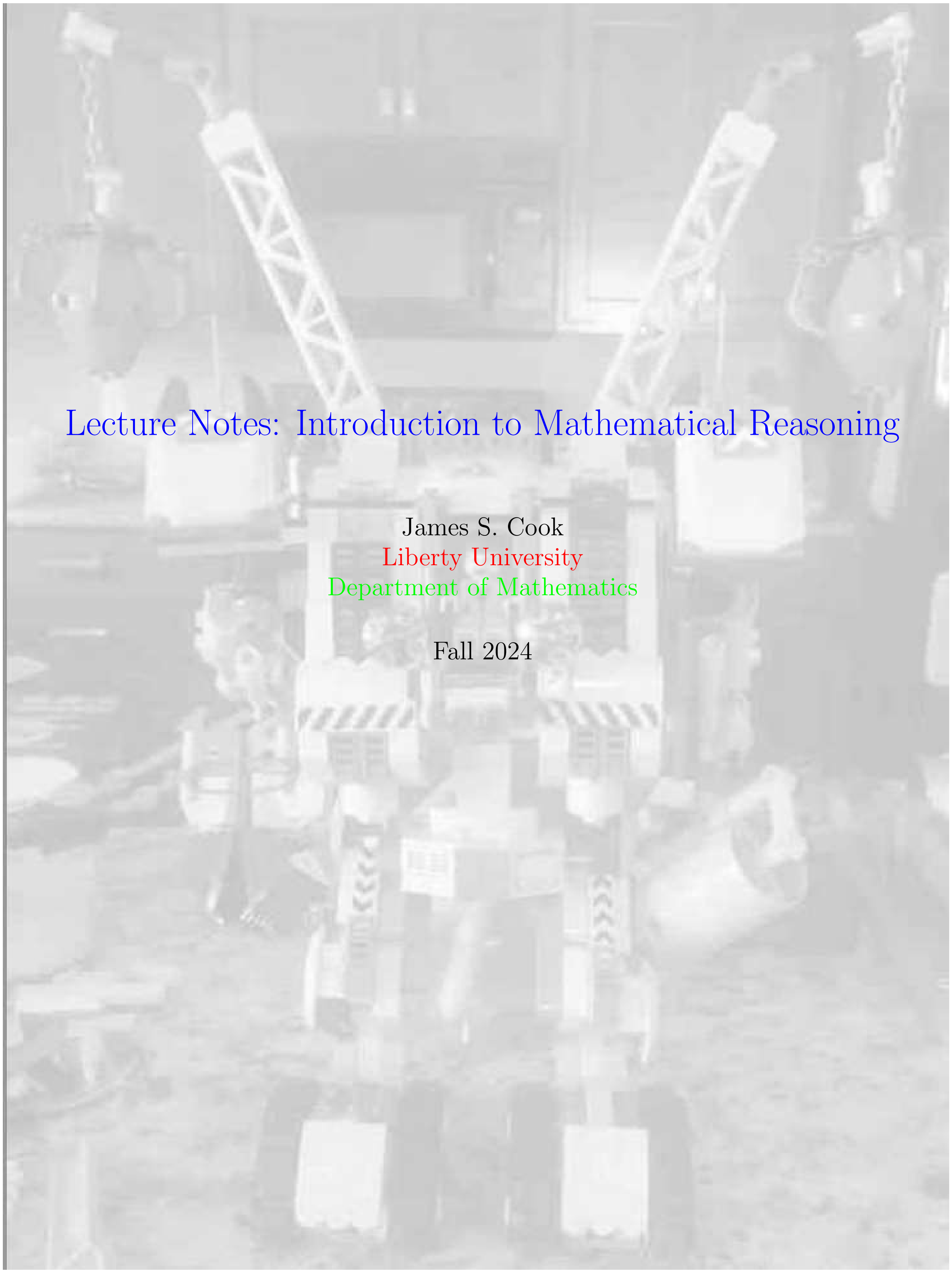


Lecture Notes: Introduction to Mathematical Reasoning

James S. Cook
Liberty University
Department of Mathematics

Fall 2024

preface

These notes are given for Math 200 at Liberty University. I intend to use Robert S. Wolf's *Proof, Logic, and Conjecture: The Mathematician's Toolbox* as a rough guide to the structure of these notes. In particular, I intend to borrow many definitions given in Wolf's text as well as a number of theorems. It is likely I have less discussion than does Wolf, so if you wish for an extended version of these notes then purchasing that text would be wise. In addition, these notes will not have exercises. I'll likely take examples both from Wolf and the text by Chattrand, Polimeni and Zhang.

sources

I should confess, I have borrowed ideas from:

1. *Mathematical Proofs: a Transition to Advanced Mathematics* by Chattrand, Polimeni and Zhang., 4th-edition.

2. *Proof, Logic, and Conjecture: The Mathematician's Toolbox* by Robert S. Wolf

3. *A Transition to Advanced Mathematics*, 4th Edition (probably, I took this course from that textbook circa 2000 and taught it with this book around 2009) by Smith, Eggen and St. Andre.

style guide

I use a few standard conventions throughout these notes. They were prepared with LaTeX which automatically numbers sections and the hyperref package provides links within the pdf copy from the Table of Contents as well as other references made within the body of the text.

I use color and some boxes to set apart some points for convenient reference. In particular,

1. definitions are in green.

2. remarks are in red.

3. theorems, propositions, lemmas and corollaries are in blue.

4. proofs start with a **Proof:** and are concluded with a $\square$.

However, I do make some definitions within the body of the text. As a rule, I try to put what I am defining in **bold**. Doubtless, I have failed to live up to my legalism somewhere. If you keep a list of these transgressions to give me at the end of the course it would be worthwhile for all involved.

The symbol $\square$ indicates that a proof is complete. The symbol $\triangledown$ indicates part of a proof is done, but it continues.

prerequisites

These notes were written for Math 200 of Spring 2025. The course was titled *Introduction to Mathematical Reasoning.* The course covers basic logic, proofs, select elementary number theory topics, proofs from Calculus I or II, equivalence relations and partitions, cardinality. Other topics are possible, but the focus here is on the process of proof and the importance of axioms and definition. This is not a problem solving course. This course is almost entirely about learning how to formulate precise mathematical arguments based firmly on definition, axiom and logical deduction.

I don't claim these notes are self-contained. Far from it. We will assume the existence of rational ($\mathbb{Q}$), real ($\mathbb{R}$), and complex ($\mathbb{C}$) number fields. We will assume the existence of natural numbers ($\mathbb{N} = \{1, 2, \dots\}$) and integers ($\mathbb{Z} = \{0, \pm 1, \pm 2, \dots\}$). Furthermore, set theory will be introduced in the naive fashion. We might discuss the Zermelo Frankel Cantor (ZFC) foundations for set theory, but we will not attempt rigor on that point. In short, I will explain how we understand and prove assertions of set theory in this course in the usual informal manner which is typical of math courses (outside say a foundations of set theory course where you would dig into the nuts and bolts of the ZFC type axiomatics). Similarly, the constructions of $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ etc. are left for another course, we will simply set forth their properties as axiomatic systems and show how theorems flow from such base assumptions. Rest assured the standard number systems can all be constructed using little more than set theory and undergraduate mathematics (but, some of that math you have not learned yet, so I can't very well use it here!).

overview

Chapter 1 covers the basics of logic. We use Chapter 1 in everything. Chapter 2 is a collection of basic definitions and elementary proofs. Chapter 3 introduces set theory formally (although, truth be told, we do assume some previous understanding of set theory). Chapter 4 covers proof by induction. Chapter 5 introduces the concept of a relation and pays special attention to equivalence relations and the correspondence between partitions and equivalence classes. Chapter 6 covers integers and their arithmetic. The division algorithm, Euclidean algorithm and primes are discussed. This lays the foundation for calculation in the modular integers which we denote $\mathbb{Z}_n$. The example of $\mathbb{Z}_n$ usually plays a big role in the abstract algebra course. Chapter 7 covers the theory of functions. We learn how to carefully prove a function is injective or surjective. Images and inverse images of sets are defined and studied. Chapter 8 introduces the concept of cardinality. We learn a little transfinite arithmetic.[1] Chapter 9 covers a collection of analysis topics taken from Calculus I and II as well as a section on the big-O notation due to Landau. What parts of Chapter 9 we cover in lecture depend on the semester and the interest of the students. Finally, Chapter 10 is a survey of algebra, in contrast to Chapter 9, it is almost entirely about things you have not yet seen in all probablility.

The current edition of these notes was finished on January 7, 2025. They are a work in progress, so please let me know by email if you find errors. I will try to add new examples in lecture. There should be something to be gained from studying these notes in parallel to class. Many homework problems arose from unfinished thoughts in this set of notes.

Thanks!
James Cook

[1] you can ask Dr. Sprano about what comes past these notes on transfinite math.

Contents

Chapter 1

Logic

Our goal here is to describe how logical argumentation is commonly made in mathematics. We seek to describe the structure of proofs by using precise logical operations. Unfortunately, some of the words we use have a broader informal meaning in conversational english. Therefore, we must take care to define terms with precision.

The situation is somewhat akin to that found in Theology proper. To understand what a doctrine means we must first understand the meaning of the words used to formulate a doctrine. Theology, unlike mathematics, rests on more than logic. We have special revelation from God which gives us insight into His character. That special revelation, given by Holy Scripture, combined with our God given ability to find conclusions drawn from syllogisms etc. leads us to doctrines which comprise Theology.

God is far more subtle than Mathematics and I would argue there is more room for disagreement on what constitutes proper Theology. In contrast, once we settle the axioms of mathematics, the theorems which comprise mathematics are not a matter of interpretation. However, I would argue, the content of mathematics is a breath taking example of the beauty of God's creation and to my taste one of the most exciting chapters in God's general revelation. Furthermore, the mystery that we can understand it at all, and that mathematics is woven into physics and vice-versa, this testifies to God's providence, indeed the goodness of His creation.

You can also read *Mathematical Proofs: a Transition to Advanced Mathematics* by Chattrand, Polimeni and Zhang., 4th-edition. Chapter 2 for additional examples and practice problems on logic. If time permits I may use that text for additional examples beyond those given here.

1.1 propositional logic

Definition 1.1.1. *A* **proposition** *is any declarative sentence (including mathematical sentences such as equations) that is true or false. If P is a* **propositional variable** *then P is either true or false. A* **predicate** *or* **open statement** *is a proposition whose truth value is a function of one or more variables.*

Example 1.1.2. *The statement "$x > 5$" is a predicate since we cannot know if it is true or false unless we are given the value of x. In contrast, the compound statement "$x = 10$ and $x > 5$" is a proposition which happens to be true. In contrast, "$x = 10$ and $x > 11$" is a proposition which is false. We will focus on propositions in this section and the next then we turn to the study of predicates in the third section.*

We also write $P = T$ to express that P is true, or $P = F$ to express that P is false. Since propositions take values in $\{T, F\}$ we can define operations on propositions via the use of truth tables.

Definition 1.1.3. *Let P be a proposition then we define* **negation** *of P by*

P	$\sim P$
F	T
T	F

We read $\sim P$ as " not P".

In words, $\sim P$ takes the opposite truth value of P. Notice, the table below gives the other three possible **uniary** operations on a single proposition P.

P	I	II	III
F	F	T	F
T	T	T	F

We could also express these by:

$$I : P \mapsto P, \qquad II : P \mapsto T, \qquad III : P \mapsto F$$

I would call case I the **identity operation** it merely maps P to P. Cases II. and III. are the **constant maps** to true and false respectively.

If a proposition cannot be naturally divided then it is called **simple** or **atomic**. Often we have propositions that depend on two or more component propositions. Such propositions are called *compound*.

Definition 1.1.4. *Let P, Q be propositions. We define* **conjunction** *by*

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

We read $P \wedge Q$ as "P and Q". Here P and Q are the **conjuncts** *of the conjunction $P \vee Q$.*

The logical operation of "and" is true if and only if both of the input propositions are true.

Definition 1.1.5. *Let P, Q be propositions. Define* **disjunction** *by:*

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

We read $P \vee Q$ as "P or Q" and P, Q are **disjuncts***.*

Notice this idea of "or" differs from the usual meaning of "or" in common conversation. Mathematical "or" (also known as **inclusive-or** is true if either or both of the members is true. For instance consider the following statement:

> The paint is black or white.

This is not a mathematical usage of the logical connective *or*. In mathematics, if we wish to communicate the sentiment of the above quote we use langauge such as follows:

> The paint is either black or white.

Logically, this corresponds to the so-called *exclusive or*

Definition 1.1.6. *Let P, Q be propositions. Define* **exclusive-or** *as follows:*

P	Q	$P \oplus Q$
F	F	F
F	T	T
T	F	T
T	T	F

A connective between two propositions is a assigns four cases the values of T or F, this means there are $2^4 = 16$ distinct logical operations on a pair of propositions. Don't worry, I'm not going to name all of them. Certainly $\wedge$, $\vee$ and $\Rightarrow$ are the most important and commonly used connectives in mathematical argumentation.

Definition 1.1.7. *Let P, Q be propositions. We define the* **conditional** *or* **implication** *as follows:.*

P	Q	$P \Rightarrow Q$
F	F	T
F	T	T
T	F	F
T	T	T

Notice the only way for $P \Rightarrow Q$ to be false is for P to be true yet Q is false. In the implication $P \Rightarrow Q$ the proposition P is known as the **hypothesis** or **antecedent** and Q is the **conclusion** or **consequent**. There are several related connectives to the conditional:

- $Q \Rightarrow P$ is the **converse** of $P \Rightarrow Q$.
- $\sim P \Rightarrow \sim Q$ is the **inverse** of $P \Rightarrow Q$.

- $\sim Q \Rightarrow \sim P$ is the **contrapositive** of $P \Rightarrow Q$.

Both the converse and inverse are logically distinct from the implication, however, the contrapositive of the implication is logically equivalent; the contrapositive is true if and only if the implication is true. This means we can prove an implication by proving the contrapositive. This method is known as *proof by contraposition.*

Example 1.1.8. *Consider the implication, if a cat is alive then it is evil. Here P is the proposition that the cat is alive and Q is the proposition that the cat is evil.*

- **converse:** $(Q \Rightarrow P)$ *if the cat is evil then it is alive.*
- **inverse:** $(\sim Q \Rightarrow \sim P)$ *if the cat is dead then the cat is good.*
- **contrapositive:** $(\sim Q \Rightarrow \sim P)$ *if the cat is good then the cat is dead.*

Here I have assumed the negation of evil is good and the negation of alive is dead. I do not allow the category of zombie cats for this example. Nearly all real world examples fail if you apply the principle of achually[1] *to them.*

There are many ways for the conditional to appear in english. The following sentences are logically equivalent[2]: I decided to use a mathematical example for a change,

- (P implies Q). Differentiability of f implies continuity of f.
- (If P then Q). If f is differentiable then f is continuous.
- (If P, Q). If f is differentiable, f is continuous.
- (Q if P). The function is continuous if it is differentiable.
- (P only if Q). The function is differentiable only if it is continuous.
- (P is sufficient for Q). Differentiability of f is sufficient to give continuity for f.
- (Q is necessary for P). Continuity of f is necessary for differentiability of f.
- (Whenever P, Q). Whenever f is differentiable, f is continuous.
- (Q whenever P). The function is continuous whenever it is differentiable.

What does this list mean ? It means we have to think about the meaning of sentence, sometimes the logical structure is hidden behind unfamilar wording. There is no substitute for thinking in this course.

In common english the implication is often conflated with the biconditional.

Definition 1.1.9. *Let P, Q be propositions. We define the* **biconditional** *or* **equivalence** *by:*

P	Q	$P \Leftrightarrow Q$
F	F	T
F	T	F
T	F	F
T	T	T

[1] see meme culture.

[2] thanks again to the excellent text by Wolf where I found this list on page 30.

Like the conditional, there are many ways that the biconditional appears in english sentences.

- (P if and only if Q): f is analytic if and only if f is holomorphic.
- (P is necessary and sufficient for Q): Analyticity is necessary and sufficient for holomorphicity.
- (P is equivalent to Q): Analyticity is equivalent to holomorphicity.
- (P and Q are equivalent): Analyticity and holomorphicity are equivalent conditions.

Notice the biconditional allows us to express equivalence of claims. I'll use it in the next remark.

Remark 1.1.10. *Parenthesis for order of operation are encouraged generally, but if needed, we generally follow the following* **priority of connectives** *as a matter of custom; from highest to lowest priority* $\sim, \wedge, \vee, \Rightarrow, \Leftrightarrow$*. For example,*

$$\{\sim P \wedge Q \Rightarrow S \Leftrightarrow \sim Q \vee P\} \;\Leftrightarrow\; \{[((\sim P) \wedge Q) \Rightarrow S] \Leftrightarrow [((\sim Q) \vee P)]\}$$

However, there is not universal agreement on the priority of $\vee$ *and* $\wedge$ *so we should include parenthesis as to give the meaning to* $P \vee Q \wedge R$*:*

$$P \vee (Q \wedge R) \qquad \textit{as opposed to} \qquad (P \vee Q) \wedge R$$

the statments above are not logically equivalent. In contrast, $P \wedge Q \wedge R$ *and* $P \vee Q \vee R$ *are logically unambiguous as we will soon explain. One last matter of custom to explain,*

$$P \Rightarrow Q \Rightarrow R \quad \Leftrightarrow \quad (P \Rightarrow Q) \wedge (Q \Rightarrow R).$$

and $P \Leftrightarrow Q \Leftrightarrow R$ *is logically equivalent to* $(P \Leftrightarrow Q) \wedge (Q \Leftrightarrow R)$*.*

Truth tables are convenient to unambiguously communicate casewise logic. However, it is also useful to write the definitions in sentence form.

Definition 1.1.11. *The* **truth functions** *of the connectives* $\wedge, \vee, \sim, \Rightarrow, \Leftrightarrow$ *are defined as follows:*

- $P \wedge Q$ *is true provided both* P *and* Q *are true,*
- $P \vee Q$ *is true provided at least one of the statements* P *and* Q *is true,*
- $\sim P$ *is true provided* P *is false,*
- $P \Rightarrow Q$ *is true provided* P *is false, or* Q *is true (or both),*
- $P \Leftrightarrow Q$ *is true provided* P *and* Q *are both true or both false.*

If in doubt, consult the truth table. That said, we do not use truth tables in typical proof writing. Mostly their introduction here is to remove uncertainty about the basic logical terms.

Definition 1.1.12. *A* **tautology***, or a* **law of propositional logic***, is a statement whose truth function has all* T*'s as outputs. A* **contradiction** *is a statement whose truth function has all* F*'s as outputs. In other words, a contradiction is a statmen whose negation is a tautology. Two statements are called* **propositionally equivalent** *if a tautology results when the connective* $\Leftrightarrow$ *is put between them.*

There are a number of tautologies which inform our standard methods of proof.

Theorem 1.1.13. *Let P, Q, R be propositions. The following are tautologies:*

(1.) *Law of excluded middle:* $P \vee \sim P$

(2.) *Law of noncontradiction:* $\sim (P \wedge \sim P)$

(3.) *Basis for modus ponens:* $[P \wedge (P \Rightarrow Q)] \Rightarrow Q$

(4.) *Basis for modus tollens:* $[\sim Q \wedge (P \Rightarrow Q)] \Rightarrow \sim P$

(5.) *Transitivity of implication:* $[(P \Rightarrow Q) \wedge (Q \Rightarrow R)] \Rightarrow (P \Rightarrow R)$.

(6.) *Transitivity of equivalence:* $[(P \Leftrightarrow Q) \wedge (Q \Leftrightarrow R)] \Rightarrow (P \Leftrightarrow R)$.

(7.) *De Morgan's Laws:* $\sim (P \wedge Q) \Leftrightarrow \sim P \vee \sim Q$ *and* $\sim (P \vee Q) \Leftrightarrow \sim P \wedge \sim Q$

(8.) *Law of contraposition:* $(P \Rightarrow Q) \Leftrightarrow (\sim Q \Rightarrow \sim P)$

(9.) *Basis for indirect proof*[3]*:* $[P \Rightarrow (Q \wedge \sim Q)] \Leftrightarrow \sim P$

Proof: we use casewise analysis to prove this theorem. My method of proof assumes the reader is ready, willing and able to apply definitions of conjunction, disjunction, negation, implication and biconditional to form the arguments given below.

(1.): if $P = T$ then $P \vee \sim P = T \vee F = T$. Likewise, if $P = F$ then $P \vee \sim P = F \vee T = T$. Therefore, $P \vee \sim P$ is true in every case.

(2.): if $P = T$ then $P \wedge \sim P = T \wedge F = F$. Likewise, if $P = F$ then $P \wedge \sim P = F \wedge T = F$. Therefore, $P \wedge \sim P = F$ in every case and hence $\sim (P \wedge \sim P) = \sim F = T$ in every case of P.

(3.): we use a truth table which is to be read left to right:

P	Q	$P \Rightarrow Q$	$P \wedge (P \Rightarrow Q)$	$[P \wedge (P \Rightarrow Q)] \Rightarrow Q$
F	F	T	F	T
F	T	T	F	T
T	F	F	F	T
T	T	T	T	T

Thus $[P \wedge (P \Rightarrow Q)] \Rightarrow Q$ is a tautology.

(6.) Since P, Q, R take two values each we face eight cases. Consider,

P	Q	R	$P \Leftrightarrow Q$	$Q \Leftrightarrow R$	$[(P \Leftrightarrow Q) \wedge (Q \Leftrightarrow R)]$	$P \Leftrightarrow R$	$[(P \Leftrightarrow Q) \wedge (Q \Leftrightarrow R)] \Rightarrow (P \Leftrightarrow R)$
F	F	F	T	T	T	T	T
F	F	T	T	F	F	F	T
F	T	F	F	F	F	T	T
F	T	T	F	T	F	F	T
T	F	F	F	T	F	F	T
T	F	T	F	F	F	T	T
T	T	F	T	F	F	F	T
T	T	T	T	T	T	T	T

[3] I typically call this "proof by contradiction"

Thus $[(P \Leftrightarrow Q) \wedge (Q \Leftrightarrow R)] \Rightarrow (P \Leftrightarrow R)$ is a tautology.

I leave the proofs of the remaining parts as exercises for the reader. It is likely we do another case in class which is not given here. □

I hope the reader will forgive me for omitting proof of the following theorem. Once more, all of these tautologies make excellent homework exercises.

Theorem 1.1.14. *Let P, Q, R be propositions. The following are tautologies:*

(1.) *Law of double negation:* $\sim\sim P \Leftrightarrow P$

(2.) *Basis for simplification:* $(P \wedge Q) \Rightarrow P$ *and* $(P \wedge Q) \Rightarrow Q$

(3.) *Basis for addition:* $P \Rightarrow (P \vee Q)$ *and* $Q \Rightarrow (P \vee Q)$

(4.) $Q \Rightarrow (P \Rightarrow Q)$ *and* $\sim P \Rightarrow (P \Rightarrow Q)$

(5.) $[\sim P \wedge (P \vee Q)] \Rightarrow Q$ *and* $P \Rightarrow [Q \Rightarrow (P \wedge Q)]$

(6.) $(P \Rightarrow Q) \Rightarrow [(P \vee R) \Rightarrow (Q \vee R)]$ *and* $(P \Rightarrow Q) \Rightarrow [(P \wedge R) \Rightarrow (Q \wedge R)]$

(7.) $\sim (P \Rightarrow Q) \Leftrightarrow P \wedge \sim Q$

(8.) $(P \Rightarrow Q) \Leftrightarrow (\sim P \vee Q)$

(9.) $(P \Leftrightarrow Q) \Leftrightarrow [(P \Rightarrow Q) \wedge (Q \Rightarrow P)]$

(10.) $(P \Leftrightarrow Q) \Leftrightarrow [(P \wedge Q) \vee (\sim P \wedge \sim Q)]$

(11.) $[(P \Rightarrow Q) \wedge (P \Rightarrow R)] \Leftrightarrow [P \Rightarrow (Q \wedge R)]$ *and* $[(P \Rightarrow R) \wedge (Q \Rightarrow R)] \Leftrightarrow [(P \vee Q) \Rightarrow R]$

(12.) $[P \Rightarrow (Q \Rightarrow R)] \Leftrightarrow [(P \wedge Q) \Rightarrow R]$

(13.) *Distributive Laws:* $[P \wedge (Q \vee R)] \Leftrightarrow [(P \wedge Q) \vee (P \wedge R)]$ *and* $[P \vee (Q \wedge R)] \Leftrightarrow [(P \vee Q) \wedge (P \vee R)]$

1.2 propositional consequence and proofs

In practice mathematicians rarely give formal proofs[4]. That said, it is generally understood that any proper mathematical proof could be distilled into a formal proof if the need arose. What constitutes an acceptable proof is a subtle matter which is only answered by experience. Ultimately, the goal of a proof is to convince your reader that the argument given is correct. In this course, I will model many informal proofs and it is generally expected you create proofs of similar style and rigor. The proof you might give in a journal article might be entirely different. Anyway, enough about what we're going to mainly do, we should first be careful so we can better understand which liberties are generally taken outside this formal approach. [5]

[4] I should give a handout on Appendices I and II from Wolf which lay out a formal system from which line-by-line careful proofs can be constructed. It will be a couple weeks before we can understand those Appendices as we ought

[5] I'm sure professional logicians cut this discussion more finely than I have here, my goal is not to be perfectly rigorous. This is not a course in logic, it is a course where we use logic. I'm not teaching how to build a hammer, I'm teaching how to pound some nails. Later, we use a nail gun.

Definition 1.2.1. *A statement Q is said to be* **propositional consequence** *of statements P_1,P_2, $\dots, P_n$ if and only if the single statement $(P_1 \wedge P_2 \wedge \cdots \wedge P_n) \Rightarrow Q$ is a tautology. We often drop the term propositional and simply refer to consequence for the sake of brevity. The assertion Q is the consequence of some list of statements is called an* **argument**. *The statments in the list are called* **premises** *or* **hypotheses** *or* **givens** *of the argument and Q is called the* **conclusion** *of the argument. If Q really is a consequence of the list of statements, the argument is said to be* **valid**.

Mathematical theorems aim to communicate logical interaction of mathematical concepts. When the preconditions of a given theorem are met then the conclusions of the theorem hold true. If the preconditions are never met, then the theorem can say whatever and it will be sound. The term *theorem* is often used for an argument, or collection of arguments, which merits special attention, it originates from a similar sounding Greek word whose meaning is roughly *hey, look at this*. A *corollary* is a result which follows from a given theorem with little further argumentation. The word *corollary* is based on some Latin phrase which means a floral wreath. The idea is that a corollary is a celebratory gift of the theorem. Or, if you like, you can think of a corollary as a flower which grows from the theorem. We also use the term *proposition* for less important theorems, and we use the term *lemma* as a result which is used in support of proving a deeper theorem. To be honest, the terms theorem, proposition and lemma are more or less used with the same meaning. On a personal level, if you look at the thousands of pages of notes I've written you'll find my use of proposition and theorem varies from work to work as my sense of style has morphed over the years.

Theorem 1.2.2. *Suppose statement R is a consequence of premises $P_1, \dots, P_n$ and suppose Q is a consequence of primises $P_1, \dots, P_n$ and R. Then Q is a consequence of $P_1, \dots, P_n$.*

Proof: let $P = P_1, \dots, P_n$ and assume $P \Rightarrow R$ and $(P \wedge R) \Rightarrow Q$ are tautologies. If P is true then R is true hence $P \wedge R$ is true. Therefore, Q is true by the given tautology $(P \wedge R) \Rightarrow Q$. In summary, we have shown Q is true whenever P is true and it follows Q is a consequence of $P = P_1, \dots, P_n$. □

In my estimation we have to wait until we introduce quantifiers and open statements before we have many interesting theorems to prove. I'll model a formal proof for the proposition to follow. The backdrop for this proof is the assumption that Theorems 1.1.13 and 1.1.14 are given to be true.

Proposition 1.2.3. *Let P, Q be propositions then $(P \Rightarrow Q) \Leftrightarrow [\sim (P \wedge \ \sim Q)]$*

Proof (formal): let P, Q be propositions.

(1.) $(P \Rightarrow Q) \Leftrightarrow \ (\sim P \vee Q)$ by (7.) of Theorem 1.1.14.

(2.) $(\sim P \vee Q) \Leftrightarrow [\sim\sim (\sim P \vee Q)]$ by (1.) of Theorem 1.1.14.

(3.) $(P \Rightarrow Q) \Leftrightarrow [\sim\sim (\sim P \vee Q)]$ by (6.) of Theorem 1.1.14 applied to (1.) and (2.).

(4.) $[\sim (\sim P \vee Q)] \Leftrightarrow [(\sim\sim P) \wedge (\sim Q)]$ by (7.) of Theorem 1.1.13.

(5.) $[(\sim\sim P) \wedge (\sim Q)] \Leftrightarrow [P \wedge (\sim Q)]$ by (1.) of Theorem 1.1.14.

(6.) $[\sim (\sim P \vee Q)] \Leftrightarrow [P \wedge (\sim Q)]$ by (6.) of Theorem 1.1.14 applied to (4.) and (5.).

(7.) $(P \Rightarrow Q) \Leftrightarrow [\sim [P \wedge (\sim Q)]]$ substituting (6.) into (3.). □

Let me give an informal proof as to contrast the proof above.

Proof (informal): let P, Q be propositions. Observe, by (7.) of Theorem 1.1.14, double-negation and De Morgan's Laws we have the following logical equivalences:

$$(P \Rightarrow Q) \Leftrightarrow \ (\sim P \vee Q) \Leftrightarrow \sim [\sim (\sim P \vee Q)] \Leftrightarrow \sim [(\sim\sim P) \wedge (\sim Q)]$$

However, $\sim\sim P \Leftrightarrow P$ hence $(P \Rightarrow Q) \Leftrightarrow [\sim (P \wedge (\sim Q))]$. $\square$

Perhaps you recognize this sort of distinction from your work in Calculus I on limits. Some instructors insist students systematically use the limit laws in step-by-step fashion without missing any step. Each step in the formal proof was directly based on a previously known theorem. In contrast, I combined several steps at once. Essentially, my informal proof rests on a theorem which says $A_1 \Leftrightarrow A_2$, $A_2 \Leftrightarrow A_3$, $A_3 \Leftrightarrow A_4$ then $A_1 \Leftrightarrow A_4$. We have not proved that result, but, on the other hand, it is not too hard to see how you could easily prove it by repeated application of (6.) of Theorem 1.1.14.

I think that is enough to get us started, we will return to the problem of describing proof techniques in later sections.

1.3 open statements and predicate logic

Let us begin by specifying some terms we already use, often without thinking.

Definition 1.3.1. *A* **mathematical variable** *is some symbol, or combination of symbols, that represents some unspecified number or other object. The collection of numbers or objects from which a particular variable can take its values is known as the* **domain** *or* **universe** *of the variable. Variables with the same domain are known as variables of the same* **sort***.*

Not every symbol is a mathematical variable. For example, e or π are *constants*.

Definition 1.3.2. *A symbol, or combination of symbols, that represents some* **fixed** *number or other object is called a* **constant symbol** *or simply a* **constant***.*

Given a set of mathematical variables of a particular sort we are usually able to form predicates using the variables and appropriate operations. For instance, given real variables x, y we can consider open statements such as $x + y < 10$ or $\cos(x + y) = 1$ or $\sqrt{x} = 3$. We can also create **expressions** such as or e^x or $\log(x)$ or $\cosh(x)/\sinh(y)$ etc. An **expression** is a combination of mathematical variables.

Notice, variables and expressions need not be numbers. In the study of modern geometry, we consider variables which represent points. If A, B are points then AB denotes the line segment with endpoints A and B. On the other hand, $\overrightarrow{AB}$ denotes the directed-line-segment from A to B. Likewise $|AB|$ denotes the length of the line segment AB. Given three points A, B, C we can denote a triangle T_{ABC} to denote the triangle with vertices A, B, C. Or $\angle(A, B, C)$ to denote the angle made between $\overrightarrow{BA}$ and $\overrightarrow{BC}$ at B.

In Topology we might use X and Y to denote topological spaces. In linear algebra, we use V or W to denote vector spaces. In group theory we use G or H to denote groups. In graph theory, we might discuss Γ as an arbitrary graph. The concept of a variable extends far past your experience with calculus thus far.

Definition 1.3.3. *The symbol $\forall$ is the* **universal quantifier** *it denotes the phrase* **for all** *or* **for any** *or* **for every**. *The symbol $\exists$ is the* **existential quantifier** *denotes the phrase* **there exists** *or* **there is** *or* **for some**.

A quantifier applied to an open sentence may produce a proposition.

Example 1.3.4. *Let $R(x)$ denote the open sentence "x is a real number". Let $Q(x)$ denote the open sentence "x is a rational number". Let $N(x)$ denote the open sentence "x is a natural number". Let $Z(x)$ denote the open sentence "x is an integer".*

- *Each rational number is also a real number: $\forall x(Q(x) \Rightarrow R(x))$.*
- *Each natural number is also an integer: $\forall x(N(x) \Rightarrow Z(x))$.*
- *Some real numbers are also rational numbers: $\exists x(R(x) \wedge Q(x))$.*
- *Some integers are also natural numbers: $\exists x(Z(x) \wedge N(x))$.*
- *Each real number is also an integer: $\forall x(R(x) \Rightarrow Z(x))$.*

Which proposition above is false[6] *? There are four true and one false.*

Example 1.3.5. *Each sentence is paired with a symbolic formulation in terms of quantifiers: let $C(x)$ denote the open sentence "x is a cat" and let $M(x)$ denote the open sentence "x is a mammal". Let $A(x)$ denote the open sentence "x is an animal". We can use these predicates and quantifiers to reformulate the sentences as follows:*

- *All cats are mammals: $\forall x(C(x) \Rightarrow M(x))$*
- *Some animals are cats: $\exists y(A(y) \wedge C(y))$*
- *A cat is not an animal: $\forall z(C(z) \Rightarrow (\sim A(z)))$*
- *Some animals are not cats: $\exists y(A(y) \wedge (\sim C(y)))$*

Example 1.3.6. *Let $M(x, y)$ be the open sentence "x has mother y" and $F(x, y)$ be the open sentence "x has father y". I'll give three equivalent symbolic versions of the sentence:*

- *Everyone has a father and mother: $\forall x\ [(\exists y)(M(x, y)) \wedge (\exists z)(F(x, z)]$*
- *Everyone has a father and mother: $\forall x\ \exists y\ \exists z[M(x, y) \wedge F(x, z)]$*
- *Everyone has a father and mother: $\forall x\ \exists y, z\ [M(x, y) \wedge F(x, z)]$*

Whenever we have multiple quantifiers we can use abbreviated notation. In particular, $\exists y\ \exists z$ can be replaced with $\exists y, z$ and $\forall x \forall y$ can be replaced with $\forall x, y$. However, we should take care to maintain the proper ordering of quantifiers since the meaning can be quite different if we reverse $\exists$ and $\forall$.

Example 1.3.7. *Suppose x is a human living in Virginia. Let $B(x, y)$ denote the sentence x is the boss of y. Let $J(x)$ denote the sentence x is a two-faced annoying loser.*

- $\forall x \exists y(J(x) \wedge B(x, y))$*: This means for each person x living in Virginia, $\exists y(J(x) \wedge B(x, y))$. That is, each Virginian is a two-faced annoying loser who is the boss of at least one person.*

[6] I will define this carefully soon

- $\exists y \forall x (J(x) \wedge B(x,y))$: *This means there exists a person y living in Virginia such that $\forall x (J(x) \wedge B(x,y))$. That is, there exists a person y in Virginia for which every two-faced annoying loser is their boss.*

These are clearly distinct statements[7]

I'll give a mathematical example illustrating the distinction explored above, but first we should introduce a few more terms to help understand the nuances of working with open sentences and quantifiers.

Definition 1.3.8. *A mathematical variable occurring in a symbolic statement is called* **free** *if it is unquantified and* **bound** *if it is quantified. If a statement has no free variables it's* **closed**. *Otherwise, it's called a* **predicate**, *an* **open sentence**, *an* **open statement** *or a* **propositional function**. *The set of all x for which an open statement $P(x)$ is true is called its* **truth set**.

Example 1.3.9. *In the statement $\forall x \exists y (x + y + z = 0)$ the variables x, y are bound and z is free hence this statement is an open statement. We could label the statement $P(z)$. In contrast, the statement $\forall t (t > 0)$ has variable t which is bound and the statement is a closed statement.*

Definition 1.3.10. *A statement of the form $\forall \ P(x)$ is defined to be true provided $P(x)$ is true for each particular value of x from its domain. Similarly, $\exists x \ P(x)$ is defined to be true provided $P(x)$ is true for at least one x from its domain.*

Example 1.3.11. *In the statement P given by $\forall x (x < 0)$, the variable x is bound hence the statement P is closed. Here P is true or false depending on the domain of the variable x. If the domain is the interval $(-2, -1)$ then P is true whereas if the domain is all real numbers then P is false.*

Example 1.3.12. *Consider the statement "$x + 6 = 1$. Notice this is not a proposition because it is neither true nor false. We cannot decide unless we know the value of x. In contrast, if we specify that the domain of x is natural numbers then $\exists x (x + 6 = 1)$ is false since clearly $x = -5$ is the solution of the equation $x + 6 = 1$. Likewise, $\forall x (x + 6 = 1)$ is false since 1 is a natural number and $2 + 6 = 8 \neq 1$ thus $x + 6 = 1$ is not true for all x. On the other hand, if we declare the domain of x to be integers then the statement $\exists x (x + 6 = 1)$ is true since -5 is an integer and $-5 + 6 = 1$.*

Remark 1.3.13. *As I have shown thus far, we usually denote the variables for an open statement explicitly. For example, $P(x)$ is an open statement with free variable x, $Q(x, y)$ is an open statement with free variables x, y. However, we do not legalistically enforce this rule as explicit listing of all variables is at times unhelpful and burdensome. Choosing the right notation is an art. Another custom we should enforce is to not use the same variable both as a free and bound variable in the same statement. You've run across this issue when your professor wrote $\frac{d}{dx} \int_a^x f(t) dt = f(x)$ rather than $\frac{d}{dx} \int_a^x f(x) dx = f(x)$ which is frowned upon (as in, I'd take off points to communicate my demeanor reading it).*

Example 1.3.14. *Consider the statement "x has a cube root". This has a hidden quantifier because to define the cube root we require there exists y for which $y^3 = x$. Symbollically, "x has a cube root" can be formulated as $\exists y \ (y^3 = x)$. Here notice x is free while y is bound.*

[7] my boss is great, for the record.

The examples given on pages 57-58 of *Proof, Logic, and Conjecture: The Mathematician's Toolbox* by Robert S. Wolf are helpful and I will give them here.

Example 1.3.15. *Consider the statement $x + y = 0$ where x, y are real variables. We can quantify this by $\exists x \exists y(x + y = 0)$. Is this true ? Certainly, there are many examples, $x = 3$ and $y = -3$ solve $x + y = 0$ so $\exists x \exists y(x + y = 0)$ is true.*

Example 1.3.16. *Consider the statement $\forall x \forall y(x + y = 0)$ where x, y are real variables. This is clearly false. For example, $x = 1$ and $y = 1$ give $1 + 1 = 2 \neq 0$ hence $\forall x \forall y(x + y = 0)$ is false.*

Example 1.3.17. *Consider the statement $\forall x \exists y(x + y = 0)$ where x, y are real variables. This means for each x there exists y for which $x + y = 0$. Indeed, for each x we simply choose $y = -x$ and note $x + y = x + (-x) = 0$ hence the statement is true.*

Example 1.3.18. *Consider the statement P defined by $\exists x \forall y(x + y = 0)$ where x, y are real variables. This means there exists x such that $x + y = 0$ for all y. Suppose such x exists and $x + y = 0$ for all y. Then $x + 1 = 0 = x + 2$ hence $x = -1$ and $x = -2$ which is false. It follows there cannot exist such x and $\exists x \forall y(x + y = 0)$ is false.*

We often find the need to negate a proposition which is formed with quantifiers. The theorem below gives us the roadmap for forming such negations.

Theorem 1.3.19. *For any statement $P(x)$,*

(i.) *$\sim [\forall x P(x)]$ is logically equivalent to $\exists x[\sim P(x)]$*

(ii.) *$\sim [\exists x P(x)]$ is logically equivalent to $\forall x[\sim P(x)]$*

Proof: (i.) $\sim [\forall x P(x)]$ means it is not true that $P(x)$ holds for all x. Thus there exists at least some t for which $P(t)$ is false. Consequently $\sim P(t)$ is true and we find $\exists x[\sim P(x)]$.

(ii.) $\sim [\exists x P(x)]$ means it is not true that there exists x for which $P(x)$ is true. Thus every x makes $P(x)$ false. Hence, every x makes $\sim P(x)$ true. That is, $\forall x[\sim P(x)]$. $\square$

Example 1.3.20. *Consider the statement $\forall x \exists y P(x) \wedge Q(y)$ then*

$$\sim [\forall x \exists y \left(P(x) \wedge Q(y)\right)] \Leftrightarrow \exists x \left(\sim [\exists y P(x) \wedge Q(y)]\right) \Leftrightarrow \exists x \forall y \left(\sim [P(x) \wedge Q(y)]\right)$$

Finally, apply De Morgan's Law to deduce

$$\sim [\forall x \exists y \left(P(x) \wedge Q(y)\right)] \Leftrightarrow \exists x \forall y \left((\sim P(x)) \vee (\sim Q(y))\right)$$

Example 1.3.21. *Consider the statement "all cowboys are ninjas". If $C(x)$ is the statement "x is a cowboy" and $N(x)$ is the statement "x is a ninja" then symbolically our given statement can be written $\forall x \left(C(x) \Rightarrow N(x)\right)$. We found $P \Rightarrow Q \Leftrightarrow \sim [P \wedge (\sim Q)]$ in Example 1.2.3. It follows that $\sim (P \Rightarrow Q) \Leftrightarrow P \wedge (\sim Q)$ hence:*

$$\sim [\forall x \left(C(x) \Rightarrow N(x)\right)] \Leftrightarrow \exists x \left[\sim \left(C(x) \Rightarrow N(x)\right)\right] \Leftrightarrow \exists x \left[C(x) \wedge (\sim N(x))\right].$$

Hence the negation of the given statement reads "there exists a cowboy who is not a ninja".

Given a particular universe of discourse we often face variables which are further constrained. For example, if x is a real variable and $x \leq 10$ and we wished to characterize the existence of an x which satisfied some statement P then symbolically,

$$\exists x((x \leq 0) \wedge P)$$

or if we wished to characterize all $x \leq 10$ solving a given statement P then symbolically,

$$\forall x((x \leq 0) \Rightarrow P)$$

It is convenient to introduce notation to fold constraints into the quantifying notation.

Definition 1.3.22. *Suppose P is a statement and x is any variable whose domain has an ordering $<$ then for any constant c we denote:*

(i.) *$\exists(x < c)P$ is logically equivalent to $\exists x((x < c) \wedge P)$*

(ii.) *$\forall(x < c)P$ is logically equivalent to $\forall x((x < c) \Rightarrow P)$*

We also allow replacing $<$ in the expressions above with $>, \leq, \geq$.

Example 1.3.23. *Let me illustrate the notation further:*

$$\exists(x \leq 3)P \Leftrightarrow \exists x((x \leq 3) \wedge P)$$
$$\forall(x > c)P \Leftrightarrow \forall x((x > c) \Rightarrow P).$$

Example 1.3.24.

$$\begin{aligned} \forall(x > 0)\exists(y > 0)[x - y \leq 1] &\Leftrightarrow \forall(x > 0)Q \qquad (1.1)\\ &\Leftrightarrow \forall x((x > 0) \Rightarrow Q)\\ &\Leftrightarrow \forall x((x > 0) \Rightarrow (\exists(y > 0)[x - y \leq 1]))\\ &\Leftrightarrow \forall x((x > 0) \Rightarrow (\exists y[(y > 0) \wedge [x - y \leq 1)]]) \end{aligned}$$

If you think about the above proposition geometrically it is easy to see it is true. Notice $x - y \leq 1$ is equivalent[8] to the inequality $x - 1 \leq y$ or $y \geq x - 1$. In short, (x, y) is in the solution set of this inequality if the point (x, y) is above, or on, the line $y = x - 1$. In other words, the solution is a half-plane. For any x there is certainly a point in the solution set for which $y > 0$. Can you find the point explicitly ? (there are many choices, I'd draw a picture to help see it)

Often a constraint is formulated in terms of some subset of a given domain. The notation below parallels that we already introduced for inequalities.

Definition 1.3.25. *Let P be a statement and x a variable whose domain has subset A then*

(i.) *$\exists(x \in A)P$ is logically equivalent to $\exists x((x \in A) \wedge P)$*

(ii.) *$\forall(x \in A)P$ is logically equivalent to $\forall x((x \in A) \Rightarrow P)$.*

[8] This concept of equivalence is the judged by the solution set, two inequalities are equivalent if they share the same solution set. We will discuss equivalence of equations and inequalities in-depth at some time soon. Thus far we have simply assumed past course work gave sufficient insight into our analysis.

We discuss subsets and sets in more depth a bit later in the course, but I hope you have some familarity from your previous course work.

Example 1.3.26. *Consider the statement $\exists(x \in \mathbb{N})(\sin(x) = 0)$. Since $\sin(x) = 0$ if and only if $x = n\pi$ for some $n \in \mathbb{Z}$ we find the statement is true since $n\pi \notin \mathbb{N}$ for any $n \in \mathbb{Z}$. In contrast, $\forall(x \in \mathbb{N})(\sin(\pi x) = 0)$ is true since $x \in \mathbb{N}$ gives $\sin(\pi x) = 0$.*

Definition 1.3.27 (unique existence)**.** *For an open sentence $P(x)$, the proposition $(\exists! x)P(x)$ is read "there exists a unique x such that $P(x)$" and is true iff the truth set of $P(x)$ has exactly one element. The symbol $\exists!$ is called the unique existence quantifier.*

We can use any of the characterizations in the theorem above to test for unique existence.

Example 1.3.28. *Let x be a real variable. Consider the statement $\exists! x(\sinh(x) = 0)$. Indeed, this is a true statement since $\sinh(0) = 0$ but there is no other value for which the hyperbolic sine is zero. In contrast, $\exists! x(\cosh(x) = 0)$ is false since there does not exist a solution of $\cosh(x) = 0$. In fact, if we recall our study of the hyperbolic cosine we ought to recall $\cosh(x) \geq 1$.*

Example 1.3.29. *Let x be a complex variable. The statement $\exists! x(x^4 = 1)$ is false. Notice $x^4 = 1$ can be rewritten as $x^4 - 1 = 0$ and this factors as $(x^2-1)(x^2+1) = (x+1)(x-1)(x-i)(x+i) = 0$ thus, by the factor theorem of highschool algebra, $x = 1, -1, i, -i$ are the solutions of $x^4 = 1$. Clearly there is not a unique solution. In fact, there are four. In contrast, we could study $\exists!(x \in [0,\infty))(x^4 = 1)$ and find this statement to be true since $x = 1$ is the unique solution of $x^4 = 1$ given $x \in [0,\infty)$.*

Theorem 1.3.30. *If $A(x)$ is an open sentence with variable x, then*

(i.) $(\exists! x)A(x) \implies (\exists x)A(x)$.

(ii.) $(\exists! x)A(x)$ *is equivalent to* $\big[(\exists x)A(x) \wedge (\forall y)(\forall z)\big(A(y) \wedge A(z) \implies y = z\big)\big]$.

Proof: Let's prove $(i.)$. Let U be any universe. Assume there exists a unique $x = x_o \in U$ such that $A(x_o)$ is true. Then $A(x_o)$ is true so there exists $x = x_o$ such that $A(x)$ is true. Thus $\exists A(x)$ since the truth set of $A(x)$ is nonempty. This proves the implication. We have shown that when the antecedent is true then the consequent is true. Thus the implication labled a. is true. (*Usually I would not be so verbose, but since we are starting out I'll say a little extra to get us going.*)

Now we prove $(ii.)$. This is an $\Leftrightarrow$ proof. We need to establish that the implications $\Rightarrow$ and $\Leftarrow$ both hold true.

$(\Rightarrow)$: assume that $(\exists! x)A(x)$ relative to the universe U. We know the truth set of $A(x)$ is nonempty and contains only one element $x_o \in U$. Suppose $\exists A(x)$ and let $y, z \in U$ such that $A(y) \wedge A(z)$ is true. Then both $A(y)$ and $A(z)$ are true hence $y = x_o$ and $z = x_o$. Consequently, $y = z$. We have shown that $(\exists! x)A(x)$ implies that whenever there exists y, z such that $A(y)$ and $A(z)$ are true then $y = z$.

$(\Leftarrow)$: Assume that $(\exists x)A(x) \wedge (\forall y)(\forall z)\big(A(y) \wedge A(z) \implies y = z\big)$. This means that both $(\exists x)A(x)$ and $(\forall y)(\forall z)\big(A(y) \wedge A(z) \implies y = z\big)$ are true. Suppose that x_0, x_1 are in the truth set of $A(x)$ (*we can do this since $\exists A(x)$ is assumed true*). Then $A(x_0) \wedge A(x_1)$ is true, hence by the second portion of the initial assumption $x_0 = x_1$. We have shown that any two arbitrary elements of the truth set are equal, hence the truth set has only one element $x_0 = x_1$. Hence $(\exists! x)A(x)$. $\Box$.

Remark 1.3.31. *When a biconditional proof transitions from the $\Rightarrow$ to the $\Leftarrow$ it is customary to drop the assumptions made in the $\Rightarrow$ portion of the proof. It is acceptable to use the same notation in both directions, however it is crucial to order your statements in their proper logical order. Two paragraphs can have all the same statements and yet one is correct and the other is incorrect. The fact that the conditional sentence is not logically equivalent to it's converse means we must be careful to state our assumptions seperate from our desired conclusions.*

Theorem 1.3.32. *Let x, y be mathematical variables and $P(x)$ a statement. The following statements are equivalent,*

(i.) $\exists x \, (P(x) \wedge \forall y[P(y) \Rightarrow x = y])$

(ii.) $\exists x P(x) \wedge (\sim \exists x, y[P(x) \wedge P(y) \wedge x \neq y])$

(iii.) $\exists x P(x) \wedge \forall x, y[P(x) \wedge P(y) \Rightarrow x = y]$

(iv.) $\exists x \forall y (P(y) \Leftrightarrow y = x)$

Proof: I will not give a proper proof here. However, if you think about the conditions above they all mean the same thing: there exists an x which makes $P(x)$ true and there is only one such x. $\square$
We can use any of the characterizations in the theorem above to test for unique existence.

1.4 axioms and assumed background

I've delayed giving the formal definitions in this section by assuming knowledge from previous coursework up to this point. Going forward, I thought it would be healthy to collect definitions of the basic number systems and some of their derived properties in one easy to find section.

Real numbers can be constructed from set theory and about a semester of mathematics. We will accept the following as **axioms**[9]

Definition 1.4.1. *real numbers*

The set of real numbers is denoted $\mathbb{R}$ and is defined by the following axioms:

(A1) addition commutes; $a + b = b + a$ for all $a, b \in \mathbb{R}$.

(A2) addition is associative; $(a + b) + c = a + (b + c)$ for all $a, b, c \in \mathbb{R}$.

(A3) zero is additive identity; $a + 0 = 0 + a = a$ for all $a \in \mathbb{R}$.

(A4) additive inverses; for each $a \in \mathbb{R}$ there exists $-a \in \mathbb{R}$ and $a + (-a) = 0$.

(A5) multiplication commutes; $ab = ba$ for all $a, b \in \mathbb{R}$.

(A6) multiplication is associative; $(ab)c = a(bc)$ for all $a, b, c \in \mathbb{R}$.

(A7) one is multiplicative identity; $a1 = a$ for all $a \in \mathbb{R}$.

[9] an axiom is a basic belief which cannot be further reduced in the conversation at hand. If you'd like to see a construction of the real numbers from other math, see Ramanujan and Thomas' *Intermediate Analysis* which has the construction both from the so-called Dedekind cut technique and the Cauchy-class construction.

(A8) multiplicative inverses for nonzero elements;
for each $a \neq 0 \in \mathbb{R}$ there exists $\frac{1}{a} \in \mathbb{R}$ and $a\frac{1}{a} = 1$.

(A9) distributive properties; $a(b + c) = ab + ac$ and $(a + b)c = ac + bc$ for all $a, b, c \in \mathbb{R}$.

(A10) totally ordered field; for $a, b \in \mathbb{R}$:

(i) antisymmetry; if $a \leq b$ and $b \leq a$ then $a = b$.

(ii) transitivity; if $a \leq b$ and $b \leq c$ then $a \leq c$.

(iii) totality; $a \leq b$ or $b \leq a$

(A11) least upper bound property: every nonempty subset of $\mathbb{R}$ that has an upper bound, has a least upper bound. This makes the real numbers **complete**.

Modulo A11 and some math jargon this should all be old news. An **upper bound** for a set $S \subseteq \mathbb{R}$ is a number $M \in \mathbb{R}$ such that $M > s$ for all $s \in S$. Similarly a lower bound on S is a number $m \in \mathbb{R}$ such that $m < s$ for all $s \in S$. If a set S is bounded above and below then the set is said to be **bounded**. For example, the open set (a, b) is bounded above by b and it is bounded below by a. In contrast, rays such as $(0, \infty)$ are not bounded above. Closed intervals contain their least upper bound and greatest lower bound. The bounds for an open interval are outside the set.

Definition 1.4.2. *standard subsets of real numbers* $\mathbb{R} = (-\infty, \infty)$,

- natural numbers (positive integers); $\mathbb{N} = \{1, 2, 3, \dots\}$.
- integers; $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$. Note, $\mathbb{Z}_{>0} = \mathbb{N}$.
- non-negative integers; $\mathbb{Z}_{\geq 0} = \{0, 1, 2, \dots\} = \mathbb{N} \cup \{0\}$.
- negative integers; $\mathbb{Z}_{<0} = \{-1, -2, -3, \dots\} = -\mathbb{N}$.
- rational numbers; $\mathbb{Q} = \{\frac{p}{q} \mid p, q \in \mathbb{Z},\ q \neq 0\}$.
- irrational numbers; $\mathbb{I} = \{x \in \mathbb{R} \mid x \notin \mathbb{Q}\}$.
- open interval from a to b; $(a, b) = \{x | a < x < b\}$.
- closed interval; $[a, b] = \{x \mid a \leq x \leq b\}$.
- half-open intervals; $[a, b) = \{x \mid a \leq x < b\}$ and $(a, b] = \{x \mid a < x \leq b\}$
- closed rays; $[a, \infty) = \{x \mid x \geq a\}$ and $(-\infty, a] = \{x \mid x \leq a\}$
- open rays; $(a, \infty) = \{x \mid x > a\}$. and $(-\infty, a) = \{x \mid x < a\}$.

The cartesian product of $\mathbb{R}$ and $\mathbb{R}$ gives us $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R} = \{(x, y) \mid x, y \in \mathbb{R}\}$. In this context (x, y) is called an **ordered pair** of real numbers. Notice that the notation (a, b) could refer to a point in $\mathbb{R}^2$ or it could refer to a open interval. These are very different objects yet we use the same notation for both. The point $(a, b) \in \mathbb{R}^2$ whereas the interval $(a, b) \subseteq \mathbb{R}$. Question: is $(4, 3)$ a point or an open interval? Why is there no danger of ambiguity in this case?

The real numbers and rational numbers are examples of **fields**. A field is a set which satisfies axioms A1-A9. In fact, both $\mathbb{Q}$ and $\mathbb{R}$ are ordered fields which means follow axioms A1-A10. However, the rational numbers are not complete. To complete the rational numbers you have to throw in the irrational numbers which gives the whole real number system. Beyond the real and rational fields we can consider the complex number field.

Definition 1.4.3. Complex numbers *are defined by* $\mathbb{C} = \{a + ib \mid a, b \in \mathbb{R} \text{ and } i^2 = -1\}$*. The* **length** *of a complex number* $z = x + iy$ *is given by* $|z| = \sqrt{x^2 + y^2}$ *and the* **complex conjugate** *is* $\bar{z} = x - iy$*. If* θ *is the standard angle of* $(x, y) \neq (0, 0)$ *then the* $z = |z|e^{i\theta}$ *where* $e^{i\theta} = \cos\theta + i\sin\theta$ *defines the* **imaginary exponential***. If* $a, b \in \mathbb{R}$ *then* $z = a + ib$ *is in* **Cartesian form***. If* $r, \theta \in \mathbb{R}$ *and* $r \geq 0$ *then* $z = re^{i\theta}$ *is in* **polar form***.*

The complex numbers are not ordered[10] however they are **algebraically complete** this means we can factor any polynomial into linear factors with complex numbers. In contrast, the real numbers only allow us to factor a polynomial into linear factors together with irreducible quadratic factors. For example, $x^2 + 1$ cannot be factored over $\mathbb{R}$ but $x^2 + 1 = (x + i)(x - i)$. The proof that the complex numbers are algebraically complete was provided by Gauss in the nineteenth century. We often prove it in the complex variables (Math 331) course here at LU. We will find many occasions to use complex numbers in calculus and differential equations. Like it or not real problems often have complex solutions. Take the quadratic formula as a prime example of this phenomenon. The concept of a variable is so fundamental it bears mention at this juncture (I already used this concept in the definition of $\mathbb{R}$ if you think about it):

Definition 1.4.4. *A* **real variable** x *is a symbol which is allowed to assume any value in* $\mathbb{R}$*. A* **complex variable** z *is a symbol which is allowed to assume any value in* $\mathbb{C}$*.*

It is useful to catalogue the following properties of inequalities:

Theorem 1.4.5. *properties of inequalities: Let* $a, b, c, d \in \mathbb{R}$*,*

(1.) *square of real number is non-negative;* $a^2 \geq 0$*,*

(2.) *square zero only if number is zero;* $a^2 = 0$ *iff* $a = 0$*,*

(3.) *add or subtract from both sides at once; if* $a < b$ *then* $a + c < b + c$ *and* $a - c < b - c$*,*

(4.) *add inequalities;* $a < b$ *and* $c < d$ *implies* $a + c < b + d$*,*

(5.) *transitivity;* $a < b$ *and* $b < c$ *implies* $a < c$*,*

(6.) *if* $ab > 0$ *then* $a < b$ *implies* $1/a > 1/b$*.*

The last statement $ab > 0$ is just a tricksy way of saying that a and b are either both positive or both negative. This theorem can be proven from the axioms of the real numbers, but I will not offer those details here. You should not be surprised to hear that a similar theorem also holds if we replace $<$ with $>$ or $\leq$ with $\geq$.

Definition 1.4.6. *The* **absolute value** *of a real number* x *is denoted* $|x|$ *and is defined* $|x| = \sqrt{x^2}$*. Notice this formula is equivalent to the case-wise formula:*

$$|x| = \begin{cases} x & if\ x \geq 0 \\ -x & if\ x \leq 0 \end{cases}$$

This distance between $a, b \in \mathbb{R}$ *is denoted* $d(a, b)$ *and it is defined by* $d = |b - a|$*.*

We should recall that the square root function is by definition the positive root; $\sqrt{x} \geq 0$. Therefore, we can characterize a nonzero **positive** number by the equation $x = |x|$ whereas a nonzero **negative** number x has $|x| = -x$. It is useful to catalogue the following properties absolute values:

[10] hopefully we will define the concept of ordering a set carefully in our study of relations later in this course

Theorem 1.4.7. *properties of absolute value: Let $a, b, \epsilon \in \mathbb{R}$ with $\varepsilon > 0$,*

1. *absolute value is non-negative; $|a| \geq 0$,*
2. *absolute value is zero only if number is zero; $|a| = 0$ iff $a = 0$,*
3. *absolute value of product is product of absolute values; $|ab| = |a||b|$,*
4. *bounded absolute value same as double inequality; $|a| < \varepsilon \Leftrightarrow -\varepsilon < a < \varepsilon$,*
5. *triangle inequalities ;*

$$(i.)\ |a+b| \leq |a| + |b| \qquad (ii.)\ |a-b| \geq |a| - |b| \qquad (iii.)\ \big||a| - |b|\big| \leq |a-b|$$

Proof: (you can skip these proofs for your first read, we'll circle back to these later).

Item (1.) is immediately obvious from the definition $|x| = \sqrt{x^2}$.

To prove (2.) consider that if $a = 0$ then clearly $|0| = \sqrt{0^2} = 0$. Conversely, $\sqrt{a^2} = 0$ implies $a = 0$.

To prove (3.) note that $|ab| = \sqrt{(ab)^2} = \sqrt{a^2b^2} = \sqrt{a^2}\sqrt{b^2} = |a||b|$.

I leave (4.) for the reader to prove.

The proof of (5.) requires a bit more thought, I'll prove part (i.) and leave (ii.) and (iii.) for the reader. Notice that $|a+b|^2 = (a+b)^2$. Consider then

$$|a+b|^2 = (a+b)^2 = a^2 + 2ab + b^2 = |a|^2 + 2ab + |b|^2$$

To complete the proof of (4.) part (i.) we need to break into cases:

1. If $a, b > 0$ then $|a| = a$ and $|b| = b$ thus the equation above yields $|a+b|^2 = |a|^2 + 2|a||b| + |b|^2 = (|a| + |b|)^2$ hence $|a+b| = |a| + |b|$.
2. If both $a, b < 0$ then we have $|a| = -a$ and $|b| = -b$ thus $2ab = 2(-a)(-b) = 2|a||b|$ which gives us that $|a+b|^2 = (|a| + |b|)^2$ which again yields $|a+b| = |a| + |b|$.
3. If $a > 0$ and $b < 0$ then $2ab = -2a(-b) = -2|a||b|$ therefore $|a+b|^2 = |a|^2 - 2|a||b| + |b|^2$. Since $|a|, |b| > 0$ it is certainly true that adding $4|a||b|$ to the r.h.s. of the equality gives the following inequality, $|a+b|^2 = |a|^2 - 2|a||b| + |b|^2 < |a|^2 + 2|a||b| + |b|^2 = (|a| + |b|)^2$. Therefore, $|a+b| < |a| + |b|$.
4. If $a < 0$ and $b > 0$ then by the argument above with $a \leftrightarrow b$ shows $|a+b| < |a| + |b|$.
5. If either $a = 0$ or $b = 0$ then the (4.) is clearly true.

Thus $|a+b| \leq |a| + |b|$ for all possible cases hence the proposition is true[11]. $\square$

[11] Note that in mathematics our standard for true and false is much stricter than other disciplines. When we ask if something is true it is usually the case that we implicitly mean to ask "is this true for all possible cases". If we wish to ask a question relative to a restricted set of cases then we are obligated to reduce the set of answers for the question which is asked. This is often a source of confusion between professors and students. Typically I'll answer the question which was literally asked whether or not that was the intended question.

Chapter 2

Proofs

Most proofs goes through three stages:

- understanding the given problem
- choosing a proof strategy
- writing the proof

You can also read Chapters 3,4,5,7,8 and perhaps the first section in Chapter 12 of *Mathematical Proofs: a Transition to Advanced Mathematics* by Chattrand, Polimeni and Zhang., 4th-edition. These chapters overlap with the subject matter of this chapter of my notes. As before, if time permits, I may use that text or Wolf for additional examples. There are many additional practice problems there if you need further practice.

2.1 even, odd and divisibility of integers

Let us begin by settling the definitions needed and looking at some elementary proofs.

Definition 2.1.1. even *and* **odd** *integers:*
We say that $n \in \mathbb{Z}$ is **even** *iff $\exists k \in \mathbb{Z}$ such that $n = 2k$.*
We say that $n \in \mathbb{Z}$ is **odd** *iff $\exists k \in \mathbb{Z}$ such that $n = 2k + 1$.*

To prove 47 is odd we can write $47 = 2(23) + 1$ and note $23 \in \mathbb{Z}$. To prove 10 is even we note $10 = 2(5)$ where $5 \in \mathbb{Z}$. Notice $\sqrt{12} = 2\sqrt{3}$ does not show $\sqrt{12}$ is even because $\sqrt{3} \notin \mathbb{Z}$. It is important to verify the choice of k is actually an integer in proofs concerning even and odd integers. One criticism I would make of my old Math 200 notes, and possibly the homework solutions from that 2009 course, is I failed to adequately emphasize the step of verifying $k \in \mathbb{Z}$. To be clear, I am merely using the letter k for the sake of readability, in practice any letter can be used. For example, if $k, l \in \mathbb{Z}$ then $2k$ is even and $2l + 1$ is odd.

Example 2.1.2. *(simple even integer proof).*

> **Claim:** *Let $n \in \mathbb{Z}$, we can show $2n^2 + 4n + 8$ is even.*
>
> **Proof:** *observe $2n^2 + 4n + 8 = 2(n^2 + 2n + 4) = 2k$ where $k = n^2 + 2n + 4 \in \mathbb{Z}$ since the sum and products of integers is an integer. Thus $2n^2 + 4n + 8$ is an even integer.* □

Example 2.1.3. *(simple odd integer proof)*

> **Claim:** *Let $n \in \mathbb{Z}$, we can show $2n^2 + 4n + 7$ is odd.*
>
> **Proof:** *Observe that $2n^2 + 4n + 7 = 2(n^2 + 2n + 3) + 1$ and $k = n^2 + 2n + 3 \in \mathbb{Z}$. Thus conclude $2n^2 + 4n + 7 = 2k + 1$ is an odd integer.* $\square$

Definition 2.1.4. divisibility, **factors** *and* **multiples***:*
Let $a, b \in \mathbb{Z}$ then we say that b is a factor a iff $\exists k \in \mathbb{Z}$ such that $a = kb$. We also say b is a **multiple** *of a in this case. In addition, we say b* **divides** *a iff b is a factor of a and we write $b \mid a$ to mean "b divides a". The notation $b \nmid a$ means "b does not divide a"*

Divisibility is **not** division. Please be careful to understand the process of division and the trait of divisibility are related but distinct. Notice, $14/7 = 2$ means $14 = 2(7)$ which shows $2 \mid 14$ and $7 \mid 14$.

Example 2.1.5. *(divisibility proof)*

> **Claim:** *If $n \in \mathbb{Z}$, then 3 divides $(n + 1)^2 + 2n^2 + n + 2$.*
>
> **Proof:** *Let $n \in \mathbb{Z}$ and note that:*
>
> $$(n + 1)^2 + 2n^2 + n + 2 = n^2 + 2n + 1 + 2n^2 + n + 2 = 3(n^2 + n + 1).$$
>
> *It is clear that $n^2 + n + 1$ is an integer. The fact that I can factor out 3 shows that 3 divides $(n + 1)^2 + 2n^2 + n + 2$.*

Remark 2.1.6. *The idea of factoring extends to polynomials and other number systems besides just the integers. Technically speaking, we ough to say something is divided by something else with respect to the universe of allowed objects. Our universe in this course is often $\mathbb{Z}$. However, for other universes definition of "divides by" is very similar, for example we can say that $x^2 + x$ is divided by $(x + 1)$ since $x^2 + x = x(x + 1)$ in the universe $\mathbb{R}[x]$ (this denotes polynomials in x with real coefficients). On the other hand if $r \in \mathbb{R}$ with $r \neq 0$ we can show that 4 divides r with respect to $\mathbb{R}$; notice that $r = 4\left(\frac{r}{4}\right)$. In fact any nonzero real number will divide r by the same argument. If a polynomial is not divided by a non-constant polynomial then the polynomial is said to be an* **irreducible polynomial***. For example, $x^2 + 1$ is irreducible over $\mathbb{R}$ but $x^2 + 1 = (x + i)(x - i)$ so $x^2 + 1$ is* **reducible** *over $\mathbb{C}$.The problem of factoring is the problem of writing a given polynomial as a product of irreducible factors with respect to the given context (usually $\mathbb{R}$ or $\mathbb{C}$, but we do consider other contexts in later math courses).*

2.2 direct proofs

The examples given thus far in this chapter have been *direct proofs*. We look at several further examples then we turn to other methods in the next section. Each method is based on a tautology we discussed earlier in the course.

Example 2.2.1. Prove: If x, y are even integers then xy is even.
Proof: Let $x, y \in \mathbb{Z}$ be even integers. Then, by definition of even integers, $\exists a, b \in \mathbb{Z}$ such that $x = 2a$ and $y = 2b$. Observe that $xy = (2a)(2b) = 2(2ab)$ where $2ab \in \mathbb{Z}$ thus xy is even. $\square$

In the example above, P was the statement that x, y were even. Then Q was the statement that xy was even. We assumed P and found that Q necessarily followed. Thus, $P \Rightarrow Q$.

Remark 2.2.2. *The example just given made an argument for arbitrary integers x and y. Therefore, if x, y are integer variables, we can conclude $(\forall x)(\forall y)(x \text{ and } y \text{ even } \Rightarrow xy \text{ even})$.*

Example 2.2.3. Prove: If $x \in \mathbb{R}$ then $|x| = \sqrt{x^2}$.
Proof: Recall that $|x| = x$ if $x \geq 0$ and $|x| = -x$ if $x < 0$. If $x \geq 0$ then $|x| = x = \sqrt{x^2}$. If $x < 0$ then $-x > 0$ and $\sqrt{x^2} = -x$ (since by definition the squareroot function is non-negative) hence $|x| = -x = \sqrt{x^2}$. Therefore, $|x| = \sqrt{x^2}$ for all $x \in \mathbb{R}$. □

Example 2.2.4. Prove: If $a, b \in \mathbb{R}$ then $|ab| = |a||b|$.
Proof: Let $a, b \in \mathbb{R}$, and recall $|x| = \sqrt{x^2}$ thus,

$$|ab| = \sqrt{(ab)^2} = \sqrt{a^2b^2} = \sqrt{a^2}\sqrt{b^2} = |a||b|,$$

by the laws of exponents and radicals. □

We take properties of the real numbers such as laws of exponents and radicals as axioms unless otherwise instructed in this course. An axiom is a truth which is basic and does not follow from other more basic truths. One goal of mathematics in general is to find a minimal set of axioms. We prefer to assume as little as possible at the base of things. The more things we can build from base-principles the better. However, you should be aware that it has been proven in mathematics that there are questions which are undecideable. Godel showed that any system of mathematics which contains arithmetic will necessarily have unanswerable "statements". That is they will not fit the narrow-minded definition of proposition we gave the first day in this course. Godel showed it will not be possible to prove them true or false. Thus, even after we choose suitable axioms for a particular realm of mathematics we will not necessarily be able to answer all questions. This would seem to cast aspersion on those rather ambitious physicists who seek a theory of everything. If mathematics is not entirely self-contained then what hope have we that physics will explain itself?

Next, we prove the product of an integer and its immediate successor is an even integer.

Example 2.2.5. Prove: The product of x and $x+1$ is even for each $x \in \mathbb{Z}$.
Proof: Let $x \in \mathbb{Z}$ be an integer. It is clear that x is either even or odd. Let us proceed casewise:

1.) **even case:** *$x = 2m$ for $m \in \mathbb{Z}$. The immediate successor of x is $x + 1 = 2m + 1$. Note that $x(x+1) = 2m(2m+1) = 2[m(2m+1)]$ and $m(2m+1) \in \mathbb{Z}$ thus $x(x+1)$ is even.*

2.) **odd case:** *$x = 2m + 1$ for $m \in \mathbb{Z}$. The immediate successor of x is $x + 1 = 2m + 2$. Note that $x(x+1) = (2m+1)(2m+2) = 2[(2m+1)(m+1)]$ and $(2m+1)(m+1) \in \mathbb{Z}$ thus $x(x+1)$ is even.*

Therefore, as $x \in \mathbb{Z}$ was arbitrary, we find $x(x+1)$ is even $\forall x \in \mathbb{Z}$. □

In the example above, we assumed x was a generic integer. When we wish to prove some claim for all objects it is crucial that we make no additional assumptions beyond what is contained in the given claim. For example, this proof would have been incomplete is we had assumed that the integer was even from the beginning. When we added that even assumption in one case we were obliged to address the other odd case seperately.

The logic of cases follows from the tautology below:

$$[P_1(x) \vee P_2(x)] \Rightarrow Q(x) \ \Leftrightarrow \ [P_1(x) \Rightarrow Q(x)] \vee [P_2(x) \Rightarrow Q(x)]$$

Actually, the tautology is less strict then what we usually mean by breaking up into "cases". The statement above does not assume the cases are non-overlapping. In the example, $P_1(x)$ was "x is even" while $P_2(x)$ was "x is odd". Clearly, $P_1(x) \wedge P_2(x)$ is a contradiction for $x \in \mathbb{Z}$. However, we could even break up into cases which overlapped. So long as the cases cover all possibilities for the quantifier then we can conclude the proof holds for all $x \in U$. The preceding example had $U = \mathbb{Z}$.

Remark 2.2.6. *In the example 2.2.4 we would have to have treated 4 cases for the different sign combinations of a, b. Fortunately, we knew $|x| = \sqrt{x^2}$ which is super-nice since it avoids cases. Beware, not all questions about absolute value can be nicely solved without resorting to cases. Take a look at my proof of case (5.) for Theorem 1.4.7. Sometimes, that sort of casewise work is just unavoidable.*

Example 2.2.7. Let $a, b \in \mathbb{Z}$. If $a, b > 0$ and $a|b$ and $b|a$, then $a = b$.
Proof: since $a|b$, $\exists x \in \mathbb{Z}$ such that $b = ax$. Moreover, since $b|a$, $\exists y \in \mathbb{Z}$ such that $a = by$. Since $a, b > 0$ it follows that $x, y > 0$ thus,

$$\frac{b}{a} = x \text{ and } \frac{b}{a} = \frac{1}{y} \quad \Rightarrow x = \frac{1}{y}$$

This is a very interesting equation in $\mathbb{Z}$. It says that y has a multiplicative inverse of x. There are only two integers with multiplicative inverses, 1 and -1. We have $x > 0$ thus we find the solution must be $x = 1$. The claim follows. □

Example 2.2.8. Let $a, b, c, d \in \mathbb{Z}$, if $a|b$ and $c|d$ then $ac|bd$.
Proof: since $a|b$, $\exists x \in \mathbb{Z}$ such that $b = ax$. Moreover, since $c|d$, $\exists y \in \mathbb{Z}$ such that $d = cy$. Observe

$$bd = (ax)(cy) = ac(xy) = acj$$

where $j = xy \in \mathbb{Z}$ thus $ac \mid bd$. □

2.3 proof by contradiction

The following is an example of "proof by contradiction" or the "method of indirect proof". We assume the negation of the claim then work towards seeing why it is unreasonable. Then once we see the negation is always wrong we conclude that the claim must be true. The symbol $\rightarrow\leftarrow$ means "contradiction", it points out there is a proposition in the proof which is always false. To be kind to the reader it is nice to announce you are using proof by contradiction at the beginning of the proof. It is also nice to point out explicitly what the contradiction is. Mathematicians are not always nice.

Example 2.3.1. The circle $x^2 + y^2 = 1$ does not intersect the line $y = 2$.
Proof (by contradiction): Assume that the circle and line intersect. If (a, b) is a point of intersection then that point must satisfy both the equation of the line and the equation of the circle:

$$(i.)\ a^2 + b^2 = 1 \qquad\qquad (ii.)\ b = 2$$

But then if we substitute (ii.) into (i.) we obtain $a^2 + 4 = 1$ which is equivalent to $a^2 = -3$, thus $a \notin \mathbb{R}$ which provides a $\rightarrow\leftarrow$. Therefore, using proof by contradiction, we find the circle does not intersect the line. □

The contradiction here was that $a \in \mathbb{R}$ and $a \notin \mathbb{R}$. This proof method is logically anchored to the tautology we saw in Theorem 1.1.13 part (9.) the *basis for indirect proof:*

$$P \Leftrightarrow [(\sim P) \implies (Q \wedge \sim Q)].$$

The interesting thing about this pattern is that Q appears just on the RHS. There is a lot of freedom in what Q is seen to be. In practice, for a given problem is does have something to do with P but not directly. Here P was the proposition that the circle intersected the line, however Q was the proposition that a was a real number. You can easily verify that Q is not some trivial logical operation applied to P. The connection between P and Q stems from the theory behind the proof, not from logic alone. We should discuss a definition and theorem before our next example.

Definition 2.3.2. *Let $p \in \mathbb{N}$ with $p \neq 1$ then we say that p is a* **prime** *iff the only factors of p are p and 1. If $n \in \mathbb{N}$ and $n = ab$ where $1 \neq a, b \in \mathbb{N}$ then n is a* **composite** *integer.*

There is an obvious extension of the concept of primes to $\mathbb{Z}$, if we wish to talk about primes in the context of both positive and negative integers then we define a prime to be integer $p \neq 0, 1$ for which the only divisors of p are $\pm p$ and ± 1. I'll try to focus our attention to positive primes.

Theorem 2.3.3. *Fundamental Theorem of Arithmetic (FTA). Let $n \in \mathbb{N}$ then there exist distinct primes $p_1, p_2, \dots, p_s$ and exponents $m_1, \dots, m_s \in \mathbb{N}$ for some $s \in \mathbb{Z}$ with $s \geq 0$ such that*

$$n = p_1^{m_1} p_2^{m_2} \cdots p_s^{m_s}.$$

Here $s = 0$ gives $n = 1$ in our current notation. Furthermore, if there is any other collection of distinct primes $q_1, q_2, \dots, q_r$ and exponents $n_1, \dots, n_r \in \mathbb{N}$ for some $r \in \mathbb{Z}$ with $r \geq 0$ and

$$n = q_1^{n_1} q_2^{n_2} \cdots q_r^{n_r}$$

then $s = r$ and $q_1^{n_1}, q_2^{n_2}, \dots, q_r^{n_r}$ is the same list as $p_1^{m_1}, p_2^{m_2}, \dots, p_s^{m_s}$.

In words, the FTA says there is a unique (up to re-ordering) decomposition of any positive integer into a product distinct prime powers. For the purpose of making the following proof exceedingly clear, let us square the prime decomposition for n and see what happens:

$$n^2 = (p_1^{m_1} p_2^{m_2} \cdots p_s^{m_s})^2 = (p_1^{m_1})^2 (p_2^{m_2})^2 \cdots (p_s^{m_s})^2 = p_1^{2m_1} p_2^{2m_2} \cdots p_s^{2m_s}.$$

We find each power in the prime factorization of a square must be even.

Example 2.3.4. The $\sqrt{2}$ is irrational.
Proof (by contradiction): Assume that $\sqrt{2}$ is rational. Then there exist $a, b \in \mathbb{Z}$ such that $\sqrt{2} = \frac{a}{b}$. Hence, $2 = \frac{a^2}{b^2}$ which yields $2b^2 = a^2$. By the Fundamental Theorem of Arithmetic both a and b can be factored into a unique(upto ordering) product of primes. Clearly a^2 will have an even number of factors since the total number of factors for the product of aa is twice that of a. Likewise for b. We argue that a^2 and b^2 have an even number of factors of 2. Consider then $2b^2 = a^2$, since b^2 has an even number of two-factors in its factorization when we multiply by 2 we find $2b^2$ has an odd number of two-factors. Thus, as $2b^2 = a^2$ we find a^2 has an odd-number of two-factors, a $\rightarrow\leftarrow$. Therefore, using proof by contradiction, we find $\sqrt{2} \notin \mathbb{Q}$. $\square$

Notice the contradiction came from something only tangentially related to the main thrust of the theorem here. Many people (myself included) find proof by contradiction less than satisfying. Take the proof above, it leaves us with an obvious question: if $\sqrt{2}$ is not rational then what is it? The proof tells us nothing about that. Proof by contradiction is a useful method despite these comments. To reject this method of proof is to reject much of modern mathematics. I use it as a last resort. When possible, I prefer a proof which is **constructive**. Hilbert agrees, in 1928 he wrote in *Die Grundlagen der Mathematik*,

> "Taking the principle of excluded middle from the mathematician would be the same, say, as proscribing the telescope to the astronomer or to the boxer the use of his fists"

There is a camp of mathematicians who follow "mathematical intuitionism". Such mathematicians reject proof by contradiction as a valid method of proof. The founder of this camp was a Dutch mathematician named Luitzen Egbertus Jan Brouwer. At an early age he proved the highly non-trivial topological fixed point theorem. Mathematical intuitionism views mathematics as the formulation of mental constructions that are governed by self-evident laws. Brouwer had interesting opinions (Brouwer was apparently not a fan of applied mathematics):

> *"The construction itself is an art, its application to the world an evil parasite."*

I should mention that the school of "constructivist" mathematics is larger than that of intuitionism. Besides avoiding proof by contradiction, constructivists also eschew the use of the *Axiom of Choice*. If a proof relies on the Axiom of Choice then at some point it chooses objects that could not be constructed explicitly for some reason. Constructive mathematicians do not necessarily disagree with the results the follow from the Axiom of Choice. In fact, one goal is to give new constructive proofs that avoid the Axiom of Choice. This is not always possible. Certain statements in mathematics have been shown to produce the Axiom of Choice and vice-versa. For example, Sierpinski proved that Zermelo Franklin Set Theory with no Axiom of Choice (ZF) and the Generalized Continuum Hypothesis(GCH) implies the Axiom of Choice(AC), so AC and GCH are not independent in ZF. In short, there are still open questions here and the story is much deeper than I have sketched here.

I should mention that constructivists have mellowed a little since the days of Leopold Kronecker. In a famous quote he argued that arithmetic and analysis must be founded on "whole numbers", saying, "God made the integers; all else is the work of man"

If you were wondering how to define $\mathbb{R}$, a concise explaination is that it is *closure* of $\mathbb{Q}$. We can define the real numbers to be the union of the rational numbers and the accumulation points for all Cauchy-sequences of rational numbers. This is not part of the required material of Math 200, but I figure some of you are interested. You might be able to fill in the details of this idea of "closure" when you have completed the real analysis course here at LU. The structure of the real numbers is more subtle than our early education would have us believe.

2.4 proof by contraposition

In Theorem 1.1.13 part (8.) we saw the *law of contraposition:*

$$(P \Rightarrow Q) \Leftrightarrow (\sim Q \Rightarrow \sim P)$$

What this means is to prove the implication $P \Rightarrow Q$ we may instead choose to prove $\sim Q \Rightarrow \sim P$. This logical slight of hand is known as **proof by contraposition**.

Example 2.4.1. Let $x \in \mathbb{Z}$, if 8 does not divide $x^2 - 1$ then x is even.

Setting the Stage: *identify P as the sentence "$x^2 - 1$ does not divide 8" and Q as the sentence "x is even". We aim to prove $\sim Q \Rightarrow \sim P$. This means we should assume $\sim Q$ and works towards arguing $\sim P$ is true. Notice $\sim P$ is true if* 8 **does** *divide $x^2 - 1$.*

Proof (by contraposition): Suppose that x is not even, then x is odd. Thus there exists $m \in \mathbb{Z}$ such that $x = 2m + 1$. Consider,

$$\begin{aligned} x^2 - 1 &= (2m+1)^2 - 1 && (2.1)\\ &= 4m^2 + 4m + 1 - 1 && (2.2)\\ &= 4m(m+1) && (2.3)\\ &= 4(2k) \qquad m(m+1) \textit{ is even by a previous example, } k \in \mathbb{Z} && (2.4)\\ &= 8k. && (2.5) \end{aligned}$$

Thus $8|(x^2 - 1)$. Therefore, we find if 8 does not divide $x^2 - 1$ then x is even by proof by contraposition.□

Example 2.4.2. Let $x, y \in \mathbb{Z}$, if $x + y$ is even, then either x and y are even or x and y are odd.

Setting the Stage: *identify P as the statement "$x + y$ is even" and Q as the sentence "either x and y are even or x and y are odd". We aim to prove $\sim Q \Rightarrow \sim P$. This means we should assume $\sim Q$ and works towards arguing $\sim P$ is true. Notice $\sim P$ is true if $x + y$ is not even which is to say $x + y$ is odd*[1].

Proof (by contraposition): suppose both x and y are not even and both x, y are not odd. Then, either x or y must be even. Without loss of generality suppose x is even and y is odd. Then there exist $m, n \in \mathbb{Z}$ for which

$$x = 2m \qquad \& \qquad y = 2n + 1$$

by the definition of even and odd integers. Notice,

$$x + y = 2m + 2n + 1 = 2(m + n) + 1 = 2k + 1$$

where $k = m + n \in \mathbb{Z}$ hence $x + y$ is an odd integer. Therefore, $x + y$ is not an even integer. Therefore, using proof by contraposition, we have shown if $x + y$ is even, then either x and y are even or x and y are odd. □

2.5 biconditional proofs

To prove a biconditional statement we can prove a conditional statement and its converse, as was given in (9.) of Theorem 1.1.14

$$(P \Leftrightarrow Q) \Leftrightarrow [(P \Rightarrow Q) \wedge (Q \Rightarrow P)]$$

[1] perhaps you see a logical gap in these notes, you say, I haven't proved that an integer is either even or odd, but not both... correct, I have not proved that as far as I remember, but, good news, it is a problem in your homework, so, soon you will be able to prove it.

The phrase "iff" is a shibboleth for "if and only if"[2]. If you were to write an article for a journal or a chapter of a book etc. then you should write out the words "if and only if". I speak from personal experience. But, for classwork and boardwork, "iff" is a great shortcut.

Example 2.5.1. Let $a \in \mathbb{Z}$. Then a is odd iff $a+1$ is even.
Proof: Suppose a is odd, then there exists $k \in \mathbb{Z}$ such that $a = 2k+1$. Observe that $a+1 = 2k+1+1 = 2(k+1)$ where $k+1 \in \mathbb{Z}$ thus $a+1$ is even.
Conversely suppose that $a+1$ is even, then there exists $m \in \mathbb{Z}$ such that $a+1 = 2m$. Observe that $a = 2m-1 = 2m-2+1 = 2(m-1)+1$ where $m-1 \in \mathbb{Z}$ thus a is odd. Therefore a is odd iff $a+1$ is even. □

We might benefit from having another characterization of odd integers.

Example 2.5.2. Let $a \in \mathbb{Z}$. Then a is odd iff there exists $j \in \mathbb{Z}$ for which $a = 2j-1$.
Proof: Suppose a is odd, then there exists $k \in \mathbb{Z}$ such that $a = 2k+1$. Observe that

$$a = 2k+1 = 2k+2-1 = 2(k+1)-1 = 2j-1$$

where $j = k+1 \in \mathbb{Z}$.
Conversely suppose there exists $j \in \mathbb{Z}$ such that $a = 2j-1$. Observe that

$$a = 2j-1 = 2j-2+1 = 2(j-1)+1 = 2k+1$$

where $k = j-1 \in \mathbb{Z}$ hence a is odd by definition. We conclude a is odd iff there exists $j \in \mathbb{Z}$ for which $a = 2j-1$. □

2.6 proofs involving quantifiers; existence proofs

If we just need to show existence then an example will do.

Example 2.6.1. If $f(n) = 2^n$ then $\exists n \in \mathbb{N}$ such that $f(n)$ is prime
Proof: Observe that $f(1) = 2^1 = 2$ is prime. Thus, there exists $n \in \mathbb{N}$ such that $f(n)$ is prime. □

If we need to show unique existence then we must find an example and then show that any other example is the same one we already found.

Example 2.6.2. Suppose $m, b \in \mathbb{R}$ such that $m \neq 0$. There is a unique x-intercept to the line $y = mx+b$.
Proof: The intercept has $y = 0$ thus $0 = mx+b$ yielding $x = -b/m$ since $m \neq 0$ allows the required division. Suppose that x_2 is another x-intercept then $0 = mx_1 + b$ and we find $x_1 = -b/m$ hence there is just one x-intercept, namely $x = -b/m$. □

In truth, most of the proofs we have thus far discuused were "for all" proofs since we argued some property for an arbitrary object or pair of objects. For example,

- Example 2.2.7 argues for $\forall (a, b \in \mathbb{N})\, (a|b \wedge b|a \Rightarrow a = b)$
- Example 2.2.8 argues $\forall (a, b, c, d \in \mathbb{Z})\, (a|b \wedge c|d \Rightarrow ac|bd)$

We also looked at a couple non-existence proofs:

[2] if a person doesn't know what iff means then we can easily identify them as an outsider, see Judges 12:5-6.

- Example 2.3.1: There does not exist a point on both the circle and the line
- Example 2.3.4: $\sqrt{2} \notin \mathbb{Q}$.

If you examine those proofs you'll see that we proved those assertions by contradiction. In particular, $\sim [(\exists x)P(x)] \Leftrightarrow (\forall x)(\sim P(x))$.

Example 2.6.3. Prove there exist integers x, y for which $3x + 5y = 1$.

Proof: Observe $3(2) + 5(-1) = 1$ *thus* $x = 2$ *and* $y = -1$ *are integers which solve* $3x + 5y = 1$. □

Example 2.6.4. Prove there do not exist integers x, y for which $3x + 12y = 1$.

Setting the Stage: *usually to prove non-existence it is most natural to use proof by contradiction.*

Proof (by contradiction): Suppose there exist integers x, y *for which* $3x + 12y = 1$ *then observe* $3(x + 4y) = 1$ *thus* $x + 4y = \frac{1}{3}$ *which is absurd since* $x, y \in \mathbb{Z}$ *gives* $x + 4y \in \mathbb{Z}$ *and clearly* $\frac{1}{3} \notin \mathbb{Z}$. *Therefore, using proof by contradiction, we conclude there do not exist integers* x, y *for which* $3x + 12y = 1$. □

Let's look at a proof that involves both $\exists$ and $\forall$. I assume you know what a function is from calculus, we will return to functions later in this course and take a deeper look, but for now I rest on your knowledge from Calculus II and its prerequisites.

Example 2.6.5. All functions on $\mathbb{R}$ are the sum of an even function and an odd function

Setting the Stage: *if* $\mathcal{F}$ *is the set of all functions from* $\mathbb{R}$ *to* $\mathbb{R}$ *then symbolically we face*

$$\forall(f \in \mathcal{F})\exists(f_o, f_e \in \mathcal{F})\,(f = f_o + f_e \wedge [\forall(x \in \mathbb{R})(f_o(-x) = -f_o(x))] \wedge [\forall(x \in \mathbb{R})(f_e(-x) = f_e(x))])$$

To argue this we must study an arbitrary function f *and show it can be written as the sum of* f_o *and* f_e. *The heart of the proof before is a bit of a trick, it involves adding zero in a clever fashion.*

Proof: Let me restate the claim: for each function f, *there exists an odd function* f_o *and an even function* f_e *such that* $f = f_o + f_e$. *Here I can give a constructive proof. Given the function* f, *define*

$$f_e(x) = \frac{1}{2}\Big(f(x) + f(-x)\Big) \qquad\qquad f_o(x) = \frac{1}{2}\Big(f(x) - f(-x)\Big)$$

Clearly, $f(x) = f_o(x) + f_e(x)$ *for each* $x \in \mathbb{R}$ *thus* $f = f_o + f_e$. *Moreover, we can check that* $f_e(-x) = f_e(x)$ *and* $f_o(-x) = -f_o(x)$ *for each* $x \in \mathbb{R}$. □

Notice, that we cannot prove the assertion by just taking a particular example and showing it works. It is true that $f(x) = x + x^2$ has $f_e(x) = x^2$ and $f_o(x) = x$ but that is not enough to prove the claim in the example. It was important we took an arbitrary function.

Remark 2.6.6. *By the way, another fun example is*

$$e^x = \underbrace{\frac{1}{2}(e^x + e^{-x})}_{\cosh x} + \underbrace{\frac{1}{2}(e^x - e^{-x})}_{\sinh(x)}$$

Note $\cosh(x)$ *is even while* $\sinh(x)$ *is odd and* e^x *is neither even nor odd. Notice the similarity with Euler's Formula for the imaginary exponential* $e^{ix} = \cos x + i \sin x$. *In fact,*

$$\cos x = \frac{1}{2}(e^x + e^{-x}) \qquad \& \qquad \sin x = \frac{1}{2i}(e^x + e^{-x}).$$

The formulas above unlock many mysteries of trigonometry.

2.7 necessary conditions verses sufficient conditions

A condition is said to be "necessary" when it is needed for the conclusion to follow. A condition is said to be "sufficient" when the conclusion follows automatically on the basis of that condition alone. However, every sufficient condition is not necessarily a necessary condition because the sufficient condition might contain extra uneeded assumptions.

Example 2.7.1. *Consider $s = \sum_{n=0}^{\infty} c_n$. The condition $\lim_{n\to\infty} c_n = 0$ is a necessary condition for the series s to converge. However, it is not sufficient since $\sum_{n=0}^{\infty} \frac{1}{n}$ diverges.*

A necessary and sufficient condition for s to converge is that the limit of the partial sums of s converges. Indeed, the condition on the sequence of partial sums is precisely the definition of convergence of a series.

Another sufficient condition would be that the series is alternating and the postive terms go to zero. For example, the alternating $p = 1$ series converges to $\ln(2)$; $1 - 1/2 + 1/3 - 1/4 + \cdots = \ln(2)$. However, the alternating condition is certainly not necessary since there exist convergent series which are not alternating. For example, $1 + 1/2 + 1/2^2 + \cdots = \frac{1}{1-1/2} = 2$ is a well-known convergent geometric series which is not alternating. Perhaps you recall from Calculus II we learned a number of criteria that were sufficient for the series to converge.

Example 2.7.2. *Differentiability of a function at a point is a sufficient condition for continuity of a function at that point. However, differentiability is not a necessary condition since $f(x) = |x|$ is continuous and not differentiable at zero.*

There are conditions which are both necessary and sufficient conditions. Every good definition has this form. A well-thought out defintion gives the conditions which are necessary and sufficient to encapsulate an idea.

Remark 2.7.3. *Collecting both necessary and sufficient conditions for a given mathematical claim is a wise course of study. Generally, to understand a mathematical concept we need both examples and counter-examples as to compare and contrast the idea with other ideas we already know. Math is not a collection of independent stories, rather, it is a vast map with all sorts of special missions which at times give surprising insights into missions on the completely opposite side of the map. Nearly every course you take you will need to use in future courses in some way or another. Also, for those of you thinking about graduate school in mathematics, the Math Subject GRE will test everything. Everything I ever talked about in calculus but didn't find a way to put it on the test. That is the question on the GRE. To paraphrase a quote from a past student, a very good student, "that test was just evil". The nice thing is, if you ace that test it usually opens many doors for graduate school.*

Chapter 3

Set Theory

Brilliant mathematicians have spent their lifetimes refining the nuanances of axiomatic set theory. It is a story involves Cantor, Russel, Hilbert, Zermelo, Fraenkel, Godel and Cohen and a host of others too numerous to name. Cantor proved many interesting results in the late 19-th century. Particularly, Cantor developed ideas about infinity that boggle the mind. Cantor gave arguments that led to a string of infinities each one larger than the last. However, Cantor built his theory on an intuitive foundation. In short, Cantor failed to rule out the ”set of all sets” begin a set. This is known as Russel’s paradox, it can be restated as:

> ”A barber in a certain town has stated he will cut the hair of all those persons and only those persons who do not cut their own hair. Does the barber cut his own hair?”

In response to this problem, Zermelo provided a set of axioms on which to base set theory. Later, Fraenkel refined Zermelo’s axioms further. The axiom of choice found a prominent place among these axioms. Moreover, the axiom of choice proved useful in many new branches of mathematics such as infinite dimensional linear algebra, topology, algebraic topology, ring theory and so forth... From a pragmatical perspective, many mathematicians would be reluctant to give up on the axiom of choice. However, another camp of mathematicians had deep misgivings about the axiom and Zermelo’s axioms in general.

Hilbert had also brought forth a set of axioms to describe geometry. However, in contrast to Zermelo he proved his axioms were consistent with something else which was known. Zermelo didn’t bother, instead he claimed they could probably be proved consistent with further effort. Around 1930 Godel put forth a series of powerful results. Godel showed that it was impossible to prove consistency. However, Godel did prove in 1935 that the axioms were ”relatively consistent”. Godel also showed that the continuum hypothesis was relatively consistent with Zermelo-Fraenkel axioms. Finally, in 1963 Paul Cohen was able to show that the axiom of choice and the continuum hypothesis are independent relative to Zermelo-Fraenkel axiomatic set theory (without the axiom of choice).

What this means is that there is not just one ”set-theory”. Rather, there are multiple axiom systems which put forth differing set theories. All of this said, we will not dwell on questions which cut so finely. I just wanted to give you a little sketch of some of the history here. My source for this discussion was section 18.1 of Victor Katz’ text *A History of Mathematics*, 2nd-ed. If you are interested in such things, its a nice source and it actually does have some math in it, not to mention antiquated notations. It’s a little dry though. Other books worth perusing for this sort of thing: *Men of Mathematics* by E.T. Bell, *Godel Escher Bach* by Douglas Hofstadter, and *Road to Reality* by Roger Penrose. Penrose's book has deep and insightful discussions of what calculus and advanced mathematics.

You can also read Chapter 1 of *Mathematical Proofs: a Transition to Advanced Mathematics* by Chattrand, Polimeni and Zhang., 4th-edition. These chapters overlap with the subject matter of this chapter of my notes. As before, if time permits, I may use that text or Wolf for additional examples. There are many additional practice problems there if you need further practice.

3.1 elements and subsets

Naive set theory rests on two axioms:

- **axiom of comprehension:** any collection of objects which you can describe and list can collectively viewed as a set
- **axiom of extensionality:** if two sets have the same elements then they are the same set. In other words, nothing but the elements contained in the set characterize the set.

It turns out these axioms lead to an inconsistent theory of sets. If you consider the set of all sets that are not members of themselves then this leads to a contradiction (this is known as Russel's Paradox). The solution to this problem is a bit murky, but it seems to me the main idea is to forbid the construction of the paradoxical set of sets. I'd rather not explain the technical details of the axiom system which accomplishes this... at least one solution is given by the Zermelo Frankel Cantor set theory. Wolf points out it has served mathematics well for a century, so, it seems it is a good work around. We practice naive set theory in the sense that we will not get into those axioms and we'll be content to set the foundations of the subject with a few believeable, but admittedly fuzzy, definitions.

Definition 3.1.1. *We say that a set is a collection of elements. If $x \in S$ then we say that x is an element of S. The set $\emptyset$ is the set with no elements. The set $\{a_1, a_2, \dots\}$ is in* **roster notation** *and it has elements $a_1, a_2, \dots$. The set below is in* **set-builder** *notation:*

$$\{x \in U \mid P(x)\}$$

contains elements in $x \in U$ which make $P(x)$ true.

A set with elements a, b, c is denoted { a,b,c }. Unless otherwise stated, no ordering is assumed and we keep only one of each distinct element. If $a = b$ then the set with elements a, b, c would just be $\{a, c\}$ or you could say $\{b, c\}$. There is some freedom in how we formulate a given set in the set-builder notation,

$$\{x \in U \mid P(x)\} = \{x \mid \forall(x \in U)(P(x))\}.$$

Definition 3.1.2. *If A and B are sets then $A = B$ iff A and B have the same elements.*

In other words, if $A = B$ then $x \in A$ iff $x \in B$. Conversely, if $x \in A$ iff $x \in B$ then $A = B$.

Example 3.1.3. *Same elements means same set: $\{a, b, c\} = \{b, c, a\} = \{c, a, b\}$.*

Example 3.1.4. *These are the same set, the* **empty set***, the set with no elements:*

$$\emptyset = \{x \in \mathbb{R} \mid x^2 = -1\} = \{n \in \mathbb{N} \mid n < 0\} = \{x \mid \sim P \wedge P\} = \{\}.$$

Example 3.1.5. *Let me illustrate another freedom the set-builder notation allows:*

$$S = \{n \in \mathbb{Z} \mid n = k^2 \text{ for some } k \in \mathbb{Z}\} = \{n \in \mathbb{Z} \mid \exists(k \in \mathbb{Z})(n = k^2)\} = \{k^2 \mid k \in \mathbb{Z}\}$$

Furthermore, $S = \{k^2 \mid k \in \mathbb{Z}\} = \{k^2 \mid k \in \mathbb{Z}, k \geq 0\} = \{0, 1, 4, 9, \dots\}$ where the last formulation of S is given in the roster notation. In words, S is the set of non-negative integer squares.

Subsets are important.

Definition 3.1.6. *Let A and B be sets, if $x \in A$ implies $x \in B$ for any $x \in A$ then we say that A is a* **subset** *of B and write $A \subseteq B$.*

In other words, $A \subseteq B \;\; \Leftrightarrow (\forall x)(x \in A \Rightarrow x \in B)$. Notice that $\emptyset \subseteq A$ for any set A. This follows trivially from the definition since there does not exist $x \in \emptyset$. Let me give some additional terminology which is nice to use at times:

Definition 3.1.7. *Let A and B be sets and assume $A \subseteq B$. We say B is a* **superset** *of A and write $B \supseteq A$ which is read "B* **contains** *A". If $A \neq B$ then A is a* **proper subset** *of B. If $A \neq \emptyset$ then A is a* **non-empty subset** *of B.*

Proposition 3.1.8. *Let A be a set, then $A \subseteq A$ and $\emptyset \subseteq A$.*

Proof: Let $x \in A$ then $x \in A$ therefore, $A \subseteq A$. Since $\exists x \in \emptyset$ is false the implication $x \in \emptyset \Rightarrow x \in A$ is true. Therefore, $\emptyset \subseteq A$. $\square$

Proposition 3.1.9. *Let A, B be sets. Then $A = B$ iff $A \subseteq B$ and $B \subseteq A$.*

Proof: if $A = B$ then A and B have the same elements thus $x \in A$ implies $x \in B$ and likewise $x \in B$ implies $x \in A$. Consequently, by definition of subset, $A \subseteq B$ and $B \subseteq A$.

Conversely, if we assume $A \subseteq B$ and $B \subseteq A$. Then if $x \in A$ we find $x \in B$ as $A \subseteq B$. Likewise, if $x \in B$ then $x \in A$ since $B \subseteq A$. Thus $A = B$ since we have argued these sets have the same elements. $\square$

Remark 3.1.10. *When we use the above proposition we often refer to it as* **double containment***. As in, we prove two sets are equal via arguing double containment of the given sets.*

Proposition 3.1.11. *Let A, B be sets with no elements, then $A = B$.*

Proof: $(\forall x)(x \in A \Rightarrow x \in B)$ is trivially true since the antcedent $x \in A$ is false. Thus $A \subseteq B$. By symmetry $B \subseteq A$ thus $A = B$. $\square$

The proposition above shows that the empty set is unique. When we say $\emptyset$ there is no ambiguity in what is meant. You might be tempted to think that the empty set in different contexts is a different empty set, but we have no such freedom when we work with the definitions which have been given in this work. The empty set in a set of functions is the same empty set as the empty set in a set of cats.

Example 3.1.12 (Constructing Natural Numbers)**.** *The natural numbers are also called counting numbers for the obvious reason. Let me sketch how you can construct* $\mathbb{N}$ *from set theory:*

$$\begin{aligned} &0 \approx \emptyset \\ &1 \approx \{\emptyset\} \\ &2 \approx \{\emptyset, \{\emptyset\}\} \\ &3 \approx \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\} \end{aligned}$$

Then addition in $\mathbb{N}$ *is defined in a somewhat subtle fashion. It's not just union. I leave the details for a different course.*

Remark 3.1.13. *All the number systems we commonly use can be constructed from base principles starting with the example above. Past* $\mathbb{N}$ *you can define* $\mathbb{Z}$ *in terms of differences of natural numbers. Then* $\mathbb{Q}$ *is the field of fractions for* $\mathbb{Z}$ *(which is something we carefully prove in the second course in Abstract Algebra). Obtaining* $\mathbb{R}$ *from* $\mathbb{Q}$ *is typically done either with the theory of completion from analysis or with Dedekind cuts as may be shown in the Real Analysis course. Then* $\mathbb{C}$ *is obtaining from* $\mathbb{R}$ *is fairly easy, I show several ways in the complex analysis class. Constructing* $\mathbb{C}$ *from* $\mathbb{R}$ *in the theory of field extensions is as simple as writing* $\mathbb{R}[x]/(x^2+1)$*. That creates as set of objects which obey the algebra of polynomials in* x *where we also impose* $x^2 = -1$*. Anyway, my larger point here is that we can't give you proper complete models of the standard number systems because you don't know enough math (yet). Learning new math is not just about new math, it is always about understanding basic math more deeply. So, for the time being, we are content to work with* $\mathbb{N}, \mathbb{Q}, \mathbb{R}$ *etc. in terms of their properties. You'll have to trust that they do in fact exist.*

3.2 set operations

You are probably already familar with unions and intersections. We use them in calculus in discussing domains and ranges etc... For example,

$$[0,1] \cup [1,2] = [0,2], \qquad (0,2] \cup [1,3) = (0,3), \qquad (0,2) \cap (1,3) = (1,2)$$

A point is in the union if it is in either set being unioned whereas a point is in the intersection if the point is in both sets. These concepts extend well past $\mathbb{R}$.

Definition 3.2.1. *Let* A, B *be sets then we define the* **union** *of* A *and* B *as follows:*

$$A \cup B = \{x | x \in A \text{ or } x \in B\}$$

Example 3.2.2. *Let* $\mathcal{E} = 2\mathbb{Z} = \{2k \mid k \in \mathbb{Z}\}$ *be the set of even integers and let* $\mathcal{O} = 2\mathbb{Z} + 1 = \{2k+1 \mid k \in \mathbb{Z}\}$ *be the set of odd integers. Clearly* $\mathcal{E}, \mathcal{O} \subseteq \mathbb{Z}$*. Then we claim* $\mathcal{E} \cup \mathcal{O} = \mathbb{Z}$*.*

Proof: *if* $x \in \mathcal{E} \cup \mathcal{O}$ *then* $x \in \mathcal{E}$ *or* $x \in \mathcal{O}$ *hence* $x \in \mathbb{Z}$ *as* $\mathcal{E}, \mathcal{O} \subseteq \mathbb{Z}$*. Therefore,* $\mathcal{E} \cup \mathcal{O} \subseteq \mathbb{Z}$*.*

Next suppose $x \in \mathbb{Z}$*. If* $2 \mid x$ *then* $x = 2k$ *for* $k \in \mathbb{Z}$ *hence* $x \in \mathcal{E}$*. Otherwise* $2 \nmid x$*. Recall we proved* x *is odd iff* $x+1$ *is even. Notice* $2 \nmid x$ *means* x *is not even hence* $x+1$ *cannot be odd. Thus* $x+1$ *is even which means* $x+1 = 2k$ *for some* $k \in \mathbb{Z}$ *and we find* $x = 2k-1 \in \mathcal{O}$*. Thus, in all cases,* $x \in \mathcal{E} \cup \mathcal{O}$*. Hence* $\mathbb{Z} \subseteq \mathcal{E} \cup \mathcal{O}$ *and we conclude by double containment,* $\mathcal{E} \cup \mathcal{O} = \mathbb{Z}$*.* $\square$

There may be an easier way to argue $\mathcal{E} \cup \mathcal{O} = \mathbb{Z}$. Certainly if we had already studied the division algorithm I would have given a different argument.

Definition 3.2.3. *Let A, B be sets then we define the* **intersection** *of A and B as follows:*

$$A \cap B = \{x | x \in A \text{ and } x \in B\}$$

When the intersection is empty that is often interesting. We give this a name:

Definition 3.2.4. *Sets A and B are* **disjoint** *if $A \cap B = \emptyset$. If $A \cap B \neq \emptyset$ then A and B* **meet***.*

Example 3.2.5. $\mathbb{N} \cap (0, 3) = \{1, 2\}$ *whereas* $\mathbb{N} \cap (0, 1) = \emptyset$.

Example 3.2.6. $\mathbb{N} \cap \mathbb{Q} = \mathbb{N}$*. In fact, generally if $A \subseteq B$ then $A \cap B = B$. Try proving it.*

Definition 3.2.7. *Let A, B be sets then we define the* **difference** *of A and B as follows:*

$$A - B = \{x | x \in A \text{ and } x \notin B\}$$

Sometimes $A - B$ is also called the **complement** *of B in A.*

The concept of set difference is sometimes taken relative to a universal set U, in that case the difference is called the *complement* of a set:

Definition 3.2.8. *If U is the universe and $B \subseteq U$ then the* **complement** *of B relative to U is $\widetilde{B} = U - B$.*

Example 3.2.9. *Let $U = \mathbb{R}$ then $\widetilde{[0, 1]} = (-\infty, 0) \cup (1, \infty)$. Another fun example: $\widetilde{\emptyset} = \mathbb{R}$. The complement of the rational numbers $\mathbb{Q}$ is $\widetilde{\mathbb{Q}} = \mathbb{R} - \mathbb{Q} = \mathbb{I}$ the set of irrational numbers. We proved that $\sqrt{2} \in \widetilde{\mathbb{Q}}$.*

Example 3.2.10. *Let $A = \{1, 2, 3\}$, $B = \{0, 1, 2\}$ and $C = \{4, 5\}$ then*

$$\begin{aligned} A \cup B &= \{0, 1, 2, 3\} \\ A \cap B &= \{1, 2\} \\ A - B &= \{3\} \\ B - A &= \{0\} \\ A \cap C &= B \cap C = \emptyset \end{aligned}$$

We see that C is disjoint from A and B.

Examples are not nearly as fun as theorems. There are many things we can say in general for set operations.

Theorem 3.2.11. *Let A, B and C be sets,*

(a.) *If $A \subseteq B$ and $B \subseteq C$ then $A \subseteq C$.*

(b.) $A \subseteq A \cup B$.

(c.) $A \cap B \subseteq A$.

(d.) $A \cap \emptyset = \emptyset$.

(e.) *$A \cup \emptyset = A$.*

(f.) *$A \cap A = A$.*

(g.) *$A \cup A = A$.*

(h.) *$A \cup B = B \cup A$.*

(i.) *$A \cap B = B \cap A$.*

(j.) *$A - \emptyset = A$.*

(k.) *$\emptyset - A = \emptyset$.*

(l.) *$A \cup (B \cup C) = (A \cup B) \cup C$.*

(m.) *$A \cap (B \cap C) = (A \cap B) \cap C$.*

(n.) *$A \cap (B \cup C) = (A \cap B) \cup (A \cap C$.*

(o.) *$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.*

(p.) *$A \subseteq B$ iff $A \cup B = B$.*

(q.) *$A \subseteq B$ iff $A \cap B = A$.*

(r.) *If $A \subseteq B$, then $A \cup C \subseteq B \cup C$.*

(s.) *If $A \subseteq B$, then $A \cap C \subseteq B \cap C$.*

Proof: follows quickly from the definition of subsets, unions, differences and intersection in each case. I would wager we will prove some of these in class or homework or both. □.

Theorem 3.2.12. *Let U be the universe of discourse and $A, B \subseteq U$,*

(a.) *$\tilde{\tilde{A}} = A$.*

(b.) *$A \cup \tilde{A} = U$.*

(c.) *$A \cap \tilde{A} = \emptyset$.*

(d.) *$A - B = A \cap \tilde{B}$.*

(e.) *$A \subseteq B$ iff $\tilde{B} \subseteq \tilde{A}$.*

(f.) *$\widetilde{A \cup B} = \tilde{A} \cap \tilde{B}$. (De Morgan's Law)*

(g.) *$\widetilde{A \cap B} = \tilde{A} \cup \tilde{B}$. (De Morgan's Law)*

(h.) *$A \cap B = \emptyset$ iff $A \subseteq \tilde{B}$.*

Proof: follows quickly from the definitions of subsets, unions, differences and intersection in each case. We'll work out some in lecture. A Venn diagram is a good place to start some of the proofs, it helps guide the proof □.

Remark 3.2.13. *$\widetilde{A \cap B} = \tilde{A} \cup \tilde{B}$ and $\widetilde{A \cup B} = \tilde{A} \cap \tilde{B}$ are called De Morgan's Laws for set theory because they rest on the laws of logic by the name name. Suppose $x \in \tilde{A} \cup \tilde{B}$ then $x \in \tilde{A}$ or $x \in \tilde{B}$ hence $\sim (x \in A) \vee \sim (x \in B)$ which, by De Morgan's Law, gives $\sim [(x \in A) \wedge (x \in B)]$ which means $\sim [x \in A \cap B]$ thus $x \notin A \cap B$. We find $x \in \widetilde{A \cap B}$. Hence, $\tilde{A} \cup \tilde{B} \subseteq \widetilde{A \cap B}$. The proof of the other containment is left as an exercise for the reader.*

3.3 families of sets

A family of sets is simply a set of sets. For example, the power set of S is the family of all subsets of S. Often it is convenient to label the sets in the family by elements from an *indexing* set.

Definition 3.3.1. *Let $\Delta \neq \emptyset$. If there exists a set A_α for each $\alpha \in \Delta$ then $\mathcal{A} = \{A_\alpha | \alpha \in \Delta\}$ is a family of sets indexed by Δ. The elements of Δ are called* **indices** *in this context.*

Example 3.3.2. *Let $A_n = (0, n)$ for each $n \in \mathbb{N}$. The family of sets $\{(0,1), (0,2), \dots\} = \{(0,n) | n \in \mathbb{N}\}$ is indexed by the natural numbers $\mathbb{N}$.*

We can define unions and intersections over families of sets:

Definition 3.3.3. *Let $\mathcal{A}$ be a family of sets, the union over $\mathcal{A}$ is,*

$$\bigcup_{A \in \mathcal{A}} A = \{x \mid \exists B \in \mathcal{A} \text{ such that } x \in B\}$$

If A has index set Δ we can write the union over $\mathcal{A}$ as,

$$\bigcup_{\alpha \in \Delta} A_\alpha = \{x \mid \exists \beta \in \Delta \text{ such that } x \in A_\beta\}$$

Finally, if we have the case $\Delta = \mathbb{N}$ then we can write the union over $\mathcal{A}$ as,

$$\bigcup_{i=1}^{\infty} A_i = \{x \mid \exists j \in \mathbb{N} \text{ such that } x \in A_j\}$$

We also may use the same notation for other subsets of $\mathbb{Z}$. (could run the index to negative values, or starting at zero, two or whatever is convenient to the problem)

Example 3.3.4. *Let $A_n = [0, n)$ for each $n \in \mathbb{N}$,*

$$\bigcup_{n=1}^{\infty} A_n = [0, \infty) \qquad \bigcup_{n=1}^{\infty} A_{1/n} = [0, 1)$$

Can you prove the assertions above ? It will be helpful to define the **floor function** *by $\lfloor y \rfloor$ by $\lfloor y \rfloor \in (y-1, y] \cap \mathbb{Z}$ for any $y \in \mathbb{R}$. For example, $\lfloor 0.2 \rfloor = 0$ and $\lfloor 2.2 \rfloor = 2$ and $\lfloor 1 \rfloor = 1$.*

Proof: *Let us examine why $[0,1) \subseteq \bigcup_{n=1}^{\infty} A_{1/n}$. Let $x \in [0,1)$. If $x = 0$ then $x \in [0,1) = A_{1/1}$ hence $x \in \bigcup_{n=1}^{\infty} A_{1/n}$. Otherwise, $0 < x < 1$ hence $1/x > 1$. Let $n = \lfloor 1/x \rfloor < 1/x$ since $1/x \notin \mathbb{N}$. Thus $n \in \mathbb{N}$ and $1/x > n$. We find $x < 1/n$ hence $x \in [0, 1/n) = A_{1/n}$ and so $x \in \bigcup_{n=1}^{\infty} A_{1/n}$. Thus $[0,1) \subseteq \bigcup_{n=1}^{\infty} A_{1/n}$.*

On the other hand, if $x \in \bigcup_{n=1}^{\infty} A_{1/n}$ then there exists $A_{1/k}$ which contains x for some $k \in \mathbb{N}$. That is, $x \in A_{1/k} = [0, 1/k)$ for some $k \in \mathbb{N}$. Therefore, $0 \leq x < 1/k$ and since $1/k \leq 1$ we find $0 \leq x < 1$. Hence $x \in [0,1)$ and we find $\bigcup_{n=1}^{\infty} A_{1/n} \subseteq [0,1)$. Finally, using double containment we conclude $\bigcup_{n=1}^{\infty} A_{1/n} = [0,1)$. □

Proof that $\bigcup_{n=1}^{\infty} A_n = [0, \infty)$ is probably much easier. I leave it to the reader.

Definition 3.3.5. *Let $\mathcal{A}$ be a family of sets, the intersection over $\mathcal{A}$ is,*

$$\bigcap_{A \in \mathcal{A}} A = \{x \mid x \in B \text{ for each } B \in \mathcal{A}\}$$

If A has index set Δ we can write the intersection over $\mathcal{A}$ as,

$$\bigcap_{\alpha \in \Delta} A_\alpha = \{x \mid x \in A_\beta \text{ for each } \beta \in \Delta\}$$

Finally, if we have the case $\Delta = \mathbb{N}$ then we can write the intersection over $\mathcal{A}$ as,

$$\bigcap_{i=1}^{\infty} A_i = \{x \mid x \in A_j \text{ for each } j \in \mathbb{N}\}$$

We also may use the same notation for other subsets of $\mathbb{Z}$. (could run the index to negative values, or starting at zero, two or whatever is convenient to the problem)

Example 3.3.6. *Let $A_n = (0, n)$ and $B_n = (-n, n)$ for each $n \in \mathbb{N}$,*

$$\bigcap_{n=1}^{\infty} A_n = (0, 1) \qquad \& \qquad \bigcap_{n=1}^{\infty} B_n = \{0\}.$$

This time I will prove the easier assertion.

Proof: *Let $x \in \bigcap_{n=1}^{\infty} A_n$ then $x \in A_n$ for every $n \in \mathbb{N}$. Thus $x \in A_1 = (0, 1)$ and we have shown $\bigcap_{n=1}^{\infty} A_n \subseteq (0, 1)$.*

Next suppose $x \in (0, 1)$. Then $0 < x < 1 \leq n$ for each $n \in \mathbb{N}$. Thus $x \in (0, n) = A_n$ for every $n \in \mathbb{N}$. Hence, by definition of intersection over $\mathbb{N}$, $x \in \bigcap_{n=1}^{\infty} A_n$. Consequently, $(0, 1) \subseteq \bigcap_{n=1}^{\infty} A_n$ and we conclude $\bigcap_{n=1}^{\infty} A_n = (0, 1)$ via double containment. $\square$

Given a particular set we can find all possible subsets of that set.

Example 3.3.7. *Suppose $S = \{a, b, c\}$. We observe that S has subsets:*

$$\emptyset,\ \{a\},\ \{b\},\ \{c\},\ \{a, b\},\ \{a, c\},\ \{b, c\},\ \{a, b, c\}.$$

A set with three elements apparently has $2^3 = 8$ subsets.

Definition 3.3.8 (Power Set)**.** *Given a set S the power set of S is the set of all subsets of S. We denote the power set of S by $\mathcal{P}(S)$. That is, $U \in \mathcal{P}(S)$ iff $U \subseteq S$.*

The power set of a given set is bigger than the set. In some sense, finding the power set is like exponentiating the set, crudely speaking.

Example 3.3.9. *Suppose $S = \{a, b, c\}$. The power set of S is:*

$$\mathcal{P}(S) = \{\emptyset,\ \{a\},\ \{b\},\ \{c\},\ \{a, b\},\ \{a, c\},\ \{b, c\},\ \{a, b, c\}\}.$$

Each element of the power set $\mathcal{P}$ is actually a subset of S.

Example 3.3.10 (fun with the empty set)**.** *There is a big difference between $\emptyset$ and $\{\emptyset\}$. The empty set has no elements, however the set containing the empty set has one element.*

$$\mathcal{P}(\emptyset) = \{\emptyset\}$$

$$\mathcal{P}(\mathcal{P}(\emptyset)) = \{\emptyset, \{\emptyset\}\}$$

$$\mathcal{P}(\mathcal{P}(\mathcal{P}(\emptyset))) = \{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}, \{\emptyset, \{\emptyset\}\}\}.$$

Notice that the empty set has no elements and the number of elements in $\mathcal{P}(\emptyset)$ is simply $2^0 = 1$; $\#(\mathcal{P}(\emptyset)) = 1$ where $\#(S)$ denotes the number of elements in the set S[1]*. Likewise,*

$$\#(\mathcal{P}(\mathcal{P}(\emptyset))) = 2^1 = 2$$

$$\#(\mathcal{P}(\mathcal{P}(\mathcal{P}(\emptyset)))) = 2^2 = 4$$

You might guess that if $\#(S) = n$ then $\#(\mathcal{P}(S)) = 2^n$. You would be correct, we can prove it by a technique known as **induction***.*

3.3.1 introduction to topology

Topology is the study of continuity. This branch of mathematics was refined in the first half of the twentieth century. Topological concepts lie at the base of most modern geometrical research. In short, a topology tells you what the open sets for a space are. The axiomatic and abstract definition given below is due to Riesz and Hausdorff. Most graduate students in mathematics will be required to take a course or two in topology. We have run an undergraduate level topology course in many recent years. Ask myself or Dr. Sprano if you wish to join us for this course sometime soon.

Definition 3.3.11. *A topology $\mathcal{T}$ for a set S is a family of subsets of S such that,*

(i.) *$\mathcal{T}$ must contain S and $\emptyset$.*

(ii.) *$\mathcal{T}$ is closed under any union of its elements,*

$$\bigcup_{U \in \mathcal{T}} U \in \mathcal{T}$$

(iii.) *$\mathcal{T}$ is closed under finite intersections of its elements. If $U_1, \dots U_n \in \mathcal{T}$ then*

$$\bigcap_{i=1}^{n} U_i \in \mathcal{T}$$

The sets in $\mathcal{T}$ are defined to be **open***. Moreover, a set is defined to be* **closed** *if its complement relative to S is open. A set S paired with a topology $\mathcal{T}$ is called a* **topological space***.*

We should all be familar with *open intervals* and *closed intervals* of $\mathbb{R}$. The open intervals are the simplest type of open set in $\mathbb{R}$. We could define the standard topology on $\mathbb{R}$ by letting $\mathcal{T}$ be the empty set together with collection of all open intervals and their unions. Since the finite

[1] there are many different notations for $\#S$ in various textbooks, just know this is not a "hashtag", I also use $|S|$ for this in other places such as the end of this course when we discuss the problem of counting when infinite sets are also involved

intersection of open intervals is again a union of open intervals, or the empty set, we will satisfy the three axioms for a topology. Notice that,

$$\mathbb{R} - [a, b] = (-\infty, a) \cup (b, \infty)$$

thus the complement of a closed interval is open. This means that the closed interval $[a, b]$ is in fact a closed set. These bizarre axioms will recover all the ordinary geometric definitions of open and closed with which we are more familar. The definintion above provides the basis for the field of *Point-Set Topology*. The other way to define open and closed sets is in terms of a metric. The concept of a metric space predates topology.

Definition 3.3.12. *A metric, or distance function, on a space M is a function $d : M \times M \to \mathbb{R}$ such that for $x, y, z \in M$,*

(i.) *d is postive definite; $d(x, y) \geq 0$ and $d(x, x) = 0$ iff $x = 0$.*

(ii.) *d is symmetric; $d(x, y) = d(y, x)$.*

(iii.) *d satisfies triangle inequality; $d(x, y) + d(y, z) \leq d(x, z)$.*

A space M together with a distance function is called a **metric space**

You can verify that $\mathbb{R}$ has the distance function $d(a, b) = |b - a|$. This means that $\mathbb{R}$ is a metric space. Every metric space can be given the structure of a topological space via the *metric topology*. You will learn about that in the real analysis course here at LU. The standard topology on $\mathbb{R}$ is the metric topology which is generated from $d(a, b) = |b - a|$.

Metric spaces are quite special. Many sets do not have a natural idea of distance. However, we can still give them a topological structure.

Example 3.3.13. *Let X be a nonempty set. Define $\mathcal{T} = \{X, \emptyset\}$. This provides a topology on X called the* **indiscrete topology**. *Axiom i. is satisfied. Then note*

$$X \cup \emptyset = X \in \mathcal{T}$$

$$X \cap \emptyset = \emptyset \in \mathcal{T}$$

Thus axioms ii. and iii. are satisfied. The set X could be most anything. For example, $X = \mathbb{R}$. With respect to the indiscrete topology, the set $(0, 1)$ is not open since $(0, 1) \notin \mathcal{T}$. There are many topologies available for a given space and they are not always compatible. For example, we can also form the **discrete topology** *on X where we simply use $\mathcal{P}(X)$ for the topolgy. In the discrete topology every possible subset of X is open.*

The power of topology is that it allows concrete definitions of very intuitive geometric terms such as *compact, disconnected* and *simply connected*. The topological definition of a continuous function states that a function is continuous if the inverse image of open sets is open for the function. We will work with that definition a little later when we discuss functions. If you'd like to learn more about topology or metric spaces then ask me sometime, I can recommend a few books.

3.4 cartesian products

Rene Descartes was a French natural philospher who lived from 1596 to 1650 AD. He is responsible for introducing the use of symbols like x, y and z for variables and a, b and c for constants. In addition, he introduced the use of exponential notation for the square function like x^2. Before this it was usually the practice of mathematicians to express equations in prose. Instead of x^2 you might write[2] something like "the quantity which is multiplied by itself". We are blessed to live in the time with the notation we currently enjoy. Another huge idea which we take for granted is the association of points in the plane with pairs of numbers. The idea that (x, y) corresponds to a point in a geometric plane, and that algebraic equations can be used to characterize curves in the plane is often attributed to Descartes. This is why we talk about *Cartesian coordinates.* I doubt Descartes gave the following definition. It is far more likely his definition was simply that a pair (a, b) is an ordered list where $(a, b) = (c, d)$ if and only if $a = c$ and $b = d$. That *formal definition* begs the question, "but what is (a, b) ? " and "how do you construct an object (a, b) which satisfies the criteria of this formal definition? ". One answer to these questions is given by the set-theoretic construction below:

Definition 3.4.1. *An ordered pair is a set of two elements with an ordering. We denoted an ordered pair of a and b by (a, b). The technical definition is:*

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

I sometimes give homework which asks you to show that $(a, b) = (x, y)$ if and only if $a = x$ and $b = y$. Notice the idea of the definition is that the element which is listed alone is the first element. That fixes an order for the pair. This means that $(1, 2)$ is distinguished from $(2, 1)$

Remark 3.4.2. *Beware that as an ordered pair $(1, 2) \neq \{x \mid 1 < x < 2\}$. There is a notational degeneracy that is unavoidable here. In practice the context of the sentence will inform you as to whether (a, b) is an open interval or an ordered pair. These are very different objects. An ordered pair is a set with two objects. An open interval of real numbers is a set with infinitely many elements. The French school of mathematics sometimes writes open intervals in the notation $)1, 2(= \{x \mid 1 < x < 2\}$, but we will not do this for we are not French.*

Generally, we can take a finite number of elements and form an ordered set that is called a tuple.

Definition 3.4.3. *If we have $n \in \mathbb{N}$ then $(x_1, x_2, \dots, x_n)$ is an n-tuple. Two tuples can only be equal if they have the same length. We say that $\vec{x} = (x_1, x_2, \dots, x_n)$ has j-th component x_j . Moreover, if $\vec{y} = (y_1, y_2, \dots, y_n)$ then we say $\vec{x} = \vec{y}$ if and only if $x_j = y_j$ for each $j = 1, 2, \dots n$.*

Notice I have not clarified where the components of the n-tuples above are taken from. They could all be taken from the same set, or we could even allow different sorts of variables in different components. Equality of two n-tuples is only possible if they share the same sort of variables in each matching component. I will not explain how to construct n-tuples from set theory here, but you can imagine how something like Definition 3.4.1 would allow for the construction of these objects.

Definition 3.4.4. *Let A and B be sets. The set of all ordered pairs with first component in A and second component in B is denoted $A \times B$. We say that $A \times B$ is the Cartesian product of A and B. To be precise,*

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

[2] But, it would probably have been in Latin since that was the scholarly langauge of antiquity.

Likewise, the defninition for the nth Cartesian product is

$$\prod_{i=1}^{n} A_i = A_1 \times \cdots \times A_n = \{(a_1, a_2, \dots a_n) \mid a_j \in A_j \ \forall j = 1, 2, \dots n\}.$$

When we take products of a set A with itself we can write $\prod_{i=1}^{n} A = A^n$.

Example 3.4.5. *(Cartesian Products are Non-Associative). Let A, B, C be sets. Let $a \in A, b \in B$ and $c \in C$. Observe:*

$$(a, b) \in A \times B$$

$$(b, c) \in B \times C$$

$$(a, b, c) \in A \times B \times C$$

$$(a, (b, c)) \in A \times (B \times C)$$

$$((a, b), c) \in (A \times B) \times C$$

$$(a, a, a, a) \in A \times A \times A \times A$$

$$((a, a), (a, a)) \in (A \times A) \times (A \times A)$$

There are of course obvious correspondences between things like $A \times (B \times C)$ and $(A \times B) \times C$. However, it is nice to be able to distinguish these objects if need be.

The xy-plane is the set of all points (x, y) such that $(x, y) \in \mathbb{R}$. The xy-plane can be identified with the Cartesian product of $\mathbb{R}$ with $\mathbb{R}$, it is customary to denote $\mathbb{R} \times \mathbb{R} = \mathbb{R}^2$. In calculus III we deal with three dimensional space which is conviently described by $\mathbb{R} \times \mathbb{R} \times \mathbb{R} = \mathbb{R}^3$.

Remark 3.4.6. *The concept of a Cartesian product is used throughout calculus and much of higher math as well. If we are given a space S then $S \times [0, 1]$ we can think of as a cylinder where each cross-section is like S. Or, we can think of $S \times [0, 1]$ as the space formed by gluing a copy of S at each point along the unit-interval. Let S^1 be the unit-circle in $\mathbb{R}^2$ then $S^1 \times S^1$ is the 2-torus embedded in $\mathbb{R}^4$. Cartesian products are essential for example-building in higher math.*

It turns out much of physics can be expressed in terms of sections of fiber bundles. A fiber bundle is an abstract space which locally corresponds to the cartesian product of its base space and its typical fiber. The physics of gauge theory is the mathematics of principle fiber bundles. It turns out the interplay between math and physics has given topologists exciting new problems in the past half century or so. A century ago, progress on the study of calculus of curved spaces was used by Einstein to formula General Relativity. Two centuries ago, multivariate calculus was used to formulate electromagnetism. Three or four centuries ago, classical mechanics promted the invention of calculus. This back and forth between mathematical discovery and invention and physical exploration is as old as we are I suspect. [3]

[3] Did there exist prediluvian physics and technologies and mathematics which were lost in the great flood ? Yeah, probably. I am very open to the idea that the technologies known to humans and the fallen angels they likely interbred with allowed for things which we currently think of as magic. The Biblical account indicates many things people currently scoff at were known realities of ancient times. I doubt this helps us much with Math 200, but hey, this is my footnote, I'm allowed to chase this rabbit wherever it goes.

Example 3.4.7. *Let A, B be sets. Prove $A \times B = \emptyset$ iff $A = \emptyset$ or $B = \emptyset$.*

Proof: *Let A, B be sets.*
($\Rightarrow$) Suppose $A \times B = \emptyset$. Towards a contradiction, suppose both A and B are nonempty. Then there exists $a \in A$ and $b \in B$ and hence $(a, b) \in A \times B$ thus $A \times B \neq \emptyset \rightarrow\leftarrow$. Consequently we find $A = \emptyset$ or $B = \emptyset$.

($\Leftarrow$) Suppose $A = \emptyset$ or $B = \emptyset$. Without loss of generality suppose $A = \emptyset$. Suppose, towards a contradiction, that $(a, b) \in A \times B$. Then $a \in A$ and $b \in B$ by definition of $A \times B$. But $a \in A$ contradicts $A = \emptyset$ hence we find there does not exist $(a, b) \in A \times B$. That is, $A \times B = \emptyset$. Therefore, $A \times B = \emptyset$ iff $A = \emptyset$ or $B = \emptyset$. □

Example 3.4.8. *Let A, B, C be nonempty sets. Prove $A \times C \subseteq B \times C$ iff $A \subseteq B$.*

Proof: *Let A, B, C be nonempty sets.*
($\Rightarrow$) Assume $A \times C \subseteq B \times C$. Let $x \in A$ then since $C \neq \emptyset$ there exists $c \in C$. Thus $(x, c) \in A \times C$. But, notice $A \times C \subseteq B \times C$ thus $(x, c) \in B \times C$. Then, we find $x \in B$ and $c \in C$. Hence $x \in A$ implies $x \in B$ which shows $A \subseteq B$ as x was arbitrary.

($\Leftarrow$) Suppose $A \subseteq B$. Let $(a, c) \in A \times C$ then $a \in A$ and $c \in C$. But, as $A \subseteq B$ we find $a \in A$ implies $a \in B$ thus $(a, c) \in B \times C$. We have shown $(a, c) \in A \times C$ implies $(a, c) \in B \times C$ thus $A \times C \subseteq B \times C$ by definition of subset. Therefore, $A \times C \subseteq B \times C$ iff $A \subseteq B$. □

Theorem 3.4.9. *Let A, B, C, D be sets. Then,*

(a.) $A \times (B \cup C) = (A \cup B) \times (A \cup C)$.

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

(c.) $A \times \emptyset = \emptyset$.

(d.) $(A \times B) \cap (C \times D) = (A \cap C) \times (B \cap D)$

(e.) $(A \times B) \cup (C \times D) \subseteq (A \cup C) \times (B \cup D)$

(f.) $A \times (B - C) = (A \times B) - (A \times C)$

Proof: See the text and homework problems. We may prove one or two of these in lecture. □

Example 3.4.10. *Let $A = \{1, 2\}$ and $B = \{dog, cat, batman\}$ then*

$$A \times B = \{(1, dog), (2, dog), (1, cat), (2, cat), (1, batman), (2, batman)\}.$$

Notice $\#(A) = 2$ and $\#(B) = 3$ while $\#(A \times B) = (\#A)(\#B)$.

Theorem 3.4.11. *Let A be a sets with m-elements and let B be a set with n-elements then $A \times B$ has mn-elements. In other words, if we denote the number of elements in a finite set A by $\#(A)$ then $\#(A \times B) = (\#A)(\#B)$.*

Proof: since this is a claim which is made for arbitrary natural numbers m, n it is best to leave this for us to prove with the tool of proof by mathematical induction. Possibly homework. □

Chapter 4

Induction

This is a rather focused chapter. We study one problem:

- Prove a claim $P(n)$ is true for all $n \in \mathbb{N}$.

We will see there are basically four methods. The first method rarely gets mentioned, but sometimes there is no need for the other methods since it is manifestly clear the claim is true for all $n \in \mathbb{N}$. For instance, $n^2 \geq 0$ for all $n \in \mathbb{N}$ is obviously true since we know $x^2 \geq 0$ for all $x \in \mathbb{R}$ and $\mathbb{N} \subseteq \mathbb{R}$. Sometimes students surprise me with direct proof which circumvent the need for the other induction techniques. But, special cases aside, we usually need to use one of the following:

- PMI: or weak induction, or simply induction, here we check $P(1)$ is true and argue $P(n)$ implies $P(n+1)$ for arbitrary $n \in \mathbb{N}$.

- PCI: or strong induction, here we check $P(1)$ implies $P(2)$ then show $P(k)$ true for $1 \leq k \leq n$ implies $P(n+1)$ is true.

- WOP: or the well ordering principle, here we construct a subset of $\mathbb{Z}$ which is nonempty and bounded below and then the smallest element's existence (granted by the WOP) is used to affirm the claim in question.

In each case, the proof technique essentially rests on the very structure of $\mathbb{N}$. We will also see that recursive definitions fit well within the logic of this chapter. It is natural to give inductive definitions for constructions which dependent on n. Such constructions are found throughout mathematics.

You can also read Chapters 1 of *Mathematical Proofs: a Transition to Advanced Mathematics* by Chattrand, Polimeni and Zhang., 4th-edition. These chapters overlap with the subject matter of this chapter of my notes. As before, if time permits, I may use that text or Wolf for additional examples. There are many additional practice problems there if you need further practice.

4.1 weak induction (PMI)

If we wish to prove a statement based on $n \in \mathbb{N}$ holds for all $n \in \mathbb{N}$ then the Principle of Mathematical Induction (PMI) is a nice method of argument. Let's see how this is set-up.

Definition 4.1.1. *If S is a subset of $\mathbb{N}$ with the following two properties:*

(i.) $1 \in S$,

(ii.) *for all $n \in \mathbb{N}$, if $n \in S$ then $n+1 \in S$.*

then S is called an **inductive set**.

From the definition of $\mathbb{N}$ we have the following result:

Theorem 4.1.2. *If S is an inductive set then $S = \mathbb{N}$.*

We should study the truth set of a proposition which depends on $n \in \mathbb{N}$. If we can show the truth set is an inductive set then it means the truth of the proposition holds on all of $\mathbb{N}$.

Corollary 4.1.3. *Suppose $P(n)$ is a proposition which depends on $n \in \mathbb{N}$. Let $S = \{n \in \mathbb{N} \mid P(n) \text{ is true }\}$. If $1 \in S$ and $n \in S$ implies $n+1 \in S$ for all $n \in \mathbb{N}$ then $S = \mathbb{N}$. Thus $P(n)$ is true for all $n \in \mathbb{N}$.*

Proof: The proof of the corollary below is simply that the truth set of $P(n)$ is an inductive set and hence must be $\mathbb{N}$. But $S = \mathbb{N}$ means $P(n)$ is true for all $n \in \mathbb{N}$. $\square$

You might have the feeling I'm not saying much in the arguments above. You might be correct. Still, I think it is helpful for us to define a method of argumentation for our future reference:

Definition 4.1.4. *Suppose $P(n)$ is a proposition defined for $n \in \mathbb{N}$. Then* **proof by mathematical induction** *or* **PMI** *constitutes the following argument:*

(1.) *Show $P(1)$ is true.*

(2.) *For all $n \geq 1$, show $P(n) \Rightarrow P(n+1)$.*

(3.) *By PMI, $P(n)$ is true for all $n \in \mathbb{N}$.*

The explicit mention of the inductive set S is not necessary. In practice, I usually just refer to the proposition $P(n)$. However, it is crucial to alert your reader to where the induction hypothesis $P(n)$ is used in formulating the argument to support the implication $P(n) \Rightarrow P(n+1)$. A good instructor will deduct points if they notice this detail is missing. I try to be good.

Example 4.1.5 (child-Gauss' observation)**. Show that**

$$1 + 2 + \cdots + n = \frac{n(n+1)}{2}.$$

Proof: Define the proposition above to be $P(n)$, we seek to show it is true for all $n \in \mathbb{N}$ Proceed by PMI. Observe $P(1) = \frac{1(2)}{2} = 1$ thus the induction hypothesis is true for n=1. Assume $P(n)$ is true for an arbitrary $n > 1$,

$$1 + 2 + \cdots + n = \frac{n(n+1)}{2}.$$

Add $n+1$ to both sides of the above equation,

$$1+2+\cdots+n+(n+1) = \frac{n(n+1)}{2} + n + 1.$$

Now make a common denominator on the rhs,

$$1+2+\cdots+n+(n+1) = \frac{n^2+3n+2}{2} = \frac{(n+1)(n+1+1)}{2}.$$

The equation above shows $P(n+1)$ is true. Hence we have shown $P(n) \Rightarrow P(n+1)$ for any $n > 1$. Therefore, by PMI, $1+2+\cdots+n = \frac{n(n+1)}{2}$ for all $n \in \mathbb{N}$

Induction is also used to give *recursive* defintions. Notice, while we have formulated PMI with a starting value of $n = 1$, it is not difficult to see all the same arguments can be formulated for an inductive set which begins at a different integer. For the sake of specificity let me make a definition

Definition 4.1.6. *If S is a subset of $\mathbb{Z}$ with the following two properties:*

- **(i.)** *$n_0 \in S$,*
- **(ii.)** *for all $n \in \mathbb{Z}$ with $n \geq n_0$, if $n \in S$ then $n+1 \in S$.*

then S is called an **inductive set** *with* **base case** *n_0.*

So, our base case in the beginning of this section was simply $n_0 = 1$. It should be entirely unsurprising that we can use a slight modification of PMI for propositions whose truth sets are a subset of $\mathbb{Z}$.

Definition 4.1.7. *Suppose $P(n)$ is a proposition defined for $n \in \mathbb{Z}$ with $n \geq n_0$. Then* **based proof by mathematical induction** *or* **PMI(n_0)** *constitutes the following argument:*

- **(1.)** *Show $P(n_0)$ is true.*
- **(2.)** *For all $n \geq n_0$, show $P(n) \Rightarrow P(n+1)$.*
- **(3.)** *By PMI(n_0), $P(n)$ is true for all $n \in \mathbb{Z}$ with $n \geq n_0$.*

You should have a fair amount of experience with the factorial from your work in Calculus II.

Definition 4.1.8. *Let $n!$ be defined by $0! = 1$ and $n! = n(n-1)!$ for $n \in \mathbb{N}$.*

This is known as a **recursive definition** since it defines one value of the given function in terms of the values which came before. Notice,

$$1! = 1(1-1)! = 1(0!) = 1, \quad 2! = 2(1!) = 2, \quad 3! = 3(2!) = 3(2)$$

and so forth.

Example 4.1.9. *Consider the claim below for $n \in \mathbb{Z}_{\geq 0}$,*

$$n! = n(n-1)(n-2)\cdots 3\cdot 2\cdot 1.$$

Proof: *Let $P(n)$ be the equation above. Let us use PMI(0) to establish the formula. Notice $P(0)$ is true since $0! = 1$. Suppose $P(n)$ is true for some $n \in \mathbb{Z}_{\geq 0}$. Consider, by definition of the factorial,*

$$(n+1)! = (n+1)n!$$

then applying the induction hypothesis we find

$$(n+1)! = (n+1)n(n-1)(n-2)\cdots 3\cdot 2\cdot 1$$

Thus $P(n) \Rightarrow P(n+1)$ and we find $n! = n(n-1)(n-2)\cdots 3\cdot 2\cdot 1$ for all $n \in \mathbb{Z}_{\geq 0}$ by PMI(0). □

Its not hard to see that induction will also hold for sets which have an upper bound in $\mathbb{Z}$ and go to $-\infty$. Let me give yet another definition.

Definition 4.1.10. *If S is a subset of $\mathbb{Z}$ with the following two properties:*

- **(i.)** $n_0 \in S$,
- **(ii.)** *for all $n \in \mathbb{Z}$ with $n \leq n_0$, if $n \in S$ then $n-1 \in S$.*

then S is called an **downward inductive set** *with* **base case** n_0.

Suppose $P(n)$ is defined on a downward inductive set with base case n_0 then define $Q(k) = P(-k)$. Notice the truth set for $Q(k)$ is related to the truth set for $P(n)$ with $n = -k$. If $n \leq n_0$ then $-n \geq -n_0$ hence $k \geq -n_0$ defines the truth set for $Q(k)$. If we apply $-n_0 - PMI$ to prove the truth set of $Q(k)$ is $\{-n_0, -n_0+1, -n_0+2, \dots\}$ then we can rightly deduce the truth set for $P(n)$ is $\{\dots, n_0-2, n_0-1, n_0\}$. This motivates the following method of proof:

Definition 4.1.11. *Suppose $P(n)$ is a proposition defined for $n \in \mathbb{Z}$ with $n \leq n_0$. Then* **proof by upsidedown induction** *from n_0 or* **IWd**(n_0) *constitutes the following argument:*

- **(1.)** *Show $P(n_0)$ is true.*
- **(2.)** *For all $n \leq n_0$, show $P(n) \Rightarrow P(n-1)$.*
- **(3.)** *By IWd (n_0), $P(n)$ is true for all $n \in \mathbb{Z}$ with $n \leq n_0$.*

Let us introduce another recursive definition to the discussion. Note, $\mathbb{Z}_{>0} = \mathbb{N} = \{1, 2, \dots\}$ and we could also denote $\mathbb{Z}_{<0} = -\mathbb{N} = \{-1, -2, \dots\}$.

Definition 4.1.12. *Let $a > 0$ be a real number. We define $a^0 = 1$ and*

- **(1.)** $a^n = a(a^{n-1})$ *for* $n \in \mathbb{Z}_{>0}$
- **(2.)** $a^n = (1/a)^{-n}$ *for* $n \in \mathbb{Z}_{<0}$

where $1/a$ is the number for which $a(1/a) = 1$.

Example 4.1.13. *Suppose $a, b \in (0, \infty)$, then $a^n b^n = (ab)^n$ for all $n \in \mathbb{Z}$.*

Proof: *Notice $\mathbb{Z} = -\mathbb{N} \cup \{0\} \cup \mathbb{N}$ shows we can treat a claim about the integers as a problem involving three cases. Note as $a, b > 0$ we find $ab > 0$ thus we can calculate $(ab)^n$ following the definition given in these notes. We use this observation throughout what follows.*

($n = 0$) By definition $a^0 = 1$, $b^0 = 1$ and $(ab)^0 = 1$ and thus $a^0 b^0 = (ab)^0$. Hence $a^n b^n = (ab)^n$ when $n = 0$.

Next consider $n \in \mathbb{N}$. Notice $a^1 = a(a^0) = a$ by the definition of a^n. Likewise $b^1 = b$ and $(ab)^1 = ab$. Thus $(ab)^1 = ab = a^1 b^1$. Suppose inductively that $a^n b^n = (ab)^n$ for some $n \in \mathbb{N}$. Consider,

$$\begin{aligned}
(ab)^{n+1} &= ab(ab)^n && \textit{definition of } n\textit{-th power} \\
&= ab(a^n b^n) && \textit{induction hypothesis} \\
&= a(a^n)b(b^n) && \mathbb{R} \textit{ multiplication commutes} \\
&= a^{n+1} b^{n+1} && \textit{definition of } (n+1)\textit{-th power}
\end{aligned}$$

Therefore, $a^nb^n = (ab)^n$ implies $(ab)^{n+1} = a^{n+1}b^{n+1}$ thus $a^nb^n = (ab)^n$ for all $n \in \mathbb{N}$ by PMI. Label this $\star$.

Next consider $n \in -\mathbb{N}$. Consider $n = -1$. Notice $a^{-1} = (1/a)^{-(-1)} = (1/a)^1 = 1/a$ by the definition and our arguments in the $n = 1$ case. Of course, the multiplicative inverse of a real number is unique, so consider:

$$(ab)(1/a)(1/b) = a(1/a)b(1/b) = 1(1) = 1 \quad \Rightarrow \quad 1/(ab) = (1/a)(1/b) \quad \star\star$$

But this means $(ab)^{-1} = a^{-1}b^{-1}$ hence $n = -1$ is true for $a^nb^n = (ab)^n$. Suppose, towards an upsidedown induction that $a^nb^n = (ab)^n$ for some $n \in -\mathbb{N}$ (meaning $n \leq -1$). Consider, $n-1 \leq -2$ hence

$$\begin{aligned}
(ab)^{n-1} &= (1/(ab))^{-(n-1)} && \textit{definition of } (n-1)\textit{-th power} \\
&= ((1/a)(1/b))^{1-n} && \textit{algebra and } \star\star \\
&= (1/a)^{1-n}(1/b)^{1-n} && 1-n \geq 2 \textit{ hence } \star \textit{ applies} \\
&= (1/a)^{-(n-1)}(1/b)^{-(n-1)} && \textit{algebra on exponents} \\
&= a^{n-1}b^{n-1} && \textit{definition of } (n-1)\textit{-th power}
\end{aligned}$$

Therefore, $a^nb^n = (ab)^n$ implies $(ab)^{n-1} = a^{n-1}b^{n-1}$ for any $n \leq -1$ hence $a^nb^n = (ab)^n$ for all $n \in -\mathbb{N}$ by IИd (-1). Finally, we conclude $a^nb^n = (ab)^n$ for all $n \in \mathbb{Z}$. □

Remark 4.1.14. *Notice the proof requires $ab = ba$. When $ab \neq ba$ then the law of exponents is not true. For example, matrices or function composition.*

Let us return to plain old induction for the next example.

Example 4.1.15. *If $n \in \mathbb{N}$ and $\#(X) = n$ then $\#\mathcal{P}(X) = 2^n$.*

Proof: *let the claim above constitute the statment $Q(n)$. If $X = \{x\}$ then $\mathcal{P}(X) = \{\emptyset, X\}$ hence $\#\mathcal{P}(X) = 2 = 2^1$ hence $Q(1)$ is true. Inductively suppose $Q(n)$ is true for some $n \in \mathbb{N}$. We assume any set of n-elements has a power set with 2^n elements.*

Consider X with $n+1$ elements and let $x_o \in X$. If $U \in \mathcal{P}(X-\{x_o\})$ then $x_o \notin U$ since $U \subseteq X-\{x_o\}$. Thus $U \cup \{x_o\}$ is a subset of X which is not a subset of $X - \{x_o\}$. Therefore, for each set in $U \in \mathcal{P}(X - \{x_o\})$ we find a corresponding set $U \cup \{x_o\} \in \mathcal{P}(X)$. If $U_1, U_2 \in \mathcal{P}(X - \{x_o\})$ and $U_1 \neq U_2$ then we may show $U_1 \cup \{x_o\} \neq U_2 \cup \{x_o\}$ thus each subset not containing x_o corresponds to a single subset of X which does contain x_o.

Consider that every subset of X either contains x_o or does not contain x_o so we have accounted for all subsets of X if we count subsets including or excluding x_o. We find the total number of subsets containing x_o and those excluding x_o are the same since these are in direct correspondence. Apply the induction hypothesis applied to $X - \{x_o\}$ to obtain $\#\mathcal{P}(X - \{x_o\}) = 2^n$ hence $\#\mathcal{P}(X) = 2^n + 2^n = 2^{n+1}$. Hence $Q(n)$ implies $Q(n+1)$ and we conclude $\#(X) = n$ implies $\#\mathcal{P}(X) = 2^n$ for all $n \in \mathbb{N}$ by PMI. □

Remark 4.1.16. *In the proof above I used a principle of counting which is perhaps intuitively clear. If a finite set can be divided into two disjoint buckets then the number of things in bucket* *one plus the number of things in bucket two gives the total number of things. I hope the proof above is reasonably clear, but I should mention this proof gets a bit easier to follow once we study bijections (also known as one-to-one correspondences). In short, if we have a bijection from one set to another then they have the same* number *of things.*

Example 4.1.17. *Let $P(n)$ be the proposition $\frac{n^3}{3}+\frac{n^5}{5}+\frac{7n}{15}$ is an integer. Prove $P(n)$ is true for all $n \in \mathbb{N}$. (solved on page 25 of this solution(link here)).*

Example 4.1.18. *Prove $4^n - 1$ is divisible by 3 for all $n \in \mathbb{N}$. (see solution(link here)).*

4.1.1 finite sums

In this section we introduce a nice notation for finite sums[1] of arbitrary size. Most of these statements are "for all $n \in \mathbb{N}$" thus proof by mathematical induction is the appropriate proof tool. I offer a few sample arguments and leave the rest to the reader. Let's begin by giving a precise definition for the finite sum $A_1 + A_2 + \cdots + A_n$:

Definition 4.1.19. *Let $A_i \in \mathbb{R}$ for $i = 1, 2, \dots n$. We recursively define:*

$$\sum_{i=1}^{n+1} A_i = A_{n+1} + \sum_{i=1}^{n} A_i$$

for each $n \geq 1$ and $\sum_{i=1}^{1} A_i = A_1$.

The "summation notation" or "sigma" notation allows us to write sums precisely. In $\sum_{i=1}^{n} A_i$ the index i is called the **dummy index of summation**. One dummy is just a good as the next, it follows that $\sum_{i=1}^{n} A_i = \sum_{j=1}^{n} A_j$. This relabeling is sometimes called *switching dummy variables*, or *switching the index of summation from i to j*. The terms which are summed in the sum are called **summands**.

Proposition 4.1.20. *Let $A_i, B_i \in \mathbb{R}$ for each $i \in \mathbb{N}$ and suppose $c \in \mathbb{R}$ then for each $n \in \mathbb{N}$,*

$$(1.)\ \sum_{i=1}^{n}(A_i + B_i) = \sum_{i=1}^{n} A_i + \sum_{i=1}^{n} B_i$$

$$(2.)\ \sum_{i=1}^{n} cA_i = c\sum_{i=1}^{n} A_i.$$

Proof: Let's begin with (1.). Notice the claim is trivially true for $n = 1$. Inductively assume that (1.) is true for $n \in \mathbb{N}$. Consider, the following calculations are justified either from the recursive

[1] the results of this section apply to objects which allow addition and multiplication by numbers, it is quite general, I simply chose sums of real numbers for the sake of specificity.

definition of the finite sum or the induction hypothesis:

$$\begin{aligned}
\sum_{i=1}^{n+1}(A_i+B_i) &= \sum_{i=1}^{n}(A_i+B_i)+A_{n+1}+B_{n+1} && \text{by definition of sum}\\
&= \left(\sum_{i=1}^{n}A_i+\sum_{i=1}^{n}B_i\right)+A_{n+1}+B_{n+1} && \text{induction hypothesis}\\
&= \left(\sum_{i=1}^{n}A_i\right)+A_{n+1}+\left(\sum_{i=1}^{n}B_i\right)+B_{n+1} && \text{addition commutes in } \mathbb{R}\\
&= \sum_{i=1}^{n+1}A_i+\sum_{i=1}^{n+1}B_i. && \text{by definition of sum}
\end{aligned}$$

Thus (1.) is true for $n+1$ and hence by proof by mathematical induction (PMI) we find (1.) is true for all $n \in \mathbb{N}$. The proof of (2.) is similar. □

Proposition 4.1.21. *Let $A_i, B_{ij} \in \mathbb{R}$ for $i, j \in \mathbb{N}$ and suppose $c \in \mathbb{R}$ then for each $m, n \in \mathbb{N}$,*

$$(1.)\ \sum_{i=1}^{n}\left(\sum_{j=1}^{m}B_{ij}\right)=\sum_{j=1}^{m}\left(\sum_{i=1}^{n}B_{ij}\right),$$

$$(2.)\ \sum_{i=1}^{n}\sum_{j=1}^{m}A_iB_{ij}=\sum_{i=1}^{n}A_i\sum_{j=1}^{m}B_{ij}.$$

Proof: Let $m \in \mathbb{N}$ be fixed. Consider, by definition of sum,

$$\sum_{i=1}^{1}\left(\sum_{j=1}^{m}B_{ij}\right)=\sum_{j=1}^{m}B_{1j}=\sum_{j=1}^{m}\sum_{i=1}^{1}B_{ij}$$

where we once more used the definition of sum in the last step. Hence (1.) holds true for $m \in \mathbb{N}$ and $n = 1$.

Assume inductively that (1.) is true for some $n > 1$. Consider,

$$\begin{aligned}
\sum_{i=1}^{n+1}\sum_{j=1}^{m}B_{ij} &= \sum_{j=1}^{m}B_{n+1,j}+\sum_{i=1}^{n}\sum_{j=1}^{m}B_{ij} && \text{by definition of sum}\\
&= \sum_{j=1}^{m}B_{n+1,j}+\sum_{j=1}^{m}\sum_{i=1}^{n}B_{ij} && \text{by induction hypothesis}\\
&= \sum_{j=1}^{m}\left(B_{n+1,j}+\sum_{i=1}^{n}B_{ij}\right) && \text{by (1.) of Proposition 4.1.20}\\
&= \sum_{j=1}^{m}\sum_{i=1}^{n+1}B_{ij} && \text{by definition of sum.}
\end{aligned}$$

Thus n implies $n+1$ for (1.) with arbitrary m therefore by proof by mathematical induction we find (1.) is true for all $n \in \mathbb{N}$ for arbitrary m. I leave (2.) as a possible homework problem. □

Example 4.1.22. *Claim:* $\sum_{i=1}^{n} 2^i = 2^{n+1} - 2$ *for all* $n \in \mathbb{N}$.

Proof: *observe* $\displaystyle\sum_{i=1}^{1} 2^i = 2^1 = 2 = 2^2 - 2$ *thus* $\displaystyle\sum_{i=1}^{n} 2^i = 2^{n+1} - 2$ *is true for* $n = 1$. *Suppose inductively that* $\displaystyle\sum_{i=1}^{n} 2^i = 2^{n+1} - 2$ *for some* $n \in \mathbb{N}$. *Consider,*

$$\begin{aligned} \sum_{i=1}^{n+1} 2^i &= 2^{n+1} + \sum_{i=1}^{n} 2^i && \textit{by definition of sum} \\ &= 2^{n+1} + 2^{n+1} - 2 && \textit{by induction hypothesis} \\ &= 2^{(n+1)+1} - 2 && \textit{algebra simplification} \end{aligned}$$

Therefore $\sum_{i=1}^{n} 2^i = 2^{n+1} - 2$ *for all* $n \in \mathbb{N}$ *by PMI.* □

Theorem 4.1.23 (binomial theorem)**.** *Let* $a, b \in \mathbb{C}$ *then*

$$(a+b)^n = a^n + na^{n-1}b + \cdots + \binom{n}{k} a^{n-k}b^k + \cdots + nab^{n-1} + b^n$$

In summation notation,

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k}b^k$$

Where

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}$$

Proof: Let $P(n)$ be the binomial theorem. We use induction starting at $n = 0$. Observe that,

$$(a+b)^0 = 1$$

Also,

$$\binom{0}{0} = \frac{0!}{0!(0-0)!} = \frac{1}{1} = 1.$$

Thus $P(0)$ is true. Assume $P(n)$ is true. For a particular $n \in \mathbb{N}$, assume that

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k}b^k. \tag{4.1}$$

We wish to show,

$$(a+b)^{n+1} = \sum_{k=0}^{n+1} \binom{n+1}{k} a^{n+1-k}b^k$$

A short calculation reveals that for $k = 1, 2, \ldots, n$

$$\binom{n+1}{k} = \binom{n}{k-1} + \binom{n}{k}$$

Whereas for, $k = 0$,

$$\binom{n+1}{0} = \frac{(n+1)!}{0!(n+1)!} = 1$$

Or for $k = n+1$,

$$\binom{n+1}{n+1} = \frac{(n+1)!}{(n+1)!(n+1-(n+1))!} = 1$$

Thus we need to show,

$$\begin{aligned} (a+b)^{n+1} &= a^{n+1} \ + \ \sum_{k=1}^{n}\left[\binom{n}{k-1} + \binom{n}{k}\right]a^{n+1-k}b^k \ + \ b^{n+1} \\ &= a^{n+1} + \sum_{k=1}^{n}\binom{n}{k-1}a^{n+1-k}b^k + \sum_{k=1}^{n}\binom{n}{k}a^{n+1-k}b^k + b^{n+1} \qquad (4.2) \end{aligned}$$

Multiply the induction hypothesis 4.1 by $(a+b)$,

$$\begin{aligned} (a+b)^{n+1} &= \sum_{k=0}^{n}\binom{n}{k}a^{n-k}b^k(a+b) \\ &= \sum_{k=0}^{n}\binom{n}{k}a^{n-k+1}b^k + \sum_{k=0}^{n}\binom{n}{k}a^{n-k}b^{k+1} \\ &= a^{n+1} + \sum_{k=1}^{n}\binom{n}{k}a^{n-k+1}b^k + \sum_{k=1}^{n-1}\binom{n}{k}a^{n-k}b^{k+1} + b^{n+1} \\ &= a^{n+1} + \sum_{k=1}^{n}\binom{n}{k}a^{n-k+1}b^k + \sum_{p=0}^{n}\binom{n}{p-1}a^{n-(p-1)}b^{p-1+1} + b^{n+1} \\ &= a^{n+1} + \sum_{k=1}^{n}\binom{n}{k}a^{n-k+1}b^k + \sum_{k=0}^{n}\binom{n}{k-1}a^{n+1-k}b^k + b^{n+1} \qquad (4.3) \end{aligned}$$

Comparing Equations 4.2 and 4.3 we see that the induction hypothesis for n yields the induction hypothesis for $n+1$. Thus, by PMI, the binomial theorem holds for all $n \in \mathbb{N} \cup \{0\}$. □

The exceptional cases of $k = 0$ and $k = n$ correspond to the edges of Pascal's triangle. Also the main calculational observation is nothing more than the formula which makes Pascal's triangle work.

4.2 strong induction (PCI)

Strong or complete induction is another equivalent form of induction. Let me state the Principle of Complete Induction(PCI):

Definition 4.2.1. *Suppose $P(n)$ is a proposition defined for $n \in \mathbb{N}$. Then* **proof by complete induction** *or* **PCI** *constitutes the following argument:*

(1.) *Show $P(1)$ implies $P(2)$,*

(2.) *Show $P(k)$ true for $1 \leq k \leq n$ implies $P(n+1)$,*

(3.) *Conclude $P(n)$ is true for all $n \in \mathbb{N}$ by PCI.*

The difference between PCI and PMI is that for PCI we get to assume that the induction hypothesis is true for all natural numbers leading up to n. In contrast, PMI says we assume $P(n)$ is true for just n then we had to show $P(n+1)$ was true. PMI also required us to show $P(1)$ was true, in contrast PCI instead requires that we show $P(1)$ implies $P(2)$. Although, PCI sometimes requires different arguments for different ranges of n (this is also true for PMI but most examples don't exhibit this subtlety). Both PCI and PMI require the implication to be shown for arbitrary n, so if the first few values are special they have to be treated separately. Finally, it should be understood that PCI can also be applied to inductive sets that start at some integer other than one and we could also write an upside down version if we had need. Again the key is that all integers to the right of the starting point for the inductive set.

Example 4.2.2. *Claim: If $n \geq 2$ then n has a prime factor.*

Proof: *To begin recall that $p \in \mathbb{N}$ is a prime iff its only factors are 1 and p. Let S be the set of $n \in \mathbb{N}$ such that n has a prime factor and $n > 1$. Clearly $2 \in S$ since 2 is prime and is obviously a factor of 2. Likewise, $3 \in S$ since 3 is a prime factor of 3. Suppose that $\{2, 3, \dots, n\} \subset S$. Then $2, 3, \dots n$ all are assumed to have a prime factor. Consider $n+1$. If $n+1$ is prime then we are done since $n+1$ would be a prime factor of $n+1$. Otherwise, by definition of prime, there must exist positive integers r, s such that $n+1 = rs$ with $r, s > 1$ but $r, s < n+1$. Therefore, $r, s \in \{2, 3, \dots, n\}$ which implies r, s have prime factors. Consequently, $n+1$ has a prime factor thus $n+1 \in S$ and we conclude every positive integer two or larger has a prime factor by PCI.* □

The Fundamental Theorem of Arithmetic states that every positive integer can be factored into a unique (upto ordering) product of primes. The example we just completed goes a long way towards the Theorem. Take a positive integer n, then $\exists p_1 \in \mathbb{N}$ prime, such that $n = n_1 p_1$ and $n_1 < n$. If n_1 is prime then we are done. Otherwise, apply our example to n_1, we can produce another prime $p_2 \in \mathbb{N}$ such that $n = n_2 p_2 p_1$. If n_2 is prime we are done. Otherwise, we can apply our example to $n_2 \in \mathbb{N}$ and so forth. In each case we will have $n_{k+1} < n_k$ as to say otherwise would violate $n_k = n_{k+1} p_{k+1}$. Observe that, $n > n_1 > n_2 > \cdots > n_k$. I argue that this list has length at most $n-1$. Each n_k is at least one smaller than n_{k-1}. If the list had n factors then n_n would be at most zero, but that is a contradiction since $n_n \in \mathbb{N}$. Hence the list has length less than $n-1$.

This almost proves the Fundamental Theorem of Arithmetic. Time permitting, we may go over a few examples from the homework solution on PCI.

Example 4.2.3. *Prove that every $n \in \mathbb{N}$ with $n > 3$ may be written as an integer-linear combination of 2 and 5, that is $\exists x, y \in \mathbb{Z}$ such that $n = 2x + 5y$. (solved on page 27 of this solution(link here)).*

4.3 well ordering principle (WOP)

The Well Ordering Principle (WOP) states:

Every nonempty subset of $\mathbb{N}$ has a smallest element.

This is equivalent to PMI and PCI, I will forego the proof in the notes for now. The next example revisits Example 4.2.2. Lets see how WOP makes it easier.

Example 4.3.1. *(Every natural number $n > 1$ has a prime factor) Let $n > 1$ and suppose n is prime, then n has a prime factor of n. Otherwise suppose n is not prime, thus n is composite. If*

S is the set of all factors of n not equal to one, then it is nonempty since n is composite. We use the WOP to select p, the smallest factor of n.

We seek to show p is prime. Suppose p is composite, then there exists r, s such that $p = rs$ such that $r, s > 1$ and $r, s < p$. Observe that $r \mid p$ and $p \mid n$ implies that $r \mid n$ thus r is a factor of n smaller than p. But this is a contradiction since the WOP allowed us to select p that was the smallest factor (not equal to one). Hence, p is prime and n has a prime factor. $\square$

The example above is typical of a WOP proof. Often the WOP is applied then contradiction is used to show the smallest element possesses some particular property. Here we saw it was prime. Proofs that use the Well Ordering Principle can require a certain amount of artistry, I am most interested in you gaining a throurough understanding of PMI. It is important to know PCI and WOP can help you when PMI fails to be obvious.

Chapter 5

Relations

The concept of a relation is quite general. Many of the constructions we have experience with for functions will also make sense for relations. For example, we can think about the graph of a relation, the composite of two relations and the inverse of a relation. We will see (in a future chapter) that functions are a special type of relation. Finally, equivalence relations generalize the idea of equality. We will see how an equivalence relation gives rise to equivalence classes. Equivalence classes partition the set. In my experience, the concept of an equivalence relation was the most important thing I learned in this course as an undergraduate. Order relations are also studied briefly including the concepts of partial ordering, total ordering, irreflexive partial orderings and total irreflexive orderings. In other words, we also examine relations which abstract the concepts of $\leq$ and $<$.

5.1 relations

A relation is simply some subset of a Cartesian product

Definition 5.1.1. *Let A, B be sets. We say that R is a relation from A to B if $R \subseteq A \times B$. Moreover, we say that xRy if $(x, y) \in R$. If xRy then we say that x is related to y. On the other hand if $(x, y) \notin R$ then we say that x is not related to y. When we say xRy, we say x is the* **input** *of the relation and y is the* **output** *of R*[1]*.*

$$Domain(R) = \{x \in A \mid \exists (y \in B)(xRy)\}$$

$$Range(R) = \{y \in B \mid \exists (x \in A)(xRy)\}$$

Finally, if $R \subseteq A \times A$ and $dom(R) = A$ then we say R is a relation on A.

If you wish, it is also common to use notation $Dom(R)$ for $Domain(R)$ and $Rng(R)$ for $Range(R)$.

Remark 5.1.2. *Notice that if R is a relation* **from** *A to B we do not require $Dom(R) = A$. On the other hand, a relation* **on** *A does require $Dom(R) = A$.*

Let me begin with a silly example,

[1] We could also use notation $R : A \to B$ if we wished to communicate the input/output working of R. However, I do at times reserve this notation for functions. We discuss functions in the next chapter.

Example 5.1.3. *(people) Let S be the set of all living creatures on earth. We can say that x is R-related to y if both x and y are people. In this sense I am R-related to Trump*[2]*. In contrast, I am not R-related to Napolean because he's dead. I am also not R-related to my mom's dogs*[3]*. They may be treated like humans but the fact remains they have tails and other dog parts that necessarily disqualify them from the category of people.*

Whenever we have a relation from $\mathbb{R}$ to $\mathbb{R}$ we can picture the relation in the Cartesian plane. (We can also do the same for relations from $\mathbb{N}$ to $\mathbb{N}$ and other subsets of the real numbers)

Example 5.1.4. *(circle) Define $R = \{(x,y) \in \mathbb{R}^2 \mid x^2+y^2=1\}$. This is a relation from $\mathbb{R}$ to $\mathbb{R}$. The points in R form a circle.*

Example 5.1.5. *(circle) Define $R = \{(x,y) \in \mathbb{R}^2 \mid x^2+y^2=R^2 \text{ for some } R>0\}$. This is a relation from $\mathbb{R}$ to $\mathbb{R}$. In this case $R = \mathbb{R}^2 - \{(0,0)\}$.*

Example 5.1.6. *(disk) Define $R = \{(x,y) \in \mathbb{R}^2 \mid x^2+y^2 \leq 1\}$. This is a relation from $\mathbb{R}$ to $\mathbb{R}$. The points in R form a circle shaded in; that is a disk.*

Example 5.1.7. *(plane with a hole) Define $R = \{(x,y) \in \mathbb{R}^2 \mid x^2+y^2 > 1\}$. This is a relation from $\mathbb{R}$ to $\mathbb{R}$. The R is the plane with the disk deleted. In other words, it is the set of all points outside the unit-circle.*

Example 5.1.8. *(positive lattice) Define $R = \{(x,y) \in \mathbb{R}^2 \mid x,y \in \mathbb{N}\}$. This is a relation from $\mathbb{R}$ to $\mathbb{R}$. Note R is a grid of points. This is not a relation on $\mathbb{R}$ since $dom(R) = \mathbb{N} \neq \mathbb{R}$.*

Example 5.1.9. *(coordinate grid) Define $R = \{(x,y) \in \mathbb{R}^2 \mid x \in \mathbb{Z}, y \in \mathbb{R}\} \cup \{(x,y) \mid x \in \mathbb{R}, y \in \mathbb{Z}\}$. This is a relation from $\mathbb{R}$ to $\mathbb{R}$. You can visualize R as a grid of horizontal and vertical lines.*

There is no end to these geometric examples. Let me give a weirder example:

Example 5.1.10. *Define $R = \{(x,y) \in \mathbb{R}^2 \mid x,y \in \mathbb{Q}\} = \mathbb{Q} \times \mathbb{Q}$. This is a relation from $\mathbb{R}$ to $\mathbb{R}$. For example, $(3/4)R(134/279)$. However, π is not related to anything. This means that points in the xy-plane with x-coordinate π will not be included in R. However, points with $x = 3.1415 = 31415/10000$ will be included so it is hard to see the holes along $x = \pi$. In fact, the R looks like the whole plane. However, it has holes infinitely close to any point you pick. This is a consequence of the fact that there are infinitely many irrational numbers between any two distinct rational numbers.*

5.1.1 composite relations

Definition 5.1.11. *(composite relation) Let R be a relation from A to B and let S be a relation from B to C. The composite of R and S is*

$$S \circ R = \{(a,c) \mid b \in B \text{ such that } (a,b) \in R \text{ and } (b,c) \in S\}$$

Example 5.1.12. *Let $R = \{(1,2),(3,4),(5,6),(7,8)\}$ this is a relation from $A = \{1,3,5,7\}$ to $B = \{2,4,6,8\}$. Define $S = \{(2,1),(4,3),(6,5),(8,7)\}$. We see that S is a relation from B to A. Notice that $S \circ R$ is a relation from A to A; $S \circ R : A \to B \to A$:*

$$S \circ R = \{(1,1),(3,3),(5,5),(7,7)\}$$

[2] written on January 2, 2025 for context

[3] sadly, also dead

Since $1R2$ and $2S1$ we have $1S \circ R1$ and so forth... Likewise we can verify that $R \circ S$ is a relation from B to B; $R \circ S : B \to A \to B$:

$$R \circ S = \{(2,2),(4,4),(6,6),(8,8)\}$$

The relations we just exhibited are known as the **identity relations** *on A and B respective. We denote $I_A = S \circ R$ and $I_B = R \circ S$. The relations given in this example are inverses of each other.*

Definition 5.1.13. *Let A be a set then $Id_A = \{(x,x) \mid x \in A\}$ is the* **identity relation** *on A.*

The previous example illustrates a general construction.

Definition 5.1.14. *(inverse relation) Given a relation R from A to B we define the inverse relation R^{-1} to be the relation from B to A defined by $R^{-1} = \{(y,x) \mid (x,y) \in R\}$*

Proposition 5.1.15. *The inverse relation just defined is a relation with $Dom(R^{-1}) = Rng(R)$ and $Rng(R^{-1}) = Dom(R)$. In addition, $(R^{-1})^{-1} = R$.*

Proof: observe $(x,y) \in R$ iff $(y,x) \in R^{-1}$. Thus $x \in Dom(R)$ and $y \in Rng(R)$ iff $y \in Dom(R^{-1})$ and $x \in Rng(R)$. Thus $Dom(R) = Rng(R^{-1})$ and $Rng(R) = Dom(R^{-1})$. Let $(x,y) \in R$ then $(y,x) \in R^{-1}$ and applying the definition of inverse relation once more we find $(x,y) \in (R^{-1})^{-1}$. Thus $R \subseteq (R^{-1})^{-1}$. Conversely, if $(a,b) \in (R^{-1})^{-1}$ then there exists $(b,a) \in R^{-1}$ and so $(a,b) \in R$ by the definition of inverse relation. Thus $(R^{-1})^{-1} \subseteq R$. Therefore, $(R^{-1})^{-1} = R$ by double containment. □

Remark 5.1.16. *The concept of an inverse relation is nice in that it avoids some of the rather cumbersome restrictions that come with the idea of an inverse function. We'll get into those restrictions in a week or two, but you probably recall from precalculus courses that in order for the inverse function to exist we need the function's graph satisfy the horizontal line test. Inverse relations have no such restriction. Notice that we can form the inverse of a relation always, no horizontal line test can rain on our parade here. I should also mention, it is not generally true that $R \circ R^{-1} = Id_{Rng(R)}$ and $R^{-1} \circ R = Id_{Dom(R)}$ even if $Rng(R) = Dom(R)$. That fortunate occurence in Example 5.1.12 is not always true for relations.*

My apologies there are not pictures in these notes. I'm sure there are pictures in the textbook and I will draw some in class. Graphing a relation and its inverse is quite satisfying.

Example 5.1.17. *(inverse relation graph goes sideways) Let $S = \{(x, \sin(x)) \mid x \in \mathbb{R}\}$. This is a relation from $\mathbb{R}$ to $\mathbb{R}$. The S is the graph of the sine function in the xy-plane. The inverse of S is $S^{-1} = \{(sin(y), y) \mid y \in \mathbb{R}\}$. Consider that S^{-1} should be the same as the graph of the sine function except that $x = \sin(y)$ instead of $y = \sin(x)$. If you think about this for a moment or two you'll see that the graph of S^{-1} is the same as the graph of S just instead of running along the x-axis it runs up the y-axis.*

The fact that $graph(S^{-1})$ fails the vertical line test goes to show it is not a function. The graph of the inverse will not pass the vertical line test unless we restrict S to be smaller so it passes the horizontal line test. Customarily, the inverse sine function is just such an inverse. It is the inverse for the sine function restricted to the interval $[-\frac{\pi}{2}, \frac{\pi}{2}]$. To conclude, relations can be inverted without regard to their particular properties.

Theorem 5.1.18. *Let A, B, C, D be sets. Suppose R, S, T are relations with $R \subseteq A \times B, S \subseteq B \times C$ and $T \subseteq C \times D$ then*

(a.) $T \circ (S \circ R) = (T \circ S) \circ R$,

(b.) $I_B \circ R = R$ *and* $R \circ I_A = R$,

(c.) $(S \circ R)^{-1} = R^{-1} \circ S^{-1}$.

Proof: we may prove these in class or homework. They make nice problems. □

Item $(a.)$ says that we can write $T \circ S \circ R$ without ambiguity, composition of relations is associative. Item $(c.)$ is sometimes called the "*socks-shoes principle*". Think of it this way, if I put my socks on first and then second my shoes then when I take off my socks and shoes I have to take off my shoes first and then my socks.

5.2 equivalence relations and partitions

Given some set S we can consider various subsets of $S \times S$. Each such subset will form a relation from S to S. Of all those relations there is a particular type which has special structure which is similar to equality.

Definition 5.2.1. *Let A be a set and let R be a relation on A. We say that R is an* **equivalence relation** *if R is*

(i.) **reflexive***; for all $x \in A$, $x\ R\ x$.*

(ii.) **symmetric***; for all $x, y \in A$, if $x\ R\ y$ then $y\ R\ x$.*

(iii.) **transitive***; for all $x, y, z \in A$, if $x\ R\ y$ and $y\ R\ z$ then $x\ R\ z$.*

Remark 5.2.2. *The notation xRy for "x is related to y" is not used much outside the introductory discussion of relations. Usually, we refer to a relation by some other symbol such as $\sim$ or $\approx$ and write $x \sim y$ or $x \approx y$ in place of xRy.*

Example 5.2.3. *(equality) Suppose that S is any nonempty set. Let $x, y \in S$, define xRy iff $x = y$. Observe that*

$$x = x, \quad x = y \ \Rightarrow \ x = y, \quad x = y \text{ and } y = z \ \Rightarrow \ x = z$$

Therefore, R is reflexive, symmetric and transitive. Hence equality is an equivalence relation on S.

Example 5.2.4. *(rational numbers) Let us define an equivalence relation on $S \subseteq Z \times Z$ as follows: suppose $S = \{(a, b) \mid a, b \in \mathbb{Z} \text{ and } b \neq 0\}$, $(a, b), (c, d) \in S$ then $(a, b) \sim (c, d)$ iff $ad = bc$. I claim that $\sim$ is an equivalence relation on S. Let $(a, b), (c, d), (x, y) \in S$,*

$$ab = ba \ \Rightarrow \ (a, b) \sim (a, b)$$

$$(a, b) \sim (c, d) \ \Rightarrow \ ad = bc \ \Rightarrow \ cb = da \Rightarrow \ (c, d) \sim (a, b)$$

The proof that $\sim$ is transitive follows similarly. You should understand what this example is doing better if I use the notation $(a, b) = a/b$ which translates $(a, b) \sim (c, d)$ if $ad = bc$. If you think about it you'll realize you've been using equivalence relations your whole life. We were taught early on that $1/2$ and $2/4$ are the "same" thing. Are they? Yes, of course, but understand that the idea of "same" means that $\mathbb{Q}$ is technically made of equivalence classes. Two fractions are in the same class when they cross-multiply to yield an equality. Rather than write $\sim$ all the time we simply write " = ".

Remark 5.2.5. *I think we should say that $1/2$ and $5/10$ are the* **same** *fraction since we certainly all agree that $1/2 = 5/10$. If we wish to describe the difference between $1/2$ and $5/10$ then I propose we say $1/2$ and $5/10$ are different* **representatives** *of the fraction $1/2$.*

Definition 5.2.6. *Let S be a set with equivalence relation R. The* **equivalence class** *containing $x \in S$ is a set defined as follows:*

$$[x]_R = \{y \in S \mid xRy\}$$

The set of all equivalence classes of S with respect to the equivalence relation R is denoted

$$S/R = \{[x]_R \mid x \in S\}.$$

We often drop the R on $[x]_R$ and write $[x]$ if there is no danger of confusion.

Example 5.2.7. *Suppose that $S = \mathbb{Z}$. Suppose $x, y \in \mathbb{Z}$, define xRy iff $x - y$ is even. We can argue this is an equivalence relation.*

(1.) *Clearly R is reflexive since $x - x = 0$ which is even.*

(2.) *Let $x, y \in \mathbb{Z}$ and assume xRy thus $x - y = 2k$ for some $k \in \mathbb{Z}$. Observe $y - x = -2k = 2(-k)$ hence yRx which shows R is symmetric.*

(3.) *Suppose $x, y, z \in \mathbb{Z}$ such that xRy and yRz. This means there exist $m, k \in \mathbb{Z}$ such that $x - y = 2k$ and $y - z = 2m$. Consider,*

$$x - z = x - y + y - z = 2k + 2m = 2(k + m).$$

Hence $x - z$ is even and we have shown xRz so R is transitive.

We conclude R is an equivalence relation on $\mathbb{Z}$. It has two equivalence classes:

$$[0] = \mathcal{E} = 2\mathbb{Z} \qquad \& \qquad [1] = \mathcal{O} = 2\mathbb{Z} + 1$$

Let S, T be subsets of $\mathbb{Z}$ and define $S + T = \{s + t \mid s \in S, t \in T\}$ and $ST = \{st \mid s \in S, t \in T\}$. I invite the reader to check that:

$$[0] + [0] = [0], \quad [0] + [1] = [1] + [0] = [1], \quad [1] + [1] = [0], \quad [1][1] = 1, \quad [1][0] = [0][1] = [0].$$

Here $\mathbb{Z}/R = \{[0], [1]\}$ and you can see from the equations above this behaves as a set with two elements which has a somewhat novel arithmetic. The multiplicative identity $[1]$ has the curious property that $[1] + [1] = [0]$.

Remark 5.2.8. *(Big Idea of Equivalence Relations) There are two ways to think about S/R. First, we can think about elements of S/R as subsets of S. Second, we can think about elements of S/R as single elements formed by gluing equivalent points together. In essence, the idea of the equivalence relation is to re-define the idea of equality by lumping together similar things together. In other contexts S/R is called a quotient space and it is sometimes read "S modulo R.*

The pattern exhibited in the previous example is known as a *partition*.

Definition 5.2.9. *(Partition) Let S be a nonempty set. A family of subsets $\mathcal{A}$ is called a partition iff the following three conditions hold:*

(i.) *Each partition is nonempty; If $U \in \mathcal{A}$ then $U \neq \emptyset$,*

(ii.) *$\mathcal{A}$ is made of disjoint subsets; for all $U, V \in \mathcal{A}$, either $U = V$ or $U \cap V = \emptyset$.*

(iii.) *the union of all sets in the partition covers S;*

$$\bigcup_{U \in \mathcal{A}} U = S$$

Example 5.2.10. *Let $\mathcal{A} = \{(n, n+1] \mid n \in \mathbb{Z}\}$. This forms a partition of $\mathbb{R}$.*

Example 5.2.11. *Let $\mathcal{A} = \{[n, n+1] \mid n \in \mathbb{Z}\}$. Does not form a partition of $\mathbb{R}$ since the sets forming the family are not disjoint. Notice $[n, n+1] \cap [n+1, n+2] = \{n+1\}$ for each $n \in \mathbb{Z}$.*

Example 5.2.12. *Let $\mathcal{A} = \{3\mathbb{Z}, 3\mathbb{Z}+1, 3\mathbb{Z}+2\}$. This forms a partition of $\mathbb{Z}$ since any integer is either in $3\mathbb{Z}$, or $3\mathbb{Z}+1$, $3\mathbb{Z}+2$ and we can prove these are disjoint sets.*

There is a natural correspondence between equivalence relations and partitions. We should develop this formally. I'll begin with a lemma.

Lemma 5.2.13. *Let A be a set and suppose R is an equivalence relation on A. If $x, y \in A$ then*

(a.) *$x \in [x]$,*

(b.) *xRy iff $[x] = [y]$,*

(c.) *$\sim (xRy)$ iff $[x]$ and $[y]$ are disjoint.*

Proof: suppose A is a set containing x, y and R is an equivalence relation.

(a.) If $x \in A$ then xRx as R is reflexive. Therefore, $x \in [x]$.

(b.) ($\Rightarrow$) Suppose xRy then since R is an equivalence relation we have yRx. Notice xRy implies $y \in [x]$ by the definition of $[x]$. Likewise, $x \in [y]$. Suppose $z \in [x]$ then xRz thus zRx by symmetry. Observe, zRx and xRy hence zRy by transitivity of R. Thus yRz by symmetry and we find $z \in [y]$. Consequently, $[x] \subseteq [y]$. A similar argument shows $[y] \subseteq [x]$ hence $[x] = [y]$ by double containment.

($\Leftarrow$) Suppose $[x] = [y]$. By $(a.)$ we have $x \in [x]$ and $y \in [y]$ and as $[x] = [y]$ they have the same elements. Noteably $y \in [x]$ thus xRy by definition of $[x]$. Hence xRy iff $[x] = [y]$.

(c.) I leave for class or homework. □

Theorem 5.2.14. *Let S be a set and suppose R is an equivalence relation on S then S/R forms a partition of S. Moreover, if $\mathcal{A}$ is a partition of S then there exists an equivalence whose equivalence classes are the sets in $\mathcal{A}$.*

Proof: If S is a set and R is an equivalence relation then note $x \in [x]$ implies $[x] \neq \emptyset$ and $\cup_{x \in S}[x] = S$ thus the union of all equivalence classes covers S and each is nonempty. Furthermore, if $\sim (xRy)$ then $[x] \cap [y] = \emptyset$ so equivalence classes are disjoint. Hence S/R is a partition of S.

On the other hand, if we're given $\mathcal{A}$ is a partition of S then we define xRy iff there exists $U \in mathcalA$ for which $x, y \in A$. Notice xRx for each $x \in S$ since $x \in U$ for some $U \in \mathcal{A}$ by the definition of partition. Furthermore, if xRy then there exists $U \in mathcalA$ for which $x, y \in A$ hence $y, x \in A$ and so yRx. We have shown R is reflexive and symmetric, it remains to prove R is transitive. Suppose xRy and yRz then there exists $U, V \in \mathcal{A}$ for which $x, y \in U$ and $y, z \in V$. Thus $y \in U \cap V \neq \emptyset$ and by definition of partition we find $U = V$ which implies $x, y, z \in U$ and so xRz. Therefore, R is an equivalence relation on S. $\square$

Many of our previous examples were equivalence relations. It might be interesting to go back and determine what the equivalence classes were. In each case we'll see the equivalence classes partition the set. Sometimes the partition isn't particular interesting.

Example 5.2.15. *Let S be any nonempty set. As we discussed in Example 5.2.3 if define $x \sim y$ for $x, y \in S$ iff $x = y$ then this defines an equivalence relation. Observe $[x] = \{x\}$ for each $x \in S$.*

$$S/\sim \; = \; \{\{x\} \mid x \in S\}$$

Technically $S/\sim \; \neq S$, however, we realize this is a rather silly distinction.

Example 5.2.16. *Let S be the set of all polynomials with the form $f(x) = ax^2 + bx + c$ for some $a, b, c \in \mathbb{R}$. If $f(x), g(x) \in S$ then $f(x) \sim g(x)$ if and only if $f(x)$ and $g(x)$ have the same set of zeros. For example, $f(x) = x^2 - 2x + 1 = (x-1)^2$ and $g(x) = x^2 - 3x + 2 = (x-1)(x-2)$ are not equivalent since $f(x)$ has zeroes $1, 1$ whereas $g(x)$ has zeroes $1, 2$. I invite the reader to verify this is an equivalence relation. Let's explore the equivalence classes,*

$$[1] = [3] = [x^2 + 1] = [x^2 + 4x + 5]$$

since all the representative polynomials above have $\emptyset$ as their set of zeros.

$$[x - 1] = \{a(x - 1) \mid a \in \mathbb{R}, a \neq 0\}$$

$$[2x^2 - 6x + 4] = [x^2 - 3x + 2] = \{a(x^2 - 3x + 2) \; a \in \mathbb{R}, a \neq 0\}$$

The partition formed from the next example is geometrically interesting.

Example 5.2.17. *(path connected) A path in S from a to b is a continuous mapping f from $[0, 1]$ into S such that $f(0) = a$ and $f(1) = b$. Let S be some space S. We say that two points $a, b \in S$ are path-connected (let's denote this by R) if there is a path from a to b. Notice that R is reflexive since*

$$f(t) = a, \qquad \textit{for each } t \in [0, 1]$$

is a continuous mapping from a to a and we can construct such a map at each point in S.

Furthermore, suppose that $a, b \in S$ such that aRb then there exists $f : [0, 1] \to S$ such that $f(0) = a$ and $f(1) = b$. Define $g : [0, 1] \to S$ by the formula:

$$g(t) = f(1 - t)$$

We see that $g(0) = f(1) = b$ and $g(1) = f(0) = a$ hence g is a path from b to a. Therefore, R is symmetric.

Finally, if a, b, c are points in S such that aRb and bRc then there exist mappings $f : [0, 1] \to S$ with $f(0) = a$ and $f(1) = b$, and $g : [0, 1] \to S$ with $g(0) = b$ and $g(1) = c$ We can construct a path from a to c as follows:

$$h(t) = \begin{cases} f(2t) & \textit{if } 0 \leq t \leq 1/2 \\ g(2t - 1) & \textit{if } 1/2 \leq t \leq 1 \end{cases}$$

It's easy to check that $h(0) = a$ and $h(1) = c$ hence aRc thus R is transitive. Hence R is an equivalence relation.

It's easy to check that $h(0) = a$ and $h(1) = c$ hence $a \sim c$ thus $\sim$ is transitive. Hence R is an equivalence relation. The subsets of S which are elements of S/R are called path components of S. If S has just one path component then S is said to be path connected. This simply means any two points in S can be connected by some path. For example, $\mathbb{R}^m$ is path connected if $m \in \mathbb{N}$. Other spaces are not. For example, you could think about the set of all invertible n by n square matrices (denoted $GL(n, \mathbb{R})$ if we want matrices with real components). Some of these matrices have $det(A) > 0$ whereas others have $det(A) < 0$. However, there is no invertible matrix with $det(A) = 0$ which means you cannot find a path to connect the two cases. Thus it turns out that $GL(n, \mathbb{R})$ has two equivalence classes with respect to the R of this example. In turn, $GL(n, \mathbb{R})$ is partitioned into two disjoint sets; matrices with positive determinant and matrices with negative determinant.

Yes, I did just talk about a path of matrices in the last example. I dare you to visualize that path. When you do draw me the picture. Equivalence classes have applications you might be surprised by. The following example outlines the equivalence class of curves viewpoint for tangent vectors. Not everyone has had, or is taking, or will take, Calculus III, so relax, I'm not going to test on partial differentiation. But, some of you will learn this or are currently learning this so I hope you can forgive me for this possible digression.

Example 5.2.18. *(tangent vectors) Let $S \subset \mathbb{R}^3$ be a surface defined as the level-set of a function $F : \mathbb{R}^3 \to \mathbb{R}$; that is S is the set of points $(x, y, z) \in \mathbb{R}^3$ such that $F(x, y, z) = 0$. Parametric curves on S are paths from $\mathbb{R}$ to S. Denote the set of all smooth parametric curves on S that pass through $p \in S$ at time zero to be $C^1(p)$. Let $f, g \in C^1(p)$ then we say $f \sim g$ iff $f(0) = g(0) = p$ and $f'(0) = g'(0)$. I claim $\sim$ is an equivalence relation. Let $f \in C^1(p)$,*

$$f(0) = f(0) \text{ and } f'(0) = f'(0)$$

thus $\sim$ is clearly reflexive. Also, if $f, g \in C^1(p)$ and $f \sim g$ then $f'(0) = g'(0)$ hence $g'(0) = f'(0)$ so $g \sim f$. Moreover, if $f, g, h \in C^1(p)$ and $f \sim g$ and $g \sim h$ it follows that $f'(0) = g'(0)$ and $g'(0) = h'(0)$ hence $f'(0) = h'(0)$ which shows $f \sim h$. Thus $\sim$ is an equivalence relation on $C^1(p)$.

We can identify $\bar{\gamma} = \{f \in C^1(p) \mid f'(0) = \gamma'(0), \gamma(0) = p\}$. You can visualize $\bar{\gamma}$ in $\mathbb{R}^3$, it will be a vector that points in some direction $\vec{v} = \gamma'(0)$. The tangent space to S is formed by taking the union of all such vectors. In view of $\sim$ we can say that each element of the tangent space is an equivalence class of curves.

Besides the abstract, $\sim$ also gives us a tool to calculate the equation for the tangent plane at p. Let $g \in C^1(p)$ be a path on S then

$$F(g(t)) = 0$$

since the path $t \mapsto g(t)$ is assumed to lie on the surface S. Define the components of $g(t)$ as follows $g(t) = (a(t), b(t), c(t))$. The chain rule applied to $F \circ g$ goes as follows:

$$\frac{d}{dt}\bigg(F(a, b, c)\bigg) = \frac{\partial F}{\partial x}\frac{da}{dt} + \frac{\partial F}{\partial y}\frac{db}{dt} + \frac{\partial F}{\partial z}\frac{dc}{dt}$$

But, $F \circ g = 0$ so the derivative above must equal zero. Moreover, notice that the derivative of the parametric curve $g'(t) =< a'(t), b'(t), c'(t) >$. We can rewrite the chain-rule above as

$$(\nabla F)(g(t)) \cdot g'(t) = 0$$

If we focus our attention to time $t = 0$ where $g(0) = p$ and $\vec{v} = g'(0)$ we find the condition above tells us that

$$(\nabla F)(p) \cdot \vec{v} = 0$$

This holds for each and every tangent vector $\vec{v}$ at $p \in S$. It stands to reason that $(\nabla F)(p)$ is the normal vector to the tangent plane of S at p.

5.3 order relations

Let us begin by setting the terms.

Definition 5.3.1. *A relation R is* **antisymmetric** *iff whenever xRy and yRx, then $x = y$. A* **partial ordering** *is a relation that is reflexive, antisymmetric, and transitive. A* **total ordering** *is a partial ordering R in which xRy or yRx holds for every x and y in the domain of R. We likewise say R is a partial (or total) ordering on $dom(R)$. Sometimes total orderings are also called* **simple orderings** *or* **linear orderings**.

Notice the difference between an equivalence relation and a partial ordering is that symmetry has been replaced by antisymetry. These are not opposites. They're different. Qualitatively, equivalence relations capture a certain sameness in a set of objects whereas a partial ordering institutes some sort of hierarchy. Typically the notation xRy may be replaced with $x \leq y$ or $x \geq y$ as the context warrants. Customarily, it is understood that $x \leq y$ is interchangeable with $y \geq x$.

Example 5.3.2. *For $x, y \in \mathbb{R}$, define xRy iff $x \leq y$. Let $x, y, z \in \mathbb{R}$ in what follows. Observe that $x \leq x$ thus $\leq$ is reflexive. Also, if $x \leq y$ and $y \leq x$ then $x = y$ hence $\leq$ is antisymmetric. Consider if $x \leq y$ and $y \leq z$ then $x \leq z$ thus $\leq$ is transitive. In summary, $R = \leq$ is a total ordering on $\mathbb{R}$. Furthermore, by the same arguments, if we restrict the domain of $\leq$ to $\mathbb{N}$ or $\mathbb{Z}$ or $\mathbb{Q}$ then we find the usual $\leq$ serves to define a total ordering on $\mathbb{N}$, $\mathbb{Z}$ or $\mathbb{Q}$.*

The example above should not be surprising, the definition of $\leq$ on $\mathbb{R}$ was probably the motivation for forming such a definition. On the other hand, the example below might be a bit surprising. It also is important in the formulation of some proofs which rest on something called **Zorn's lemma**[4]. It states that a partially ordered set in which every chain is bounded contains at least one maximal element. A chain is a subset which is totally ordered in this context. There are two places I use Zorn's lemma in undergraduate mathematics. One, to prove existence of basis for arbitrary vector spaces. Two, in the theory of factorization over general rings.

Example 5.3.3. *Let X be a set and suppose $\mathcal{P}(X)$ is the power set of X. Let $U, V \in \mathcal{P}(X)$ then $U\,R\,V$ iff $U \subseteq V$. Consider $U \subseteq U$ for any $U \in \mathcal{P}(X)$ thus R is reflexive. Further, if $U, V \in \mathcal{P}(X)$ and $U\,R\,V$ and $V\,R\,U$ then $U \subseteq V$ and $V \subseteq U$ thus by double containment $U = V$. Hence R is antisymmetric. Furthermore, if $U, V, W \in \mathcal{P}(X)$ and $U\,R\,V$ and $V\,R\,W$ then $U \subseteq V$ and $V \subseteq W$ hence $U \subseteq W$ and so $U\,R\,W$ and we find R is transitive. We find $R = \subseteq$ forms a partial ordering on $\mathcal{P}(X)$.*

Definition 5.3.4. *If R is a partial ordering, x and y are called* **comparable** *with respect to R iff xRy or yRx holds. If $x, y \in Dom(R)$ but are not comparable then they are called* **incomparable**.

A total ordering has no incomparable elements. Notice, if $U, V \subseteq X$ then it may be the case that $U \subseteq V$ and $V \subseteq U$ are both false. Thus the $R = \subseteq$ is an ordering on X which is partial, but not total since there exist incomparable elements.

[4] not to be confused with Hollis Frampton's film linked above

Definition 5.3.5. *A relation is called* **irreflexive** *iff xRx is* **not** *true for any x. A relation that is irreflexive and transitive is called an* **irreflexive partial ordering**. *An* **irreflexive total ordering** *is an irreflexive partial ordering which satisfies the* **trichtomy***: for every $x, y \in Dom(R)$ either xRy or yRx or $x = y$.*

Notice that an irreflexive partial ordering R cannot have both xRy and yRx since the transitive property implies xRx which is assumed false for an irreflexive relation. You might have guessed by now, irreflexive partial orderings are modelled on the usual ”less than” or ”greater than” inequalities on $\mathbb{R}$.

Example 5.3.6. *For $x, y \in \mathbb{R}$, define xRy iff $x < y$. Observe that $x \nless x$ thus R is irreflexive. Likewise, if $x, y, z \in \mathbb{R}$ and $x < y$ and $y < z$ then $x < z$ hence R is transitive. Furthermore, given $x, y \in \mathbb{R}$ we certainly have either $x < y$, $y < x$ or $x = y$ hence R satisfies the trichotomy. Naturally, $\mathbb{R}$ is given an irreflexive total ordering via $<$.*

I'll stop here, there is always more to say, but I I'll leave any missing bits for the homework. In particular, we should see a problem about **well-ordering** and perhaps a question about the **lexographic ordering**. The lexographic ordering gives us a way to order $A \times B$ if we have an ordering for A and B respective.

Chapter 6

Modular Arithmetic

The formal study of modular arithmetic is usually attributed to Carl Friedrich Gauss. He introduced the idea in his book *Disquisitiones Arithmeticae* in around 1801. History aside, modular arithmetic is familar to us in many ways. Clocks and calendars have a periodicity that allows us to group certain days, dates or times as being all part of the same class. The rules by which we add hours and minutes are examples of modular arithmetic. We will discuss how $\mathbb{Z}_n$ is formed from equivalences classes of $\mathbb{Z}$. The equivalence classes that comprise $\mathbb{Z}_n$ are quite special because they can be added, subtracted, multiplied and *sometimes* divided. In other words, the equivalence classes that make up $\mathbb{Z}_n$ behave just like numbers in $\mathbb{R}$. However, there is a difference. We will find equations such as $1 + 1 = 0$ and $2 \cdot 3 = 0$ make sense in a certain context.

Let me begin with an example (contrary to my natural tendencies)

Example 6.0.1. *The following calculations are performed in* $\mathbb{Z}_5$*:*

$$2 + 3 = 5 \equiv 0, \qquad (2)(3) = 6 \equiv 1, \qquad (2)(4) = 8 \equiv 3$$

Here the basic idea is that numbers which differ by 5 *units are equivalent. I'm using the notation* $\equiv$ *is denote when two things are* **congruent**. *Since* $0 \equiv 5 \equiv -100 \equiv 25 \equiv \cdots$ *there is much ambiguity in the presentation of an equation "mod 5".*

We study the construction of $\mathbb{Z}_n$ in this chapter and we develop some basic calculational strategies for how we should actually calculate expressions in $\mathbb{Z}_n$. One major tool is the **Euclidean algorithm** which is based on the division algorithm of gradeschool arithmetic. We build these things from the base up using both set theory and the equivalence relations concept we learned in the last chapter. Finally, at the end of the chapter we learn the "grown-up" notation which hides much of what we do in this chapter from explicit view. Our goal here is both to learn the detailed construction of $\mathbb{Z}_n$ and also how to wisely calculuate in $\mathbb{Z}_n$ for the sake of future work.

I should mention, $\mathbb{Z}_n$ is a fundamental example of a *commutative ring with unity*, it has addition and multiplication which interact as you would expect. However, division is more nuanced. There are numbers which cannot be inverted in the multiplicative sense. In fact, the number of invertible numbers modulo n is known as $\varphi(n)$, the so-called **Euler** φ-function. It plays a foundational role in the mathematics of current cyrptography. The invertible numbers in $\mathbb{Z}_n$ are denoted $U(n)$ (the *group of units*). These provide foundational examples for Math 421. Our hope is that by exposing you to this material here it helps make the abstract algebra course considerably less troublesome. This material isn't particularly difficult, but it certainly involves a number of novelties.

6.1 $\mathbb{Z}$-Basics

Let's start at the very beginning, it is a good place to start.

Definition 6.1.1. *The integers $\mathbb{Z}$ are the set of natural numbers $\mathbb{N}$ together with 0 and the negatives of $\mathbb{N}$. It is possible to concretely construct (we will not) these from sets and set-operations.*

From the construction of $\mathbb{Z}$ it is clear (we assume these to be true)

1. the sum of integers is an integer
2. the product of integers is an integer
3. the usual rules of arithmetic hold for $\mathbb{Z}$

Much is hidden in (3.): let me elaborate, we assume for all $a, b, c \in \mathbb{Z}$,

$$\begin{aligned} a+b &= b+a \\ ab &= ba \\ a(b+c) &= ab+ac \\ (a+b)c &= ac+bc \\ (a+b)+c &= a+(b+c) \\ (ab)c &= a(bc) \\ a+0 &= 0+a = a \\ 1a &= a1. \end{aligned}$$

Where we assume the **order of operations** is done multiplication then addition; so, for example, $ab + ac$ means to first multiply a with b and a with c then you add the result.

Let me comment briefly about our standard conventions for the presentation of numbers. If I write 123 then we understand this is the **base-ten** representation. In particular,

$$123 = 1 \times 10^2 + 2 \times 10 + 3.$$

On the other hand, $1 \cdot 2 \cdot 3$ denotes the product of $1, 2$ and 3 and $1 \cdot 2 \cdot 3 = 6$. By default, algebraic variables juxtaposed denote multiplication; xy denotes x multiplied by y. If we wish for symbolic variables to denote digits in a number then we must explain this explicitly. For example, to study all numbers between 990 and 999 I could analyze $99x$ where $x \in \{0, 1, \dots, 9\}$. But, to be clear I ought to preface such analysis by a statement like: let $99x$ be the base-ten representation of a number where x represents the 1's digit.

6.2 division algorithm

Division is repeated subtraction. For example, consider $11/3$. Notice repeated subtraction of the dividing number[1] 3 gives:

$$11 - 3 = 8 \qquad 8 - 3 = 5 \qquad 5 - 3 = 2$$

[1] my resident Chinese scholar tells me in Chinese a/b has the "dividing" number b and the "divided" number a. I am tempted to call b the divisor, but the term "divisor" has a precise meaning, if b is a divisor of a then $a = mb$ for some $n \in \mathbb{Z}$. In our current discussion, to say b is a divisor assumes the remainder is zero.

then we cannot subtract anymore. We were able to subtract 3 copies of 3 from 11. Then we stopped at 2 since $2 < 3$. To summarize,

$$\boxed{11 = 3(3) + 2}$$

We say 2 is the **remainder**; the remainder is the part which is too small to subtract for the given *dividing number*. Divide the boxed equation by the divisor to see:

$$\frac{11}{3} = 3 + \frac{2}{3}.$$

The generalization of the boxed equation for an arbitrary pair of natural numbers is known as the **division algorithm**.

Theorem 6.2.1. positive division algorithm: *If $a, b \in \mathbb{Z}$ with $b > 0$ then there is a unique quotient $q \in \mathbb{Z}$ and remainder $r \in \mathbb{Z}$ for which $a = qb + r$ and $0 \leq r < b$.*

Proof (existence): suppose $a, b \in \mathbb{Z}$ and $b > 0$. Construct $R = \{a - nb \mid q \in \mathbb{Z}, \quad a - nb \geq 0\}$. The set R comprises all non-negative integers which are reached from a by integer multiples of b. Explicitly,

$$R = \{a, a \pm b, a \pm 2b, \dots\} \cap \{0, 1, 2, \dots\}.$$

To prove R is non-empty we consider $n = -|a| \in \mathbb{Z}$ yields $a - nb = a + |a|b$. If $a \geq 0$ then clearly $a + |a|b \geq 0$. If $a < 0$ then $|a| = -a$ hence $a + |a|b = -|a| + |a|b = |a|(b-1)$ but $b \in \mathbb{N}$ by assumption hence $b \geq 1$ and we find $a + |a|b \geq 0$. Therefore, as R is a non-empty subset of the non-negative integers. We apply the **Well-Ordering-Principle** to deduce there exists a smallest element $r \in R$.

Suppose r is the smallest element in R and $r \geq b$. In particular, $r = a - nb$ for some $n \in \mathbb{Z}$. Thus $a - nb \geq b$ hence $r' = a - (n+1)b \geq 0$ hence $r' \in R$ and $r' < r$. But $r' < r$ contradicts r being the smallest element. Thus, using proof by contradiction, we find $r < b$.

Proof (uniqueness): assume $q, q' \in \mathbb{Z}$ and $r, r' \in \mathbb{Z}$ such that $a = qb + r$ and $a = q'b + r'$ where $0 \leq r, r' < b$. We have $qb + r = q'b + r'$ hence $(q - q')b = r - r'$. Suppose towards a contradiction $q \neq q'$. Since $q, q' \in \mathbb{Z}$ the inequality of q and q' implies $|q - q'| \geq 1$ and thus $|r - r'| = |(q - q')b| \geq |b| = b$. However, $r, r' \in [0, b)$ thus the distance[2] between r and r' cannot be larger than or equal to b. This is a contradiction, therefore, $q = q'$. Finally, $qb + r = q'b + r'$ yields $r = r'$. $\square$

We can say more about q and r in the case $b > 0$. We have

$$\frac{a}{b} = q + \frac{r}{b} \qquad \& \qquad q = \lfloor a/b \rfloor$$

That is q is the greatest integer which is below a/b. The function $x \mapsto \lfloor x \rfloor$ is the **floor function**. For example,

$$\lfloor -0.4 \rfloor = -1, \qquad \lfloor \pi \rfloor = 3, \qquad \lfloor n + \varepsilon \rfloor = n$$

for all $n \in \mathbb{Z}$ provided $0 \leq \varepsilon < 1$. It is easy to calculate the floor function of x when x is presented in decimal form. For example,

$$\frac{324}{11} = 29.4545... \quad \Rightarrow \quad \frac{324}{11} = 29 + 0.4545... \quad \Rightarrow \quad 324 = 29(11) + (0.4545...)(11)$$

[2] for a non-geometric argument here: note $0 \leq r < b$ and $0 \leq r' < b$ imply $-r' < r - r' < b - r' \leq b$. But, $r' < b$ gives $-b < -r'$ hence $-b < r - r' < b$. Thus $|r - r'| < b$. Indeed, the distance between r and r' is less than b.

We can calculate, $0.4545 \cdot 11 = 4.9995$. From this we find

$$324 = 29(11) + 5$$

In other words, $\frac{324}{11} = 29 + \frac{5}{11}$. The decimal form of numbers and the floor function provides a simple way to find quotients and remainders.

Consider $456/(-10) = -45.6 = -45 - 0.6$ suggests $456 = (-10)(-45) + 6$. In the case of a negative divisor ($b < 0$) the division algorithm needs a bit of modification:

Theorem 6.2.2. nonzero division algorithm: *If $a, b \in \mathbb{Z}$ with $b \neq 0$ then there is a unique quotient $q \in \mathbb{Z}$ and remainder $r \in \mathbb{Z}$ for which*

$$a = qb + r \qquad \& \qquad 0 \leq r < |b|.$$

Proof: Theorem 6.2.1 covers case $b > 0$. Thus, assume $b < 0$ hence $b' = -b > 0$. Apply Theorem 6.2.1 to $a, b' \in \mathbb{Z}$ to find q', r' such that $a = q'b' + r'$ with $0 \leq r' < b'$. However, $b' = -b = |b|$ as $b < 0$. Thus,

$$a = -q'b + r'$$

with $0 \leq r' < |b|$. Identify $q = -q'$ and $r = r'$ in the case $b < 0$. Uniqueness is clear from the equations which define q and r from the uniquely given q' and r'. This concludes the proof as $b \neq 0$ means either $b < 0$ or $b > 0$. □

The selection of the quotient in the negative divisor case is given by the **ceiling** function $x \mapsto \lceil x \rceil$. The notation $\lceil x \rceil$ indicates the next integer which is greater than or equal to x. For example,

$$\lceil 456/(-10) \rceil = -45, \quad \lceil 3.7 \rceil = 4, \quad \lceil n - \varepsilon \rceil = n$$

for all $n \in \mathbb{Z}$ given $0 \leq \varepsilon < 1$.

Remark 6.2.3. The division algorithm proves an assertion of elementary school arithmetic. For example, consider the **improper fraction** 10/3 we can write it as the sum of 3 and 1/3. When you write $3\frac{1}{3}$ what is truly meant is $3 + \frac{1}{3}$. In fact, the truth will set you free of a myriad of errors which arise from the poor notation $3\frac{1}{3}$. With this example in mind, let $a, b \in \mathbb{N}$. The division algorithm simply says for a/b there exists $q, r \in \mathbb{N} \cup \{0\}$ such that $a = qb + r$ hence $a/b = q + r/b$ where $0 \leq r < b$. This is merely the statement that any improper fraction can be reduced to the sum of a whole number and a proper fraction. In other words, you already knew the division algorithm. However, thinking of it without writing fractions is a bit of an adjustment for some of us.

6.3 divisibility in $\mathbb{Z}$

Consider $105 = 3 \cdot 5 \cdot 7$. We say 3 is a *factor* or *divisor* of 105. Also, we say 35 *divides* 105. Furthermore, 105 is a *multiple* of 3. Indeed, 105 is also a multiple of 5, 7 and even 21 or 35. Examples are nice, but, definitions are crucial:

Definition 6.3.1. *Let $a, b \in \mathbb{Z}$ then we say b* **divides** *a if there exists $c \in \mathbb{Z}$ such that $a = bc$. If b divides a then we also say b is a* **factor** *of a and a is a* **multiple** *of b.*

The notation $b \mid a$ means b divides a. If b is does not divide a then we write $b \nmid a$. The divisors of a given number are not unique. For example, $105 = 7(15) = (3)(35) = (-1)(-105)$. However, the prime divisors are unique up to reordering: $105 = (3)(5)(7)$. Much of number theory is centered around the study of primes. We ought to give a proper definition:

Definition 6.3.2. *If $p \in \mathbb{N}$ such that $n \mid p$ implies $n = p$ or $n = 1$ then we say p is* **prime**.

In words: a prime is a positive integer whose only divisors are 1 and itself.

There are many interesting features of divisibility. Notice, every number $b \in \mathbb{Z}$ divides 0 as $0 = b \cdot 0$. Furthermore, $b \mid b$ for all $b \in \mathbb{Z}$ as $b = b \cdot 1$. In related news, 1 is a factor of every integer and every integer is a multiple of 1[3]

Proposition 6.3.3. *Let $a, b, c, d, m \in \mathbb{Z}$. Then,*

(i.) *if $a \mid b$ and $b \mid c$ then $a \mid c$,*

(ii.) *if $a \mid b$ and $c \mid d$ then $ac \mid bd$,*

(iii.) *if $m \neq 0$, then $ma \mid mb$ if and only if $a \mid b$*

(iv.) *if $d \mid a$ and $a \neq 0$ then $|d| \leq |a|$.*

Proof (i.) : suppose $a \mid b$ and $b \mid c$. By the definition of divisibility there exist $m, n \in \mathbb{Z}$ such that $b = ma$ and $c = nb$. Hence $c = n(ma) = (nm)a$. Therefore, $a \mid c$ as $nm \in \mathbb{Z}$.

Proof (ii.) : suppose $a \mid b$ and $c \mid d$. By the definition of divisibility there exist $m, n \in \mathbb{Z}$ such that $b = ma$ and $d = nc$. Subsitution yields $bd = (ma)(nc) = mn(ac)$. But, $mn \in \mathbb{Z}$ hence we have shown $ac \mid bd$.

Proof (iii.) : left to the reader.

Proof (iv.) : if $d \mid a$ and $a \neq 0$ then $a = md$ for some $m \in \mathbb{Z}$. Suppose $m = 0$ then $a = (0)d = 0$ which contradicts $a \neq 0$. Therefore, $m \neq 0$. Recall that the absolute value function is multiplicative; $|md| = |m||d|$. As $m \neq 0$ we have $|m| \geq 1$ thus $|a| = |m||d| \geq |d|$. $\square$

I hope you see these proofs are not too hard. You ought to be able to reproduce them without much effort.

Theorem 6.3.4. *Let $a_1, \dots, a_k, c \in \mathbb{Z}$. Then,*

(i.) *if $c \mid a_i$ for $i = 1, \dots, k$ then $c \mid (u_1 a_1 + \cdots + u_k a_k)$ for all $u_1, \dots, u_k \in \mathbb{Z}$,*

(ii.) *$a \mid b$ and $b \mid a$ if and only if $a = \pm b$.*

Proof (i.): suppose $c \mid a_1, c \mid a_2, \dots, c \mid a_k$. It follows there exist $m_1, m_2, \dots, m_k \in \mathbb{Z}$ such that $a_1 = cm_1$, $a_2 = cm_2$ and $a_k = cm_k$. Let $u_1, u_2, \dots, u_k \in \mathbb{Z}$ and consider,

$$u_1 a_1 + \cdots + u_k a_k = u_1(cm_1) + \cdots + u_k(cm_k) = c(u_1 m_1 + \cdots + u_k m_k).$$

[3] I should mention, I am partly following the excellent presentation of Jones and Jones *Elementary Number Theory* which I almost used as the text for Math 307 in Spring 2015. We're on page 4.

Notice $u_1m_1 + \cdots + u_km_k \in \mathbb{Z}$ thus the equation above shows $c \mid (u_1a_1 + \cdots + u_ka_k)$.

Proof (ii.): suppose $a \mid b$ and $b \mid a$. If $a = 0$ then $a \mid b$ implies there exists $m \in \mathbb{Z}$ such that $b = m(0) = 0$ hence $b = 0$. Observe $a = \pm b = 0$. Continuing, we suppose $a \neq 0$ which implies $b \neq 0$ by the argument above. Notice $a \mid b$ and $b \mid a$ imply there exist $m, n \in \mathbb{Z} - \{0\}$ such that $a = mb$ and $b = na$. Multiply $a = mb$ by $n \neq 0$ to find $na = mnb$. But, $b = na$ hence $na = mn(na)$ which implies $1 = mn$. Thus, $m = n = 1$ or $m = n = -1$. These cases yield $a = b$ and $a = -b$ respective hence $a = \pm b$. □

The proof above is really not much more difficult than those we gave for Proposition 6.3.3. The most important case of the Theorem above is when $k = 2$ in part (i.).

Corollary 6.3.5. *If $c \mid x$ and $c \mid y$ then $c \mid (ax + by)$ for all $a, b \in \mathbb{Z}$.*

The result above is used repeatedly as we study the structure of common divisors.

Definition 6.3.6. *If $d \mid a$ and $d \mid b$ then d is a* **common divisor** *of a and b.*

Proposition 6.3.3 part (iv.) shows that a divisor cannot have a larger magnitude than its multiple. It follows that the largest a common divisor could be is $\max\{|a|, |b|\}$. Furthermore, 1 is a divisor of all nonzero integers. If both a and b are not zero then $\max\{|a|, |b|\} \geq 1$. Therefore, if both a and b are not zero then there must be a largest number between 1 and $\max\{|a|, |b|\}$ which divides both a and b. Thus, the definition to follow is reasonable:

Definition 6.3.7. *If $a, b \in \mathbb{Z}$, not both zero, then the* **greatest common divisor** *of a and b is denoted $gcd(a, b)$.*

The method to find the greatest common divisor which served me well as a child was simply to a and b in their prime factorization. Then to find the gcd I just selected all the primes which I could pair in both numbers.

Example 6.3.8.

$$gcd(105, 90) = gcd(\underline{3 \cdot 5} \cdot 7,\ 2 \cdot 3 \cdot \underline{3 \cdot 5}) = 3 \cdot 5 = 15.$$

The method above faces several difficulties as we attempt to solve non-elementary problems.

1. it is not an easy problem to find the prime factorization of a given integer. Indeed, this difficulty is one of the major motivations RSA cryptography.

2. it is not so easy to compare lists and select all the common pairs. Admittedly, this is not as serious a problem, but even with the simple example above I had to double-check.

Thankfully, there is a better method to find the gcd. It's old, but, popular. Euclid (yes, the same one with the parallel lines and all that) gave us the **Euclidean Algorithm**. We prove a Lemma towards developing Euclid's Algorithm.

Lemma 6.3.9. *Let $a, b, q, r \in \mathbb{Z}$. If $a = qb + r$ then $gcd(a, b) = gcd(b, r)$.*

Proof: by Corollary 6.3.5 we see a divisor of both b and r is also a divisor of a. Likewise, as $r = a - qb$ we see any common divisor of a and b is also a divisor of r. It follows that a, b and b, r share the same divisors. Hence, $gcd(a, b) = gcd(b, r)$. □

We now work towards Euclid's Algorithm. Let $a, b \in \mathbb{Z}$, not both zero. Our goal is to calculate $gcd(a, b)$. If $a = 0$ and $b \neq 0$ then $gcd(a, b) = |b|$. Likewise, if $a \neq 0$ and $b = 0$ then $gcd(a, b) = |a|$. Note $gcd(a, a) = |a|$ hence we may asssume $a \neq b$ in what follows. Furthermore,

$$gcd(a, b) = gcd(-a, b) = gcd(a, -b) = gcd(-a, -b).$$

Therefore, suppose $a, b \in \mathbb{N}$ with $a > b$[4]. Apply the division algorithm (Theorem 6.2.1) to select q_1, r_1 such that

$$a = q_1 b + r_1 \qquad \text{such that} \qquad 0 \leq r_1 < b.$$

If $r_1 = 0$ then $a = q_1 b$ hence $b \mid a$ and as b is the largest divisor of b we find $gcd(a, b) = b$. If $r_1 \neq 0$ then we continue to apply the division algorithm once again to select q_2, r_2 such that

$$b = q_2 r_1 + r_2 \qquad \text{such that} \qquad 0 \leq r_2 < r_1.$$

If $r_2 = 0$ then $r_1 \mid b$ and clearly $gcd(b, r_1) = r_1$. However, as $a = q_1 b + r_1$ allows us to apply Lemma 6.3.9 to obtain $gcd(a, b) = gcd(b, r_1) = r_1$. Continuing, we suppose $r_2 \neq 0$ with $r_1 > r_2$ hence we may select q_3, r_3 for which:

$$r_1 = q_3 r_2 + r_3 \qquad \text{such that} \qquad 0 \leq r_3 < r_2.$$

Once again, if $r_3 = 0$ then $r_2 \mid r_1$ hence it is clear $gcd(r_1, r_2) = r_2$. However, as $b = q_2 r_1 + r_2$ gives $gcd(b, r_1) = gcd(r_1, r_2)$ and $a = q_1 b + r_1$ gives $gcd(a, b) = gcd(b, r_1)$ we find that $gcd(a, b) = r_2$. This process continues. It cannot go on forever as we have the conditions:

$$0 < \cdots < r_3 < r_2 < r_1 < b.$$

There must exist some $n \in \mathbb{N}$ for which $r_{n+1} = 0$ yet $r_n \neq 0$. All together we have:

$$\begin{aligned} a &= q_1 b + r_1, \\ b &= q_2 r_1 + r_2, \\ r_1 &= q_3 r_2 + r_3, \ldots, \\ r_{n-2} &= q_n r_{n-1} + r_n, \\ r_{n-1} &= q_{n+1} r_n. \end{aligned}$$

The last condition yields $r_n \mid r_{n-1}$ hence $gcd(r_{n-1}, r_n) = r_n$. Furthermore, we find, by repeated application of Lemma 6.3.9 the following string of equalities

$$gcd(a, b) = gcd(b, r_1) = gcd(r_1, r_2) = gcd(r_2, r_3) = \cdots = gcd(r_{n-1}, r_n) = r_{n-1}.$$

In summary, we have shown that repeated division of remainders into remainder gives a strictly decreasing sequence of positive integers whose last member is precisely $gcd(a, b)$.

Theorem 6.3.10. Euclidean Algorithm: *suppose $a, b \in \mathbb{N}$ with $a > b$ and form the finite sequence $\{b, r_1, r_2, \ldots, r_n\}$ for which $r_{n+1} = 0$ and $b, r_1, \ldots, r_n$ are defined as discussed above. Then $gcd(a, b) = r_n$.*

Example 6.3.11. *Let me show you how the euclidean algorithm works for a simple example. Consider $a = 100$ and $b = 44$. Euclid's algorithm will allow us to find $gcd(100, 44)$.*

[4] the equation above shows we can cover all other cases once we solve the problem for positive integers.

1. $100 = 44(2) + 12$ *divided 100 by 44 got remainder of 12*
2. $44 = 12(3) + 8$ *divided 44 by 12 got remainder of 8*
3. $12 = 8(1) + \boxed{4}$ *divided 12 by 8 got remainder of 4*
4. $8 = 4(2) + 0$ *divided 4 by 1 got remainder of zero*

The last nonzero remainder will always be the gcd when you play the game we just played. Here we find $\boxed{gcd(100, 44) = 4}$. *Moreover, we can write* 4 *as a* $\mathbb{Z}$*-linear combination of* 100 *and* 44. *This can be gleaned from the calculations already presented by working backwards from the gcd:*

3. $4 = 12 - 8$
2. $8 = 44 - 12(3)$ *implies* $4 = 12 - (44 - 12(3)) = 4(12) - 44$
1. $12 = 100 - 44(2)$ *implies* $4 = 4(100 - 44(2)) - 44 = 4(100) - 9(44)$

I call this a ”$\mathbb{Z}$*-linear combination of* 100 *and* 44 *since* $4, -9 \in \mathbb{Z}$. *We find* $\boxed{4(100) - 9(44) = 4}$.

The fact that we can always work euclid's algorithm backwards to find how the $gcd(a, b)$ is written as $ax + by = gcd(a, b)$ for some $x, y \in \mathbb{Z}$ is remarkable. I continue to showcase this side-benefit of the Euclidean Algorithm as we continue. We will give a general argument after the examples. I now shift to a less verbose presentation:

Example 6.3.12. *Find* $gcd(62, 626)$

$$626 = 10(62) + 6$$

$$62 = 10(6) + 2$$

$$6 = 3(2) + 0$$

From the E.A. I deduce $gcd(62, 626) = 2$. *Moreover,*

$$2 = 62 - 10(6) = 62 - 10[626 - 10(62)] = 101(62) - 10(626)$$

Example 6.3.13. *Find* $gcd(240, 11)$.

$$240 = 11(21) + 9$$

$$11 = 9(1) + 2$$

$$9 = 2(4) + 1$$

$$2 = 1(2)$$

Thus, by E.A., $gcd(240, 11) = 1$. *Moreover,*

$$1 = 9 - 2(4) = 9 - 4(11 - 9) = -4(11) + 5(9) = -4(11) + 5(240 - 11(21))$$

That is,

$$\boxed{1 = -109(11) + 5(240)}$$

Example 6.3.14. *Find gcd*$(4, 20)$. *This example is a bit silly, but I include it since it is an exceptional case in the algorithm. The algorithm works, you just need to interpret the instructions correctly.*

$$20 = 4(5) + 0$$

Since there is only one row to go from we identify 4 *as playing the same role as the last non-zero remainder in most examples. Clearly, gcd*$(4, 20) = 4$. *Now, what about working backwards? Since we do not have the gcd appearing by itself in the next to last equation (as we did in the last example) we are forced to solve the given equation for the gcd,*

$$20 = 4(4 + 1) = 4(4) + 4 \implies \boxed{20 - 4(4) = 4}$$

The following result also follows from the discussion before Theorem 6.3.10. I continue to use the notational set-up given there.

Theorem 6.3.15. Bezout's Identity: *if* $a, b \in \mathbb{Z}$, *not both zero, then there exist* $x, y \in \mathbb{Z}$ *such that* $ax + by = gcd(a, b)$.

Proof: we have illustrated the proof in the examples. Basically we just back-substitute the division algorithms. For brevity of exposition, I assume $r_3 = gcd(a, b)$. It follows that:

$$\begin{aligned} a = q_1b + r_1 &\quad\Rightarrow\quad r_1 = a - q_1b \\ b = q_2r_1 + r_2 &\quad\Rightarrow\quad r_2 = b - q_2r_1 \\ r_1 = q_3r_2 + r_3 &\quad\Rightarrow\quad r_3 = r_1 - q_3r_2 \end{aligned}$$

where $gcd(a, b) = r_3$. Moreover, $r_2 = b - q_2(a - q_1b)$ implies $r_3 = r_1 - q_3[b - q_2(a - q_1b)]$. Therefore,

$$gcd(a, b) = a - q_1b - q_3[b - q_2(a - q_1b)] = a - (q_1 - q_3[1 - q_2(a - q_1)]b.$$

Identify $x = 1$ and $y = q_1 - q_3[1 - q_2(a - q_1)]$. □

We should appreciate that x, y in the above result are far from unique. However, as we have shown, the method at least suffices to find a solution of the equation $ax + by = gcd(a, b)$.

Corollary 6.3.16. *There exist* $a, b, x, y \in \mathbb{Z}$ *such that* $ax + by = 1$ *if and only if* $gcd(a, b) = 1$.

Proof: the converse direction is immediate from Bezout's Identity. Suppose there exist $a, b, x, y \in \mathbb{Z}$ such that $ax + by = 1$ and let d be a common divisor of both a and b. It follows there exist $j, k \in \mathbb{Z}$ such that $a = dj$ and$b = dk$. Consequently, $djx + dky = 1$ which shows $d(jx + ky) = 1$. Thus $d = 1$ and we find $gcd(a, b) = 1$. □

Another nice application of Bezout's identity is seen in *Euclid's Lemma*: intuitively, Euclid's Lemma testifies to the indestructibly of primes.

Lemma 6.3.17. (Euclid)*: Let* $a, b \in \mathbb{Z}$. *If* $p \in \mathbb{Z}$ *is prime and* $p \mid ab$ *then* $p \mid a$ *or* $p \mid b$.

Proof: Suppose $a, b, p \in \mathbb{Z}$ and p is prime. Further, suppose $p \mid ab$ but $p \nmid a$. Since p does not divide a we have $\gcd(a, p) = 1$ and by Bezout's identity there exist $x, y \in \mathbb{Z}$ for which $ax + py = 1$. Multiply by b to obtain $bax + bpy = b$ (label this by $\star$. Since $p \mid ab$ we know there exists $c \in \mathbb{Z}$ for which $ab = cp$. Hence, returning to $\star$,

$$b = cpx + bpy = p(cx + by)$$

since $cx + by \in \mathbb{Z}$ the result above clearly shows $p \mid b$ and Euclid's Lemma follows. □

6.4 modular arithmetic

In this section we assume $n \in \mathbb{N}$ throughout. In summary, we develop a careful model for $\mathbb{Z}_n$ in this section.

Remark 6.4.1. I use some notation in this section which we can omit elsewhere for the sake of brevity. In particular, in the middle of this section I might use the notation $[2]$ or $\bar{2}$ or $[2]_n$ for $2 \in \mathbb{Z}_n$ whereas in later work we simply use 2 with the understanding that we are working in the context of modular arithmetic.

Definition 6.4.2. *$a \equiv b$ $mod(n)$ if and only if $n \mid (b-a)$.*

The definition above is made convenient by the simple equivalent criteria below:

Theorem 6.4.3. *Let $a, b \in \mathbb{Z}$ then we say a is* **congruent** *to b $mod(n)$ and write $a \equiv b$ $mod(n)$ if a and b have the same remainder when divided by n.*

Proof: Suppose $a \equiv b$ $mod(n)$ then a and b share the same remainder after division by n. By the Division Algorithm, there exist $q_1, q_2 \in \mathbb{Z}$ for which $a = q_1 n + r$ and $b = q_2 n + r$. Observe, $b - a = (q_2 n + r) - (q_1 n + r) = (q_2 - q_1)n$. Therefore, $n \mid (b-a)$.

Conversely, suppose $n \mid (b-a)$ then there exists $q \in \mathbb{Z}$ for which $b - a = qn$. Apply the Division Algorithm to find q_1, q_2 and r_1, r_2 such that: $a = q_1 n + r_1$ and $b = q_2 n + r_2$ with $0 \leq r_1 < n$ and $0 \leq r_2 < n$. We should pause to note $|r_2 - r_1| < n$. Observe,

$$b - a = qn = (q_2 n + r_2) - (q_1 n + r_1) = (q_2 - q_1)n + r_2 - r_1.$$

Therefore, solving for the difference of the remainders and taking the absolute value,

$$|q - q_2 + q_1|n = |r_2 - r_1|$$

Notice $|q - q_2 + q_1| \in \mathbb{N} \cup \{0\}$ and $|r_2 - r_1| < n$. It follows $|q - q_2 + q_1| = 0$ hence $|r_2 - r_1| = 0$ and we conclude $r_1 = r_2$. □

Congruence has properties you might have failed to notice as a child.

Proposition 6.4.4. *Let n be a positive integer, for all $x, y, z \in \mathbb{Z}$,*

(i.) *$x \equiv x$ $mod(n)$,*

(ii.) *$x \equiv y$ $mod(n)$ implies $y \equiv x$ $mod(n)$,*

(iii.) *if $x \equiv y$ $mod(n)$ and $y \equiv z$ $mod(n)$ then $x \equiv z$ $mod(n)$.*

Proof: we use Definition 6.4.2 throughout what follows.
(i.) Let $x \in \mathbb{Z}$ then $x - x = 0 = 0 \cdot n$ hence $n \mid (x - x)$ and we find $x \equiv x$ $mod(n)$.
(ii.) Suppose $x \equiv y$ $mod(n)$. Observe $n \mid (x - y)$ indicates $x - y = nk$ for some $k \in \mathbb{Z}$. Hence $y - x = n(-k)$ where $-k \in \mathbb{Z}$. Therefore, $n \mid (y - x)$ and we find $y \equiv x$ $mod(n)$.
(iii.) Suppose $x \equiv y$ $mod(n)$ and $y \equiv z$ $mod(n)$. Thus $n \mid (y - x)$ and $n \mid z - y$. Corollary 6.3.5 indicates n also divides the sum of two integers which are each divisible by n. Thus, $n \mid [(y - x) + (z - y)]$ hence $n \mid (z - x)$ which shows $x \equiv z$ $mod(n)$. □

I referenced the Corollary to prove part (iii.) to remind you how our current discussion fits naturally with our previous discussion.

Corollary 6.4.5. *Let $n \in \mathbb{N}$. Congruence modulo n forms an equivalence relation on $\mathbb{Z}$.*

This immediately informs us of an interesting **partition** of the integers. Recall, a **partition** of a set S is a family of subsets $U_\alpha \subseteq S$ where $\alpha \in \Lambda$ is some index set such that $U_\alpha \cap U_\beta = \emptyset$ for $\alpha \neq \beta$ and $\cup_{\alpha \in \Lambda} U_\alpha = S$. A partition takes a set and parses it into disjoint pieces which cover the whole set. The partition induced from an equivalence relation is simply formed by the **equivalence classes** of the relation. Let me focus on $\mathbb{Z}$ with the equivalence relation of congruence modulo a positive integer n. We define:[5]:

Definition 6.4.6. equivalence classes of $\mathbb{Z}$ modulo $n \in \mathbb{N}$:

$$[x] = \{y \in \mathbb{Z} \mid y \equiv x \ mod(n)\}$$

Observe, there are several ways to characterize such sets:

$$[x] = \{y \in \mathbb{Z} \mid y \equiv x \ mod(n)\} = \{y \in \mathbb{Z} \mid y - x = nk \text{ for some } k \in \mathbb{Z}\} = \{x + nk \mid k \in \mathbb{Z}\}.$$

I find the last presentation of $[x]$ to be useful in practical computations.

Example 6.4.7. *Congruence $mod(2)$ partititions $\mathbb{Z}$ into even and odd integers:*

$$[0] = \{2k \mid k \in \mathbb{Z}\} \qquad \& \qquad [1] = \{2k+1 \mid k \in \mathbb{Z}\}$$

Example 6.4.8. *Congruence $mod(4)$ partititions $\mathbb{Z}$ into four classes of numbers:*

$$[0] = \{4k \mid k \in \mathbb{Z}\} = \{\dots, -8, -4, 0, 4, 8, \dots\}$$

$$[1] = \{4k+1 \mid k \in \mathbb{Z}\} = \{\dots, -7, -3, 1, 5, 9, \dots\}$$
$$[2] = \{4k+2 \mid k \in \mathbb{Z}\} = \{\dots, -6, -2, 2, 6, 10, \dots\}$$
$$[3] = \{4k+3 \mid k \in \mathbb{Z}\} = \{\dots, -5, -1, 3, 7, 11, \dots\}$$

The patterns above are interesting, there is something special about [0] and [2] in comparison to [1] and [3]. Patterns aside, the notation of the previous two example can be improved. Let me share a natural notation which helps us understand the structure of congruence classes.

Definition 6.4.9. Coset Notation: *Let $n \in \mathbb{N}$ and $a \in \mathbb{Z}$ we define:*

$$n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\} \qquad a + n\mathbb{Z} = \{a + nk \mid k \in \mathbb{Z}\}.$$

Observe, in the notation just introduced, we have

$$\boxed{[a] = a + n\mathbb{Z}}$$

Example 6.4.10. *Congruence $mod(2)$ partititions $\mathbb{Z}$ into even and odd integers:*

$$[0] = 2\mathbb{Z} \qquad \& \qquad [1] = 1 + 2\mathbb{Z}.$$

Example 6.4.11. *Congruence $mod(4)$ partititions $\mathbb{Z}$ into four classes of numbers:*

$$[0] = 4\mathbb{Z}, \quad [1] = 1 + 4\mathbb{Z}, \quad [2] = 2 + 4\mathbb{Z}, \quad [3] = 3 + 4\mathbb{Z}.$$

[5] there are other notations, the concept here is far more important than the notation we currently employ

We should pause to appreciate a subtle aspect of the notation. It is crucial to note $[x] = [y]$ does **not** imply $x = y$. For example, modulo 2:

$$[1] = [3] = [7] = [100003755038598798798797 1] \qquad \& \qquad [2] = [-2] = [-42].$$

Or, modulo 9:

$$[1] = [10] = [-8], \qquad \& \qquad [3] = [12] = [-6], \qquad \& \qquad [0] = [90] = [-9].$$

Yet, modulo 9, $[1] \neq [3]$. Of course, I just said $[1] = [3]$. How can this be? Well, context matters. In some sense, the notation $[x]$ is dangerous and $[x]_n$ would be better. We could clarify that $[1]_2 = [3]_2$ whereas $[1]_9 \neq [3]_9$. I don't recall such notation used in any text. What is more common is to use the *coset notation* to clarify:

$$1 + 2\mathbb{Z} = 3 + 2\mathbb{Z} \qquad \text{whereas} \qquad 1 + 9\mathbb{Z} \neq 3 + 9\mathbb{Z}.$$

I'm not entirely sure the Proposition below is necessary.

Proposition 6.4.12. *Let $n \in \mathbb{N}$. We have $[x] = [y]$ if and only if $x \equiv y \ mod(n)$. Or, in the coset notation $x + n\mathbb{Z} = y + n\mathbb{Z}$ if and only if $y - x \in n\mathbb{Z}$.*

Proof: Observe $x \in [x]$. If $[x] = [y]$ then $x \in [y]$ hence there exists $k \in \mathbb{Z}$ for which $x = y + nk$ hence $x - y = nk$ and we find $x \equiv y \ mod(n)$. Conversely, if $x \equiv y \ mod(n)$ then there exists $k \in \mathbb{Z}$ such that $y - x = nk$ thus $x = y - nk$ and $y = x + nk$. Suppose $a \in [x]$ then there exists $j \in \mathbb{Z}$ for which $a = nj + x$ hence $a = nj + y - nk = n(j - k) + y \in [y]$. We have shown $[x] \subseteq [y]$. Likewise, if $b \in [y]$ then there exists $j \in \mathbb{Z}$ for which $b = nj + y$ hence $b = nj + x + nk = n(j + k) + x \in [x]$. Thus $[y] \subseteq [x]$ and we conclude $[x] = [y]$. □

Notice the proposition above allows us to calculate as follows: for $n \in \mathbb{N}$

$$na + b + n\mathbb{Z} = b + n\mathbb{Z} \qquad \text{or} \qquad [na + b] = [b]$$

for $a, b \in \mathbb{Z}$. There is more.

Proposition 6.4.13. *Let $n \in \mathbb{N}$. If $[x] = [x']$ and $[y] = [y']$ then*

(i.) $[x + y] = [x' + y']$,

(ii.) $[xy] = [x'y']$

(iii.) $[x - y] = [x' - y']$

Proof: Suppose $[x] = [x']$ and $[y] = [y']$. It follows there exists $j, k \in \mathbb{Z}$ such that $x' = nj + x$ and $y' = nk + y$. Notice $x' \pm y' = nj + x \pm (nk + y) = n(j \pm k) + x \pm y$. Therefore, $x \pm y \equiv x' \pm y' \ mod(n)$ and by Proposition 6.4.12 we find $[x \pm y] = [x' \pm y']$. This proves $(i.)$ and $(iii.)$. Next, consider:

$$x'y' = (nj + x)(nk + y) = n(jkn + jy + xk) + xy$$

thus $x'y' \equiv xy \ mod(n)$ we apply Proposition 6.4.12 once more to find $[xy] = [x'y']$. □

We ought to appreciate the content of the proposition above as it applies to congruence modulo n. In fact, the assertions below all apear in the proof above.

Corollary 6.4.14. *Let $n \in \mathbb{N}$. If $x \equiv x'$ and $y \equiv y'$ modulo n then*

(i.) $x + y \equiv x' + y'$ *mod*(n),

(ii.) $xy \equiv x'y'$ *mod*(n),

(iii.) $x - y \equiv x' - y'$ *mod*(n),

Example 6.4.15. *Suppose $x + y \equiv 3$ and $x - y \equiv 1$ modulo 4. Then, by Corollary 6.4.14 we add and substract the given congruences to obtain:*

$$2x \equiv 4 \qquad 2y \equiv 2$$

There are 4 cases to consider. Either $x \in [0]$, $x \in [1]$, $x \in [2]$ or $x \in [3]$. Observe,

$$\begin{array}{ll} 2(0) \equiv 0 \equiv 4, & 2(0) \not\equiv 2 \\ 2(1) \equiv 2 \not\equiv 4, & 2(1) \equiv 2 \\ 2(2) \equiv 4, & 2(2) \equiv 4 \not\equiv 2 \\ 2(3) \equiv 2 \not\equiv 4, & 2(3) \equiv 2. \end{array}$$

It follows that $x \in [0] \cup [2]$ and $y \in [1] \cup [3]$ forms the solution set of this system of congruences.

The method I used to solve the above example was not too hard since there were just 4 cases to consider. I suppose, if we wished to solve the same problem modulo 42 we probably would like to learn a better method.

Proposition 6.4.13 justifies that the definition below does give a **binary operation** on the set of equivalence classes modulo n. Recall, a *binary operation* on a set S is simply a *function* from $S \times S$ to S. It is a single-valued assignment of pairs of S-elements to S-elements.

Definition 6.4.16. modular arithmetic: *let $n \in \mathbb{N}$, define*

$$[x] + [y] = [x + y] \qquad \& \qquad [x][y] = [xy]$$

for all $x, y \in \mathbb{Z}$. Or, if we denote the set of all equivalence classes modulo n by $\mathbb{Z}/n\mathbb{Z}$ then write: for each $x + n\mathbb{Z}, y + n\mathbb{Z} \in \mathbb{Z}/n\mathbb{Z}$

$$(x + n\mathbb{Z}) + (y + n\mathbb{Z}) = x + y + n\mathbb{Z} \qquad \& \qquad (x + n\mathbb{Z})(y + n\mathbb{Z}) = xy + n\mathbb{Z}.$$

Finally, we often use the notation $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$.

Notice the operation defined above is a binary operation on $\mathbb{Z}/n\mathbb{Z}$ (not $\mathbb{Z}$). Many properties of integer arithmetic transfer to $\mathbb{Z}/n\mathbb{Z}$:

$$\begin{aligned} [a] + [b] &= [b] + [a] \\ [a][b] &= [b][a] \\ [a]([b] + [c]) &= [a][b] + [a][c] \\ ([a] + [b])[c] &= [a][c] + [b][c] \\ ([a] + [b]) + [c] &= [a] + ([b] + [c]) \\ ([a][b])[c] &= [a]([b][c]) \\ [a] + [0] &= [0] + [a] = [a] \\ [1][a] &= [a][1]. \end{aligned}$$

Furthermore, for $k \in \mathbb{N}$,

$$\begin{aligned}
[a_1] + [a_2] + \cdots + [a_k] &= [a_1 + a_2 + \cdots + a_k] \\
[a_1][a_2] \cdots [a_k] &= [a_1 a_2 \cdots a_k] \\
[a]^k &= [a^k].
\end{aligned}$$

Example 6.4.17. *Simplify* $[1234]$ *modulo* 5. *Notice,*

$$1234 = 1 \times 10^3 + 2 \times 10^2 + 3 \times 10 + 4.$$

However, $10 = 2(5)$ *thus,*

$$1234 = 1 \times 2^3 5^3 + 2 \times 2^2 5^2 + 3 \times 2 \cdot 5 + 4.$$

Note, $[5] = [0]$ *hence* $[5^k] = [0]$ *for* $k \in \mathbb{N}$. *By the properties of modular arithmetic it is clear that the* $10's$, $100's$ *and* $1000's$ *digits are irrelevant to the result. Only the first digit matters,* $[1234] = [4]$.

It is not hard to see the result of the example above equally well applies to larger numbers; if $a_k, \ a_{k-1}, \ldots, a_2, a_1$ are the digits in a decimal representation of an integer then $[a_k a_{k-1} \cdots a_2 a_1] = [a_1] \ mod(5)$.

Example 6.4.18. *Calculate the cube of* 51 *modulo* 7.

$$[51^3] = [51][51][51] = [51]^3 = [49 + 2]^3 = [2]^3 = [8].$$

Of course, you can also denote the same calculation via congruence:

$$51^3 = 51 \cdot 51 \cdot 51 \equiv 2 \cdot 2 \cdot 2 = 8 \quad \Rightarrow \quad [51^3] = [8].$$

The next example is a cautionary tale:

Example 6.4.19. *Simplify* 7^{100} *modulo* 6. *Consider,*

$$[7^{100}] = [7]^{100} = [1]^{100} = [1^{100}] = [1].$$

or, (incorrectly !)

$$[7^{100}] = [7^{[100]}] = [7^{[6(16)+4]}] = [7^4] = [28] = [4].$$

The point is this: it is **not** *true that* $[a^k] = [a^{[k]}]$.

Naturally, as we discuss $\mathbb{Z}_n$ it is convenient to have a particular choice of representative for this set of residues. Two main choices: the *set of least non-negative residues*

$$\mathbb{Z}_n = \{[0], [1], [2], \ldots, [n-1]\}$$

alternatively, *set of least absolute value residues* or simply *least absolute residues*

$$\mathbb{Z}_n = \{[0], [\pm 1], [\pm 2], \ldots\}$$

where the details depend on if n is even or odd. For example,

$$\mathbb{Z}_5 = \{[0], [1], [2], [3], [4]\} = \{[-2], [-1], [0], [1], [2]\}$$

or,

$$\mathbb{Z}_4 = \{[0], [1], [2], [3]\} = \{[-2], [-1], [0], [1]\}$$

Honestly, if we work in the particular context of $\mathbb{Z}_n$ then there is not much harm in dropping the $[\cdot]$-notation. Sometimes, I use $[x] = \bar{x}$. Whichever notation we choose, we must be careful to not fall into the trap of assuming the usual properties of $\mathbb{Z}$ when calculating in the specific context of modular arithmetic. The example that follows would be very clumsy to write in the $[\cdot]$-notation.

Example 6.4.20. *Consider $f(x) = x^2 + 2x + 3$ for $x \in \mathbb{Z}_5$. We can determine if f has a zero by explicit calculation modulo 5:*

$$f(-2) = (-2)^2 + 2(-2) + 3 = 3$$

$$f(-1) = (-1)^2 + 2(-1) + 3 = 2$$

$$f(0) = (0)^2 + 2(0) + 1 = 3$$

$$f(1) = 1 + 2 + 3 \equiv 1$$

$$f(2) = 4 + 4 + 3 \equiv 1$$

Therefore, $f(x)$ has no zero for $x \in \mathbb{Z}_5$.

The examples below are from Jones and Jones' *Elementary Number Theory* pages 42-43.

Example 6.4.21. *Calculate the least positive residue of 28×33 modulo 35. Note that $28 \equiv 28-35 = -7$ and $33 \equiv 33-35 = -2$ hence $28 \times 33 \equiv (-7) \times (-2) = 14$. Or, $[28][33] = [14]$.*

Example 6.4.22. *Calculate the least absolute residue of 15×59 mod(75). Observe $59 \equiv 59-75 = -16$ thus*

$$59 \times 15 \equiv -16 \times 15 = (-1-15) \times 15 = -15 - 3(75) \equiv -15.$$

Since $|-15| = 15 \leq 75/2$ it is clear -15 is the least absolute residue modulo 75.

Example 6.4.23. *To calculate 3^8 modulo 13 we break the problem into several doublings; $3^8 = ((3^2)^2)^2$. At each stage we take care to use modular arithmetic to simplify:*

$$3^2 = 9 \equiv -4$$

modulo 13. Next,

$$3^4 = (3^2)^2 \equiv (-4)^2 = 16 \equiv 3$$

thus

$$3^8 = (3^4)^2 \equiv 3^2 = 9.$$

Example 6.4.24. *Prove that $a(a+1)(a+2)$ is divisible by 6 for each integer a. In other words, we wish to show $a(a+1)(a+2) \equiv 0$ mod(6). Note $\mathbb{Z}_6 = \{[0], [\pm1], [\pm2], [3]\}$ so consider:*

$$\begin{aligned}
a = 0 : &\quad a(a+1)(a+2) = 0, \\
a = \pm1 : &\quad a(a+1)(a+2) = (\pm1)(1\pm1)(2\pm1) = \{6, 0\} \equiv 0, \\
a = \pm2 : &\quad a(a+1)(a+2) = (\pm2)(1\pm2)(2\pm2) = \{12, 0\} \equiv 0, \\
a = 3 : &\quad a(a+1)(a+2) = (3)(3+1)(3+2) = 60 \equiv 0.
\end{aligned}$$

Therefore, $a(a+1)(a+2) \equiv 0$ modulo 6 for all $a \in \mathbb{Z}$ hence $6 \mid a(a+1)(a+2)$ for all $a \in \mathbb{Z}$.

The claim in the example above is very obviously true if we just think about some cases $1\cdot2\cdot3$,$2\cdot3\cdot4$,...$10\cdot11\cdot12$, $11\cdot12\cdot13$ etc. You can see the reason a 6 appears is that in any triple of successive integers you have at least one number divisible by 3 and at least one number divisible by 2. This suggests a different method of proof.

Example 6.4.25. *Prove that $a(a+1)(a+2)$ is divisible by 6 for each integer a. Once again, we wish to show $a(a+1)(a+2) \equiv 0 \ mod(6)$. Observe, if $2 \mid x$ and $3 \mid x$ then $x = 2j$ and $x = 3k$ for some $j, k \in \mathbb{Z}$. It follows from the prime factorization of integers that $3 \mid j$ and $2 \mid k$ hence*[6] *there exists $m \in \mathbb{Z}$ for which $j = 3m$ and we find $x = 2j = 2(3m) = 6m$ which proves $6 \mid x$. Therefore, if we are able to show $a(a+1)(a+2)$ is divisible by 2 and 3 it follows $a(a+1)(a+2)$ is divisible by 6. Consider congruence modulo 2:*

$$\begin{aligned} a = 0: &\qquad a(a+1)(a+2) = 0, \\ a = 1: &\qquad a(a+1)(a+2) = (1)(2)(3) \equiv 0. \end{aligned}$$

Next, the modulo 3 case:

$$\begin{aligned} a = 0: &\qquad a(a+1)(a+2) = 0, \\ a = 1: &\qquad a(a+1)(a+2) = (1)(2)(3) \equiv 0, \\ a = 2: &\qquad a(a+1)(a+2) = (2)(3)(4) \equiv 0. \end{aligned}$$

Thus $a(a+1)(a+2) \equiv 0$ modulo 6 and we conclude $6 \mid a(a+1)(a+2)$ for each $a \in \mathbb{Z}$.

Notice I had to invoke the Fundalmental Theorem of Arithmetic in the example above. Let me state it without proof here:

Theorem 6.4.26. *Let $n \in \mathbb{N}$ then there exist a unique set of distinct primes $p_1, p_2, \dots, p_k$ and multiplicities $r_1, r_2, \dots, r_k$ for which $n = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}$.*

Proof: to be found in Math 307 (the number theory course). □

We already saw a specific case of the theorem below in action to solve Example 6.4.25.

Theorem 6.4.27. *Let $n \in \mathbb{N}$ such that there exist a unique set of distinct primes $p_1, p_2, \dots, p_k$ and multiplicities $r_1, r_2, \dots, r_k$ for which $n = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}$. Then $a \equiv b \ mod(n)$ if and only if $a \equiv b \ mod(p_i^{r_i})$ for each $i = 1, 2, \dots k$.*

Proof: to be found in Math 307(the number theory course). □

The theme of this section is illustrate the structure and utility of modular arithmetic. The Theorem below is certainly a showcase of the technique. The problem of determining if $f(x) = 0$ for some $x \in \mathbb{Z}$ is somewhat daunting as there are infinitely many integers. However, for polynomial $f(x)$ we are able to answer this question by analyzing the corresponding polynomial over $\mathbb{Z}_n$.

Theorem 6.4.28. *Let $f(x) \in \mathbb{Z}[x]$, that is let $f(x)$ be a polynomial with integer coefficients, and suppose $n \in \mathbb{N}$. If $a \equiv b \ mod(n)$ then $f(a) \equiv f(b) \ mod(n)$.*

Proof: Suppose $a \equiv b \ mod(n)$ and $f(x) = c_m x^m + \cdots + c_1 x + c_0$ where $c_m, \dots, c_1, c_0 \in \mathbb{Z}$. Consider then, by repeated application of Corollary 6.4.14 we have:

$$f(a) = c_m a^m + \cdots + c_1 a + c_0 \equiv c_m b^m + \cdots + c_1 b + c_0 = f(b). \quad \square$$

Logically, if there exists an $n \in \mathbb{N}$ for which there is no solution of the congruence $f(x) \equiv 0 \ mod(n)$ then it follows there cannot exist a solution of $f(x) = 0$ where $x \in \mathbb{Z}$. Here is a practical application of this theorem to a specific polynomial:

[6] yes, I could just as well have messed with k

Example 6.4.29. *Show $f(x) = x^5 - x^2 + x - 3$ has no integer roots. Consider, modulo 4,*

$$f(0) = -3, \qquad f(1) = 1 - 1 + 1 - 3 = -2,$$

$$f(-1) = -1 - 1 - 1 - 3 = -6 \equiv 2, \qquad f(2) = 32 - 4 + 2 - 3 \equiv -1.$$

This means there is no integer for which $f(x) = 0$. Why? Because $\mathbb{Z} = 4\mathbb{Z} \cup (4\mathbb{Z}+1) \cup (4\mathbb{Z}+2) \cup (4\mathbb{Z}+3)$ and we have shown each partition gives no value in $4\mathbb{Z}$ hence no integer input into $f(x)$ returns a value of 0.

This method is not generally successful in proving the non-existence of integer zeros for polynomials over the integers. See page 45 of Jones and Jones' *Elementary Number Theory* for comments[7].

There is a large difference between ordinary arithmetic in $\mathbb{Z}$ and that of $\mathbb{Z}_n$. We already saw in Example 6.4.15 the solution set of a system of equations in $\mathbb{Z}_4$ had four distinct solutions. In the context of systems of equations over $\mathbb{Z}$ we either obtain no solutions, one solution, or infinitely many. This distinction is largely tied to the fact that some numbers in $\mathbb{Z}_n$ do not have multiplicative inverses. For example, in $\mathbb{Z}_4$ the fact that $[2][2] = [0]$ implies there cannot be $[x]$ such that $[2][x] = [1]$ since that would give us $[2][2][x] = [0][x]$ implying $[2][1] = [2] = [0]$ which is absurd. Apparently, only certain numbers in $\mathbb{Z}_n$ have multiplicative inverses. Let us characterize which numbers have inverses modulo n. Let $n \in \mathbb{N}$ and $a \in \mathbb{Z}$ we seek to solve:

$$[a][x] = [1] \quad \Rightarrow \quad ax - 1 = nk$$

for some $k \in \mathbb{Z}$. This gives,

$$ax + nk = 1$$

If a and n have a common factor larger than 1 then we obtain a contradiction since 1 has no divisors. Thus, in the case there is a solution, we must have $gcd(a, n) = 1$. This is fortunate news since we have a nice method to calculate $gcd(a, n)$ and the criteria that a^{-1} exist in $\mathbb{Z}_n$ is simply that a is **relatively prime** or, if you prefer, **coprime**.

Example 6.4.30. *In Example 6.3.12 we found $gcd(62, 626) = 2$. This shows 62 does not have a multiplicative inverse modulo 626. Also, it shows 626 does not have a multiplicative inverse modulo 62.*

Example 6.4.31. *In Example 6.3.13 we found $gcd(11, 240) = 1$ and $1 = -109(11) + 5(240)$. From this we may read several things:*

$$[-109]^{-1} = [11]\ mod(240) \qquad \& \qquad [-109]^{-1} = [11]\ mod(5)$$

and,

$$[5]^{-1} = [240]\ mod(11) \qquad \& \qquad [5]^{-1} = [240]\ mod(109).$$

In terms of least positive residues the last statement reduces to $[5]^{-1} = [22]$. Of course, we can check this; $[5][22] = [110] = [1]$.

Remark 6.4.32. At this point our work on the model $\mathbb{Z}/n\mathbb{Z}$ for $\mathbb{Z}_n$ comes to an end. From this point forward, we return to the less burdensome notation

$$\mathbb{Z}_n = \{0, 1, 2, \dots, n-1\}$$

as a default. Just beware $k = k - n$ in $\mathbb{Z}_n$. Thus, $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\} = \{0, \pm 1, \pm 2\}$ as $-1 = 4$ and $-2 = 3$ in $\mathbb{Z}_5$. It is sometimes very helpful to use the $\pm$ formulation of $\mathbb{Z}_n$.

[7] give me a warning via email if you want to look at this book, I might need to grab it from home

Example 6.4.33. *The addition and multiplication and addition for $\mathbb{Z}_2$ can be written in tabular form as follows: (denoting $\overline{0}$ by 0 and $\overline{1}$ by 1 since there is no danger of confusion here)*

$+_2$	0	1
0	0	1
1	1	0

$\cdot_2$	0	1
0	0	0
1	0	1

Example 6.4.34. *The addition and multiplication and addition in $\mathbb{Z}_3$ is given by:*

$+_3$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\cdot_3$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

Example 6.4.35. *The addition and multiplication and addition in $\mathbb{Z}_4$ can be written in tabular form as follows:*

$+_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\cdot_4$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Example 6.4.36. *The addition and multiplication and addition in $\mathbb{Z}_5$ can be written in tabular form as follows:*

$+_5$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$\cdot_5$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Example 6.4.37. *The addition and multiplication and addition in $\mathbb{Z}_6$ can be written in tabular form as follows:*

$+_6$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

$\cdot_6$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Example 6.4.38. *The addition and multiplication and addition in $\mathbb{Z}_7$ can be written in tabular form as follows:*

$+_7$	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

$\cdot_7$	0	1	2	3	4	5	6
0	0	0	0	0	0	0	6
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

Remark 6.4.39. *It is of course fine to write in-between steps in $\mathbb{Z}$ where it is easier to calculate sometimes. For example, in $\mathbb{Z}_5$,*

$$4^2 + 3 = 16 + 3 = 19 = \boxed{4}$$

It wouldn't be best to leave the answer as 19. In $\mathbb{Z}_5$ we ought to leave the answer as $0, 1, 2, 3$ or 4. Also sometimes it pays it simplify as you go along, again in $\mathbb{Z}_5$ I calculate,

$$4^{20} = (4^2)^{10} = (16)^{10} = 1^{10} = \boxed{1}.$$

Obviously calculating 4^{20} directly then simplifying would have been a much harder calculation.

Example 6.4.40. *Find solutions(if possible) of $x^2 + 1 = 0$ in $\mathbb{Z}_2$. Notice that in $\mathbb{Z}_2$ we have that $2 = 0$ thus $2x = 0$. Consequently, $x^2 + 1 = x^2 + 2x + 1 = (x + 1)^2 = 0$. This has solution $x = -1$ which is otherwise known as $x = 1$ in $\mathbb{Z}_2$. To summarize, the quadratic equation $x^2 + 1 = 0$ has just the $x = 1$ solution in $\mathbb{Z}_2$.*

When we try to solve polynomial equations over $\mathbb{Z}_n$ things get weird generally speaking.

Example 6.4.41. *Does the polynomial $f(x) = x^3 + 3x^2 + 7$ have any solutions in $\mathbb{Z}_6$? Well, one solution is just to check all the possiblilities:*

$$\begin{aligned}
&f(0) = 7\\
&f(1) = 1 + 3 + 7 = 10 = 4\\
&f(2) = 8 + 3(4) + 7 = 27 = 3\\
&f(3) = 27 + 3(9) + 7 = 3 + 3 + 7 = 13 = 1\\
&f(4) = 4^3 + 3(16) + 7 = (-2)^3 + 3(4) + 7 = -8 + 12 + 1 = 5\\
&f(5) = 5^3 + 3(25) + 7 = (-1)^3 + 3(1) + 1 = 3
\end{aligned}$$

I have made extensive use of identities such as $x = x - 6$ in $\mathbb{Z}_6$. For example, I noted $5 = -1$ and $4 = -2$ to simplify the calculation of $f(4)$ and $f(5)$. We conclude that $f(x)$ has no solutions in $\mathbb{Z}_6$.

Chapter 7

Functions

Functions have found a place in the mathematical lexicon for a few centuries at this time. However, the modern viewpoint of a function is only about a century old. As recently as the mid-nineteenth century mathematicians still had not quite refined the concept of a function. What precisely is a function? How is a function described? In this chapter we take the viewpoint that a function is a special type of relation. This is equivalent to identifying a function with its graph. In practice, this viewpoint is usually adopted but almost never does one think of a function as a subset of a Cartesian product. Instead, we typically envision a function as a rule connecting two sets. In other words, we usually think of a function as a map between two sets.

7.1 domain, range and codomain

Words, words, words, so many words.

Definition 7.1.1. *A* **function** *from A to B is a relation f from A to B such that*

(i.) *$dom(f) = A$*

(ii.) *for each $x \in A$, xfy and xfz implies $y = z$.*

We write $f : A \to B$ to indicate that the function f has **domain** *A and* **codomain** *B. When $A = B$ we say that $f : A \to A$ is a function on A. We also say that $f : A \to B$ is a "B-valued function of A".*

From this point forward, we will exchange the relation notation of xfy for the more familiar notation $f(x) = y$. (this is unambiguous because of ii.)

Definition 7.1.2. *If $f(x) = y$ then we say that x is an* **argument** *of the function and y is a* **value** *of the function. We also say that if $y = f(x)$ then x is a* **preimage** *of x.*

Let $f : A \to B$. Given $x \in dom(f)$ the value $f(x)$ is uniquely prescribed. In contrast, for a given $y \in B$ there can be many preimages x such that $f(x) = y$.

Example 7.1.3. *Let $f = \{(x, y) \mid x \in \mathbb{R},\ y = x^2\}$. Notice this is a function from $\mathbb{R}$ to $\mathbb{R}$ and we can write $f(x) = x^2$. The preimages of 3 are $\pm\sqrt{3}$ since $f(\pm\sqrt{3}) = (\pm\sqrt{3})^2 = 3$.*

Definition 7.1.4. *For a function $f : A \to B$ we define,*

(i.) *for $U \subseteq A$, $f(U) = \{y \in B \mid y = f(x) \text{ for some } x \in U\}$*

(ii.) *for $V \subseteq B$, $f^{-1}(V) = \{x \in A \mid f(v) = x$ for some $v \in V\}$*

The fiber and range are special cases of the definition above.

Definition 7.1.5. *The set of all preimages of y is called the* **fiber** *of f over y*

$$f^{-1}(\{y\}) = \{x \in dom(f) \mid f(x) = y\}.$$

The **range** *of f is*

$$range(f) = \{y \mid \exists x \in dom(f) \text{ with } f(x) = y\}$$

I think that about covers it for now. Let's look at a few examples.

Example 7.1.6. *Let $f \subseteq \mathbb{R} \times \mathbb{R}$ be the relation defined by*

$$f = \{(x, 2x^2) \mid x \in [-1, 1]\}$$

This is not a function on $\mathbb{R}$ because it is not well-defined in the following sense: $f(2)$ has no value. Notice we were only given $f(x) = 2x^2$ for $x \in [-1, 1]$. Is f is a function on $[-1, 1]$? No, $f(1) = 2 \notin [-1, 1]$. Remember to say "f is a function on $[-1, 1]$" we need $f : [-1, 1] \to [-1, 1]$. Observe that $f : [-1, 1] \to \mathbb{R}$ is a function. Note, for each input $x \in [-1, 1]$, f outputs the real number x^2. Moreover, you can calculate

$$f([-1, 1]) = [0, 2] = range(f)$$

and while we're at it

$$f^{-1}(\{2\}) = \{1, -1\}.$$

You should know from your prerequisite precalculus knowledge that $f(x) = 2x^2$ has a graph which is a parabola and as such it fails the horizontal line test. The notation $f^{-1}(\{2\})$ does not indicate that f^{-1} is a function. In the present example it is only a relation since $f^{-1}(2) = 1$ and $f^{-1}(2) = -1$. Some people would call such a rule a "double valued" function, we will not use such terminology.

Remark 7.1.7. *The terminology "f is a function* **of** *A" simply means that $dom(f) = A$. In contrast, the terminology "f is a function* **on** *A" means that $dom(f) = A$ and $codomain(f) = A$.*

Example 7.1.8. *Let $f(x) = \frac{x-1}{x-1}$.* **Find the largest domain for which the formula makes sense**. *Observe that if $x \neq 1$ then $f(x)$ is well-defined since $x - 1 \neq 0$. However, if $x = 1$ then the formula for the function is ill-defined. Hence, $dom(f) = \mathbb{R} - \{1\} = (-\infty, 1) \cup (1, \infty)$. The graph of this function is the horizontal line $y = 1$ with a hole at $x = 1$.*

Often a function's domain is not specified in certain contexts. It is customary to take the largest subset of inputs for which the defining formula is well-defined. For typical examples this simply means that we must avoid division by zero or negative inputs to logarithms or even-indiced radical functions. In general the import of the term *well-defined* has many facets.

Given a set S and an equivalence relation R we can construct the set of equivalence classes S/R (which is read "S modulo R" or simply "S mod R"). A typical element of S/R is an equivalence class $[x] = \{s \in S \mid sRx\}$. If $f : S/R \to B$ is to be a function then the rule for the function must be given in such a way that the formula is independent of the representatives. If $f([x]) = g(x)$ for some function $g : S \to B$ then it must be shown that $g(x) = g(y)$ for any other $y \in [x]$. In other words, g must be constant over the equivalence classes of R.

Example 7.1.9. *Let $S = \mathbb{R}^2$ and let $\sim$ be the equivalence relation defined by $(x, y) \sim (a, b)$ iff $x^2 + y^2 = a^2 + b^2$. Notice that the equivalence relation $\sim$ partitions the plane into circles about the origin and the origin itself. Let us denote the equivalence classes by $[(x, y)] = \{(a, b) \in \mathbb{R}^2 \mid x^2+y^2 = a^2 + b^2\}$. Does the following formula decribe a function from $S/\sim$ to $\mathbb{R}$?*

$$f([(x, y)]) = x - y$$

Clearly $x - y \in \mathbb{R}$ is defined for all $x, y \in \mathbb{R}$ and it is obviously a real number. However, this is not a function because if we took a different representative of $[(x, y)]$ we would not get the same output. When giving a counter-example, it is best to give a specific counter-example. Notice $[(1, 0)] = [(0, 1)] = \{(a, b) \in \mathbb{R}^2 \mid a^2 + b^2 = 1\}$ however

$$f([(1, 0)]) = 1 - 0 \neq 0 - 1 = f([(0, 1)])$$

Thus the same equivalence class makes f output two different outputs. This means that f is not a function. We say that f is not "well-defined" when this happens. In contrast,

$$g([(x, y)]) = \sin(\sqrt{x^2 + y^2}) + 3$$

gives a well defined function since if $[(a, b)] = [(x, y)]$ then $a^2 + b^2 = x^2 + y^2$ and consequently, $g([(x, y)]) = g([(a, b)])$.

Example 7.1.10. *Let A, B be sets. Then $\pi_A(a, b) = a$ is a function from $A \times B$ to A called the projection onto A. Likewise, $\pi_B(a, b) = b$ defines π_B the projection from $A \times B$ to B. The fiber of $b \in B$ with respect to π_B is $A \times \{b\}$ since*

$$\pi_B(A \times \{b\}) = b$$

Let A be the unit circle and $B = [0, 1]$ then you can visualize $A \times B$ as the unit-cylinder. The "fiber" of a point $p \in [0, 1]$ on the unit interval is circle at the point p.

Example 7.1.11. *(identity relation on A is a function on A) Let A be a set. The identity relation on A is defined as follows:*

$$I_A = \{(a, a) \mid a \in A\}$$

Observe that $I_A(x) = x$ for each $x \in A$ is a well-defined formula for the function $I_A : A \to A$. Moreover, $dom(I_A) = range(I_A) = A$.

7.2 constructing new functions

Given several functions there are numerous ways to construct new functions by combining the given functions through addition, mulitplication, difference, composition, extension, restriction and so forth... At the heart of each construction is the following basic theorem:

Theorem 7.2.1. *Two functions f and g are equal iff*

(i.) $dom(f) = dom(g)$

(ii.) $f(x) = g(x)$ for each $x \in dom(f)$.

Proof: Since the value of the function follows uniquely from the argument it follows immediately that x is in the first component of the ordered pair with $f(x)$ in the second slot. Hence $(x, f(x)) \in f$ viewed as a relation. Of course the same is true for g, thus $(x, g(x)) \in g$. Thus, since $f(x) = g(x)$ for each $x \in dom(f)$, $(x, g(x)) \in f$. It follows that $f = g$ since they share all the same elements. □

Example 7.2.2. *Let f, g be functions such that $dom(f) = dom(g)$ and $range(f), range(g) \subseteq \mathbb{R}$. The functions $f+g$, fg, f/g are all defined point-wise: $(f+g)(x) = f(x)+g(x)$, $(fg)(x) = f(x)g(x)$ and $(f/g)(x) = f(x)/g(x)$. The domains of the new functions are $dom(f+g) = dom(fg) = dom(f)$ and $dom(f/g) = \{x \in dom(f) \mid g(x) \neq 0\}$.*

Recall that we defined the composite and inverse of relations in as much was possible. Since functions are a special type of relation we can likewise discuss inverses and composites of functions. However, there is no gaurantee that the inverse of a function will itself be a function.

Theorem 7.2.3. *Let A, B, C be sets and F, G be functions such that $F : A \to B$ and $G : B \to C$. Then $G \circ F$ is a function from A to C with $dom(G \circ F) = A$.*

Proof: Let $x \in A$ then $F(x) \in B$ since $F : A \to B$. Thus $F(x) \in dom(G)$ and $G(F(x)) \in C$ since $G : B \to C$. Hence $dom(G \circ F)$. Notice that $G \circ F$ is single valued since F is single valued at $x \in A$ and G is single valued at $F(x) \in B$. *If you don't find that convincing take a look at the text's verbose proof which is mainly about showing that the output of the composite is single-valued.* □

Remark 7.2.4 (how to find composite of two functions generally)**.** *Often when we compose two functions the range of the inside function will not match the domain of the outside function. In fact, usually we will need to place two restrictions on the domain of $f \circ g$ for $f : B \to C$ and $g : A \to B$. If you think about it we can define $f \circ g$ only for a certain restriction of g. We need two things for $f(g(x))$ to be a sensible formula:*

(1.) $x \in dom(g)$,

(2.) $g(x) \in dom(f)$.

This means that we choose $dom(f \circ g) = dom(g) \cap g^{-1}(dom(f))$. The definition of composite we gave in this section assumes that the given functions have domains and ranges which match up nicely to start with, often this is not the case.

Example 7.2.5. *Given $f(x) = \sqrt{x}$ and $g(x) = x - 2$ find $f \circ g$ and determine the domain of the composite function. Observe that,*

$$(f \circ g)(x) = f(g(x)) = f(x - 2) = \sqrt{x - 2}$$

Here $range(g) = \mathbb{R}$ and $dom(g) = \mathbb{R}$. However, $dom(f) = [0, \infty)$ and you can see that $g^{-1}([0, \infty)) = \{x \in \mathbb{R} \mid x - 2 \geq 0\} = [2, \infty)$. Therefore, $dom(f \circ g) = [2, \infty)$

If you had simply examined the formula for the composite then you would probably have concluded the same domain. However, be careful, formulas can be deceiving, especially if we do any simplifications.

Example 7.2.6. *Given $f(x) = x^2$ and $g(x) = \sqrt{x}$ find $f \circ g$ and determine the domain of the composite function. Observe that,*

$$(f \circ g)(x) = f(g(x)) = f(\sqrt{x}) = (\sqrt{x})^2 = x$$

Here $range(g) = [0, \infty)$ and $dom(g) = [0, \infty)$, this limits the domain of the composite. However, notice $dom(f) = \mathbb{R}$ imposes no restriction in this example. Therefore, $dom(f \circ g) = [0, \infty)$. If you just look at the formula $(f \circ g)(x) = x$ you might be tempted to say that the domain is all of $\mathbb{R}$ (which would be incorrect!)

Theorem 7.2.7. *Let A, B, C, D be sets and $f : A \to B$, $g : B \to C$ and $h : C \to D$. The composition of functions is associative; $(h \circ g) \circ f = h \circ (g \circ f)$.*

Proof: Observe that $h \circ g : B \to D$ and $g \circ f : A \to C$ are functions by Theorem 7.2.3. Thus, the composite of $h \circ g$ and f is a function and likewise, $h \circ (g \circ f)$ is a function. Moreover, these share the same domain, namely A. It suffices to show these are equal at an arbitrary point in A. Consider then,

$$[h \circ (g \circ f)](x) = h((g \circ f)(x)) = h((g(f(x))))$$

and similarly,

$$[(h \circ g) \circ f](x) = (h \circ g)(f(x)) = h((g(f(x)))).$$

Since the calculations above hold for all $x \in A$ we find $(h \circ g) \circ f = h \circ (g \circ f)$. □

Theorem 7.2.8. *Let $f : A \to B$ be a function and recall $I_A : A \to A$ is the* **identity relation** *on A. Then $f \circ I_A = f$ and $I_B \circ f = f$.*

Proof: Clearly $I_A : A \to A$ is a function since $I_A(x) = x$ is clearly a single-valued formula. Hence, $f \circ I_A, I_B \circ f$ are functions by Theorem 7.2.3. Consider then,

$$(I_B \circ f)(x) = I_B(f(x)) = f(x)$$

for each $x \in dom(f) = A$ thus $I_B \circ f = f$ by Theorem 7.2.1. Furthermore,

$$(f \circ I_A)(x) = f(I_A(x)) = f(x)$$

for each $x \in dom(f) = A$ thus $f \circ I_A = f$ by Theorem 7.2.1. □

Theorem 7.2.9. *Let $f : A \to B$ be a function with $range(f) = C$. If f^{-1} is a function then $f^{-1} \circ f = I_A$ and $f \circ f^{-1} = I_C$.*

Proof: Let $f : A \to B$ is a function and assume that f^{-1} is a function. We know that f^{-1} is also the inverse of the relation $f \subseteq A \times B$; if xfy then $yf^{-1}x$ in the relation notation. But this means that $x(f^{-1} \circ f)x$ for each $x \in A$. Moreover, we can be sure that y is f^{-1} related to only x since f^{-1} is a function. Thus $f^{-1} \circ f = I_A$.

Likewise, if $y \in range(f) = C$ then there exists $x \in dom(f) = A$ such that $f(x) = y$. In other words, xfy which implies $yf^{-1}x$ and since f^{-1} is a function we know that x is the unique element in A which is f^{-1} related to y. To summarize, xfy and $yf^{-1}x$ for each $x \in range(f) = C$. Thus by definition of composite, $x(f \circ f^{-1})x$ for each $x \in C$. Thus by Theorem 7.2.1, $f \circ f^{-1} = I_C$. □

Remark 7.2.10. *Notice that we can have $B \neq C$ in the preceding theorem. For example, $f(x) = \sqrt{x}$ defined to be a function from $[0, \infty)$ to $\mathbb{R}$. Then you can calculate $f^{-1}(y) = y^2$ and $dom(f^{-1}) = [0, \infty)$. Clearly, $\mathbb{R} \neq [0, \infty)$. One way to think about this is that the codomain I chose for f was needlessly large. Since $f(x) = \sqrt{x}$ it follows that the range of f is full of non-negative values, we'll never cover the negative half of $\mathbb{R}$. This is the funny thing about codomains, you can always make them bigger.*

You can also make domains smaller. This is known as restricting a function.

Definition 7.2.11. *Let $f : A \to B$ and let $U \subseteq A$ then the* **restriction of f to U** *is the function*

$$f|_U = \{(x, y) \mid x \in U \text{ and } y = f(x)\}.$$

Additionally, if g is a restriction of h then we say h is an extension of g.

Restrictions are unique once a subset U is specified. Of course given different U we can form different restrictions. Extensions on the other hand allow for much more imagination.

Example 7.2.12 (silly extension)**.** *Consider $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = \sin(x)$, I can extend this to*

$$g(x) = \begin{cases} \sin(x) & \text{if } x \in \mathbb{R} \\ \mathbb{R} & \text{if } x \in \{i\} \end{cases}$$

Here clearly $g|_{\mathbb{R}} = f$ whereas $dom(g) = \mathbb{R} \cup \{i\}$ and in my crazy example here $g(i) = \mathbb{R}$. The output in my extension is not even of the same type as f.

The ambiguity in extending a function is pretty much the same ambiguity you have faced in homework problems where you were supposed to extrapolate from a given graph.

Example 7.2.13 (less silly extension)**.** *How do we extend the sine function to complex numbers? It can be shown that exp : $\mathbb{C} \to \mathbb{C}$ is a well-defined function of $\mathbb{C}$. The definition I am fond of is simply,*

$$\boxed{exp(z) = exp(x + iy) = e^x(\cos(y) + i\sin(y))}$$

It can be shown that this exponential function satisfies the same algebraic properties over $\mathbb{C}$ as the usual exponential function does for $\mathbb{R}$. Given this you can derive that for $x \in \mathbb{R}$

$$\sin(x) = \frac{1}{2i}\left(e^{ix} - e^{-ix}\right).$$

An obvious extension of $\sin : \mathbb{R} \to [-1, 1]$ *to $\mathbb{C}$ is given by the formula*

$$\sin(z) = \frac{1}{2i}\left(e^{iz} - e^{-iz}\right)$$

for each $z \in \mathbb{C}$. If we define $f(z) = \sin(z)$ for $z \in \mathbb{C}$ (as explained above) then $f|_{\mathbb{R}}$ is simply the ordinary sine function. By the way, range(exp) $= \mathbb{C} - \{0\}$. You can take our complex variables course to learn more.

Theorem 7.2.14. *Given two functions with non-overlapping domains, we can form a new function by simply pasting the given functions together. Suppose $f : A \to C$ and $g : B \to D$ are functions and $A \cap B = \emptyset$ then $h = f \cup g \subset (A \cup B) \times (C \cup D)$ is a function. Moreover,*

$$h(x) = \begin{cases} f(x) & \text{if} \quad x \in A \\ g(x) & \text{if} \quad x \in B \end{cases}$$

for each $x \in dom(h) = A \cup B$.

Proof: The formula for $h(x)$ is clearly single-valued since $x \in A \cup B$ and $A \cap B = \emptyset$ means either $x \in A$ or $x \in B$ (but not both). So the cases are distinct and in each case the output is single-valued by virtue of the fact that f, g are functions. □

Remark 7.2.15 (theorem above is weak)**.** *We can do better. In fact we can paste together two functions f, g which have $dom(f) \cap dom(g) \neq \emptyset$ provide that the functions are equal on the overlap. This is most of what is known as the "***pasting Lemma***".*

Example 7.2.16. *If $f(x) = \sin x$ with $dom(f) = [0, \infty)$ and $g(x) = x^2$ for $dom(g) = (-\infty, 0]$ then $h = f \cup g$ defines a function since $dom(f) \cap dom(g) = \{0\}$ and $f(0) = g(0) = 0$.*

7.3 injective functions

Definition 7.3.1. *Let $f : A \to B$ be a function then we say that f is* **injective** *or* **one-to-one** *iff for all $a, b \in A$, $f(a) = f(b)$ implies $a = b$. In other words, for each output $y \in range(f)$ there is a unique input $x \in dom(f)$ such that $y = f(x)$.*

Example 7.3.2. *Suppose $f : \mathbb{R} \to [0, \infty)$ is defined by $f(x) = x^2$ then f is not injective since $f(1) = f(-1)$ yet $1 \neq -1$.*

Example 7.3.3. *Let $f(x) = e^x$ for $x \in \mathbb{R}$ define $f : \mathbb{R} \to \mathbb{R}$. Let $a, b \in dom(f)$ then $f(a) = f(b)$ implies $e^a = e^b$ and if we take the natural log of this equation we obtain $\ln e^a = \ln e^b$ thus $a = b$. Thus f is injective on $\mathbb{R}$.*

Example 7.3.4. *Let $f(x) = \sqrt{3x-1}$ define $f : [1/3, \infty) \to \mathbb{R}$. If $a, b \in [1/3, \infty)$ then $f(a) = f(b)$ gives $\sqrt{3a-1} = \sqrt{3b-1}$ and if we square this equation we obtain $(\sqrt{3a-1})^2 = (\sqrt{3b-1})^2$ thus $3a - 1 = 3b - 1$ and we deduce via algebra that $a = b$. Hence f is a one-to-one function.*

Example 7.3.5. *Suppose $f : [0, \infty) \to [0, \infty)$ is defined by $f(x) = x^2$ then f is injective. To prove this let $a, b \in [0, \infty)$ and suppose $f(a) = f(b)$,*

$$f(a) = f(b) \ \Rightarrow \ a^2 = b^2 \ \Rightarrow \ a = \pm b.$$

However, since $a, b > 0$ it follows that only the $(+)$ solution is allowed and thus $a = b$. That little argument proves f is injective.

Remark 7.3.6. *The horizontal line test is based on the same logic. If a horizontal line crosses the graph at a and b with $a \neq b$ then that means that $f(a) = f(b)$ yet $a \neq b$. A function $f : U \subseteq \mathbb{R} \to V \subseteq \mathbb{R}$ will be injective iff it passes the horizonal line test.*

The last remark is useful, but the definition we gave for injective is far more general than the horizontal line test. How can you apply the horiontal line test in a situation where the graph is 4 or 5 dimensional?

Example 7.3.7 (determinant is not 1-1)**.** *Let $\det : M_2(\mathbb{R}) \to \mathbb{R}$ be the determinant function which takes an input of an 2×2 real-entried matrix A and outputs a single number which we denote by $det(A)$. Suppose that*

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

then

$$det(A) = det \begin{pmatrix} a & b \\ c & d \end{pmatrix} = ad - bc.$$

Observe that many different matrices will have a determinant of zero.

$$det \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = det \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = det \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} = 0$$

Clearly if we look at the inverse image of $\{0\}$ with respect to det we will find that this fiber has lots of stuff in it. Many different matrices have determinant zero. It turns out that many different 2×2 matrices also have determinant 1, I just picked on zero because it's easy. To conclude, the determinant function is **not** *injective.*

Example 7.3.8. *Let $\vec{X} : \mathbb{R}^2 \to \mathbb{R}^3$ be defined by $\vec{X} = p + u\vec{A} + v\vec{B}$ where p is a point in $\mathbb{R}^3$ and $\vec{A}, \vec{B}$ are vectors in $\mathbb{R}^3$. For $\vec{X}$ to be an injective function we need $\vec{X}(u_1, v_1) = \vec{X}(u_2, v_2)$ to imply $(u_1, v_1) = (u_2, v_2)$. Consider $\vec{X}(u_1, v_1) = \vec{X}(u_2, v_2)$,*

$$p + u_1\vec{A} + v_1\vec{B} = p + u_2\vec{A} + v_2\vec{B}$$

hence

$$(u_1 - u_2)\vec{A} + (v_1 - v_2)\vec{B} = 0.$$

We need both $u_1 - u_2 = 0$ and $v_1 - v_2 = 0$. It turns out these conditions are given if the vectors $\vec{A}$ and $\vec{B}$ are not colinear. In Math 221 we characterize a pair of vectors which are not colinear as being **linearly independent**. *If $\{\vec{A}, \vec{B}\}$ is linearly independent then $\vec{X}$ as defined above is an injective map.*

Theorem 7.3.9. *If $f : A \to B$ be injective and $g : B \to C$ be injective, then $g \circ f : A \to C$ is injective. The composite of injective functions is injective*

Proof: Suppose $(g \circ f)(a) = (g \circ f)(b)$. Then $g(f(a)) = g(f(b))$ hence $f(a) = f(b)$ using the fact that g is one-one. Likewise, $f(a) = f(b)$ implies $a = b$ by one-one property for f. Therefore, $g \circ f$ is one-one. □

7.4 surjective functions

The trouble with codomains is that sometimes they are too big. Surjectivity helps us pin down this ambiguity with functions.

Definition 7.4.1. *Let $f : A \to B$ be a function. We say that f is* **onto** *$V \subseteq B$ iff for each $b \in V$ there exists $a \in A$ such that $f(a) = b$. If f is onto B then we say that f is* **surjective** *or* **onto**.

The terms "onto" and "surjective" are the same. Both can be applied to either the function as a whole or to just some subset of the codomain.

Example 7.4.2. *Let $f(x) = \sin(x)$ then f is not onto $\mathbb{R}$ since there does not exist $x \in \mathbb{R}$ such that $\sin(x) = 2$ (for example). On the other hand, f is onto $[-1, 1]$ since the graph of sine oscillates continuously between $y = 1$ and $y = -1$.*

Example 7.4.3. *Let $f(x) = \frac{\sinh(x)}{\cosh(x)}$ define $f : \mathbb{R} \to \mathbb{R}$. We can show range$(f) = (-1, 1)$ thus f is not onto. However, if we let $g(x) = \frac{\sinh(x)}{\cosh(x)}$ define $g : \mathbb{R} \to (-1, 1)$ then g is a surjection.*

Example 7.4.4. *Let $f(x) = \tan(x)$ define $f : (-\pi/2, \pi/2) \to \mathbb{R}$. Notice $y = \tan(x)$ is continuous on its domain with $\lim_{x \to \pi/2^-} \tan(x) = \infty$ and $\lim_{x \to -\pi/2^+} \tan(x) = -\infty$. It is geometrically clear that range$(f) = \mathbb{R}$ thus f is an onto function.*

Theorem 7.4.5. *The composite of surjective functions is surjective.*

Proof: Suppose that $f : A \to B$ is a surjective function and $g : B \to C$ is a surjective function. Consider $g \circ f : A \to C$. We seek to show $g \circ f$ is onto C. Let $c \in C$. There exists $b \in B$ such that $g(b) = c$ since g is onto C. Moreover, there exists $a \in A$ such that $f(a) = b$ since f is onto B. Thus, $(g \circ f)(a) = g(f(a)) = g(b) = c$ which demonstrates that the composite is surjective as claimed. □

Theorem 7.4.6. *If $f : A \to B$ and $g : B \to C$ are functions such that $g \circ f$ is surjective then g is surjective.*

Proof: Suppose $f : A \to B$ and $g : B \to C$ are functions such that $g \circ f$ is surjective. Suppose $c \in C$ then since $g \circ f : A \to C$ is onto C it follows there exists $a \in A$ such that $(g \circ f)(a) = c$. Consider then that $(g \circ f)(a) = g(f(a)) = c$. Thus we find for each $c \in C$ there exists $f(a) \in B$ such that $g(f(a)) = c$. Thus g is surjective. □

Example 7.4.7 (determinant is surjective)**.** *Let* $\det : M_2(\mathbb{R}) \to \mathbb{R}$ *be the determinant function. Let $x \in \mathbb{R}$, observe that*

$$det \begin{pmatrix} x & 0 \\ 0 & 1 \end{pmatrix} = x.$$

Thus $\det : M_2(\mathbb{R}) \to \mathbb{R}$ *is* **onto** $\mathbb{R}$.

Example 7.4.8. *Let $f(x) = \ln(x-1)$. I claim this function is onto $\mathbb{R}$. I can anticipate this result because I know with confidence what the graph of natural log looks like (I hope the same is true for you). Let $y \in \mathbb{R}$ we wish to find $x \in dom(f) = (1,\infty)$ such that $\ln(x-1) = y$. This calls for a small calculation,*

$$y = \ln(x-1) \;\Rightarrow\; e^y = x-1 \;\Rightarrow\; x = e^y + 1.$$

Now I can prove f is surjective with confidence.
Proof: *Let $y \in \mathbb{R}$ then observe that $x = e^y + 1 > 1$ thus $x \in dom(f)$ and*

$$f(x) = f(e^y + 1) = \ln((e^y + 1) - 1) = \ln(e^y) = y.$$

Therefore, $f : (1,\infty) \to \mathbb{R}$ is onto.

Is this function f also injective? Let $a, b \in (1,\infty)$, assume $f(a) = f(b)$ then $\ln(a-1) = \ln(b-1)$ take the exponential of that equation to obtain $a - 1 = b - 1$ hence $a = b$. Thus f is **injective**

7.5 inverse of a function

This definition is central to Chapter 5. Basically we will learn that two sets have the same size if you can find a bijection between them.

Definition 7.5.1 (bijection)**.** *A function $f : A \to B$ is a* **bijection** *iff f is both an injection and a surjection. In other words, f is a bijection iff it is both 1-1 and onto. Finally, we also call a bijection a 1-1 correspondence.*

Example 7.5.2. *By Example 7.4.8 we have that $f(x) = \ln(x-1)$ is a bijection.*

We characterized how the inverse function interfaces with its function but we have yet to give a general criteria as to when the inverse function exists. Inverse relations were easy to define since we just had to flip the pairs in the Cartesian product. However, for a function, once we flip the pairs then there is nothing that in general assures us that the result is a function. Given $f : A \to B$ a function it will be true that $f^{-1} \subseteq B \times A$ is a relation from B to A. What will make $f^{-1} : B \to A$ a function?

Theorem 7.5.3. *Let $f : A \to B$ then*

(a.) *f^{-1} is a function from $range(f)$ to $dom(f) = A$ iff f is injective.*

(b.) *If f^{-1} is a function, then f^{-1} is injective.*

Proof of (a.): Assume that f^{-1} is a function from $range(f)$ to $dom(f) = A$. Suppose that $f(a) = f(b)$ for $a, b \in dom(f)$. Observe,

$$f^{-1}(f(a)) = f^{-1}(f(b)) \;\Rightarrow\; a = b.$$

Therefore f is one-one.

Conversely suppose that f is injective. Then $f(a) = f(b)$ implies $a = b$. Let $y \in range(f)$ then suppose $f^{-1}(y) = x$ and $f^{-1}(y) = z$, clearly there exists at least one such x or z by definition of $range(f)$. By definition of inverse relation, $f(f^{-1}(y)) = f(x)$ and $f(f^{-1}(y)) = f(z)$ thus $f(x) = f(z)$. Since f is injective it follows $x = z$ thus the relation f^{-1} is single valued with $f^{-1} : range(f) \to dom(f)$

Proof of (b.): Assume that f^{-1} is a function relative to the function $f : A \to B$. Suppose that $f^{-1}(y) = f^{-1}(z)$ then operate on both sides by the function f to get $f(f^{-1}(y)) = f(f^{-1}(z))$ but then by definition of inverse function $y = z$. Therefore f^{-1} is injective. □

Corollary 7.5.4. *If $F : A \to B$ is a bijection then $F^{-1} : B \to A$ is a bijection.*

Proof: left to reader. □

Theorem 7.5.5. *If $f : A \to B$ and $g : B \to C$ are bijections then*

(a.) *$g \circ f : A \to C$ is a one-one correspondence.*

(b.) *$f^{-1} : B \to A$ is a one-one correspondence.*

Proof of (a.): Theorem 7.4.5 give us that $g \circ f$ is surjective. Likewise, Theorem 7.3.9 gives us that $g \circ f$ is injective. Hence $g \circ f$ is a one-one correspondence.

Proof of (b.): We know from the relations discussion that $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$ and by Corollary 7.5.4 $(g \circ f)^{-1}$ is a bijection. Furthermore, Theorem 7.4.6 shows that f^{-1} is surjective since is the outside function of a surjective composite. Finally, Theorem 7.5.3 allows us to be sure f^{-1} is injective. Therefore, f^{-1} is a bijection. □

Theorem 7.5.6. *If $f : A \to B$ and $g : B \to C$ are functions such that $g \circ f$ is injective then f is injective.*

Proof: Left to reader. This seems like a nice homework problem. □

Theorem 7.5.7. *Let $F : A \to B$ and $G : B \to A$. Then $G = F^{-1}$ iff $G \circ F = I_A$ and $F \circ G = I_B$*

Proof: Suppose $G = F^{-1}$ then $F \circ G = F \circ F^{-1} = I_B$ whereas $G \circ F = F^{-1} \circ F = I_A$ (using Theorem 7.2.9 twice). Conversely suppose $G \circ F = I_A$ and $F \circ G = I_B$. Observe that F is injective (by $G \circ F = I_A$) and surjective (by $F \circ G = I_B$) thus F^{-1} is a function on B using the Theorems of this section. Consider then, $F^{-1} = F^{-1} \circ I_B = F^{-1} \circ F \circ G = I_A \circ G = G$. □

Remark 7.5.8. *There are examples where $F \circ G = I_A$ yet $G \circ F \neq I_B$. In this case we can not say that $F^{-1} = G$. It is necessary in general to check both sides. (certain contexts make one side follow from the other, but that only happens when there is an additional stucture added to the mix)*

Example 7.5.9. *Let $f(x) = x^2$ and $g(x) = \sqrt{x}$. Clearly $(f \circ g)(x) = x$ for each $x \in dom(g) = [0, \infty)$. However, $(g \circ f)(x) = \sqrt{x^2} = \pm x$ thus we say that g has* **left inverse** *f but has no* **right inverse**. *This means that $f^{-1} \neq g$. If we restrict g to $g|_{[o,\infty)}$ then we get both left and right inverse conditions to hold and the preceding Theorem would allow us to conclude that $f^{-1} = g|_{[o,\infty)}$.*

There is more to learn past this point. What can we say about restrictions and extensions ? How does injectivity and surjectivity filter through such constructions ? Can it ? Perhaps we will have some homework about this.

7.6 on building a bijection

In this section we consider an function $f : A \to B$. Our project here is to investigate how we can modify f to create a bijection. I will describe two related, but different, methods to modify f to a bijection. Equivalently, these are two methods to replace f which is not invertible as a function to a corresponding function which is invertible.

Step 1: it is simple to make f into a surjection. We simply replace B with $f(A)$. Define $f_1 : A \to f(A)$ where $f_1(x) = f(x)$ for each $x \in A$. It should be clear that f_1 is a surjection with this simple modification.

Step 2: if f is injective then f_1 is a bijection since f_1 is a function which is both one-to-one and onto. However, if f is not injective then we will need to modify f_1 in order to obtain a bijection. There are two ways to go here:

- **restriction:** replace A with a smaller set S for which $f_1|_S$ is an injection. This injection $f_1|_S$ has inverse $f_1|_S^{-1} : f(A) \to S$ which is known as a **local inverse for** f. Local inverse for f is not usually unique since there are many choices for S.

- **passing to quotient:** replace A with $A/\sim$ where $\sim$ is the equivalence relation corresponding to the non-empty fiber partition of the domain. Then $\bar{f}([x]) = f(x)$ defines a unique bijection $\bar{f} : A/\sim \to f(A)$.

Step 3: to relate the two methods, points in S give a complete set of representatives for the equivalence classes of the non-empty fiber partition of A. On the other hand, if we can find a section of the natural map then the image of the section gives an appropriate choice for a restricting set S which allows the creation of a local inverse.

In the remainder of this section I will elaborate further on the methods sketched above.

Theorem 7.6.1. *Let $f : A \to B$ be a function. Let $x, y \in A$ then we define $x \sim y$ iff $f(x) = f(y)$. This defines an equivalence relation on A whose equivalence classes are the non-empty fibers of f.*

Proof: Let $f : A \to B$ be a function. Let $x, y \in A$ then we define $x \sim y$ iff $f(x) = f(y)$. If $x \in A$ then $f(x) = f(x)$ hence $x \sim x$ and $\sim$ is reflexive. Likewise, if $f(x) = f(y)$ then $f(y) = f(x)$ thus $x \sim y$ implies $y \sim x$ for all $x, y \in A$. Lastly, if $x, y, z \in A$ and $x \sim y$ and $y \sim z$ then $f(x) = f(y)$

and $f(y) = f(z)$ thus $f(x) = f(z)$ and we find $x \sim z$ thus $\sim$ is transitive. In total, $\sim$ forms an equivalence relation on A. Consider, the equivalence class of $\sim$ with representative $x \in A$ has form:

$$[x] = \{y \in A \mid f(x) = f(y)\}.$$

On the other hand, a fiber is the inverse image of a point in B. Consider $f(x) \in B$, then

$$f^{-1}\{f(x)\} = \{y \in A \mid f(y) \in \{f(x)\}\} = \{y \in A \mid f(y) = f(x)\}.$$

Therefore, $[x] = f^{-1}\{f(x)\}$ for each $x \in A$. $\square$

The natural map and its sections play a dual role for a given equivalence relation.

Definition 7.6.2. *Suppose A has an equivalence relation R. If $A/R = \{[x]_R \mid x \in A\}$ then $\pi : A \to A/R$ defined by $\pi(x) = [x]_R$ is the* **quotient map** *of R. A* **section** *of $\pi : A \to A/R$ is a map $s : A/R \to A$ such that $s \circ \pi = id_A$.*

Notice π is uniquely specified by the given equivalence relation R whereas there may be infinitely many choices for the construction of s. We require $s(\pi(x)) = x$ for each $x \in A$. That is, $s([x]_R) = x$ for each $x \in A$.

Example 7.6.3. *Consider the equivalence relation on $\mathbb{Z}$ given by $x \sim y$ iff $4 \mid y - x$. Then*

$$[x] = \{x + 4k \mid k \in \mathbb{Z}\}$$

Thus, the quotient map is given by

$$\pi(x) = x + 4\mathbb{Z} = \{x + 4k \mid k \in \mathbb{Z}\}$$

Define $s_1([x]) = y$ where $y \in [x] \cap \{0, 1, 2, 3\}$ then

$$s_1([0]) = 0, \quad s_1([1]) = 1, \quad s_1([2]) = 2, \quad s_1([3]) = 3$$

Define $s_2([x]) = y$ where $y \in [x] \cap \{-2, -1, 0, 1\}$ then

$$s_2([0]) = 0, \quad s_2([1]) = 1, \quad s_2([2]) = -2, \quad s_2([3]) = -1$$

since $[-1] = [3]$ and $[-2] = [2]$ working modulo 4. You can verify

$$s_1([x]) = x \qquad \& \qquad s_2([x]) = x$$

for each $x \in \mathbb{Z}$ thus $s_1 \circ \pi = Id$ and $s_2 \circ \pi = Id$. You can see the choices for sections is endless, each choice simply corresponds to a convention for choosing representatives of the mod 4 equivalence classes.

Example 7.6.4. *Define $F : \mathbb{R}^2 \to \mathbb{R}$ by $F(x, y) = y - x$. The fiber equivalence for F defined by $(x_1, y_1) \sim (x_2, y_2)$ iff $F(x_1, y_1) = F(x_2, y_2)$ has equivalence classes of the form*

$$F^{-1}\{c\} = \{(x, y) \in \mathbb{R}^2 \mid y - x = c\} = L_c.$$

We use L_c to denote the line with slope 1 and y-intercept c. Here $\pi : \mathbb{R} \to \mathbb{R}^2$ is defined by $\pi(c) = L_c$. Define $s : \mathbb{R}^2/\sim \to \mathbb{R}$ by $s([(a, b)]) = b - a$. Notice L_c is the collection of $(x, y) \in \mathbb{R}^2$ for which $y = x + c$. If $(a, b) \in L_c$ then $b = a + c$ hence $c = b - a$. Thus $[(a, b)] = L_{b-a}$ and $L_c = [(0, c)]$. For instance, Consider,

$$s(\pi(c)) = s(L_c) = s([(0, c)]) = c - 0 = c \quad \Rightarrow \quad s \circ \pi = Id_{\mathbb{R}}.$$

Theorem 7.6.5. *Let $f : A \to B$ be a surjective function and suppose $\pi : A \to A/\sim$ defined by $\pi(x) = [x] = \{y \in A \mid f(x) = f(y)\}$. Then $\bar{f} : A/\sim \to B$ defined by $\bar{f}([x]) = f(x)$ is a bijection.*

Proof: we begin by showing $\bar{f}$ is well-defined. Suppose $[x] = [y]$ then $f(x) = f(y)$ thus $\bar{f}([x]) = \bar{f}([y])$ hence $\bar{f}$ is single-valued and hence $\bar{f}$ is a function. Let $b \in B$ then since f is surjective there exists $a \in A$ for which $f(a) = b$. Consequently, $\bar{f}([a]) = f(a) = b$ is surjective. It remains to show $\bar{f}$ is injective. Suppose $\bar{f}([x]) = \bar{f}([y])$ then $f(x) = f(y)$ thus $[x] = [y]$ and we find $\bar{f}$ is injective. Thus $\bar{f}$ is a bijection. □

Example 7.6.6. *In Example 7.6.4 we explored the equivalence relation for $F(x, y) = y - x$. Let $t \in \mathbb{R}$ then $F(0, t) = t$ thus F is onto $\mathbb{R}$. If we apply the construction of the theorem above to F,*

$$\bar{F}([(x, y)]) = F(x, y) = y - x.$$

The function $\bar{F}$ is a bijection from $\mathbb{R}^2/\sim \to \mathbb{R}$. In contrast, $F : \mathbb{R}^2 \to \mathbb{R}$ is not injective. In particular, $F(x + k, y + k) = y + k - (x + k) = y - x = F(x, y)$ for any $k \in \mathbb{R}$ gives insight as to why F is not one-to-one. For instance, $F(0, 1) = F(-1, 0) = 1$ thus F is not injective.

Example 7.6.7. *Beginning with $F : \mathbb{R}^2 \to \mathbb{R}$ if set $S_1 = \{(x, y) \mid x = 0, y \in \mathbb{R}\}$ then notice $F|_{S_1} : S_1 \to \mathbb{R}$ is a bijection. Let $(x_1, y_1), (x_2, y_2) \in S_1$ and suppose $F|_{S_1}(x_1, y_1) = F|_{S_1}(x_2, y_2)$. Thus $F(x_1, y_1) = F(x_2, y_2)$ and we find $y_1 - x_1 = y_2 - x_2$. However, $x_1 = x_2 = 0$ hence $y_1 = y_2$ and we find $(x_1, y_1) = (x_2, y_2)$. Therefore, $F|_{S_1}$ is injective. If $t \in \mathbb{R}$ then $(0, t) \in S_1$ and $F|_{S_1}(0, t) = t - 0 = t$. Consequently $F|_{S_1}$ is a bijection. If we set $S_m = \{(x, y) \in \mathbb{R}^2 \mid y = mx,\ m \neq 1\}$ then $F|_{S_m} : S_m \to \mathbb{R}$ is a bijection. I might assign this as a homework.*

Chapter 8

Cardinality

My goal for us is to get the big picture about cardinality. In particular I want you to learn the meaning of the terms ”finite”, ”denumerable”, ”countable” and ”infinite”. I want you to gain a deeper appreciation for the difference between real and rational numbers. My apologies in advance if some proofs are missing here. As is my usual custom, I will endeavor to give proofs in lecture, but I know we probably do not have time for everything. That said, the concept of cardinality is important as a backdrop to every upper level math course so we certainly should cover it in this course. The examples in this chapter also give us additional experience in the problem of judging injectivity and surjectivity of maps as well as the deeper problem of how to construct such maps when the need arises.

8.1 one-one correspondence and finite sets

Definition 8.1.1. *Two sets A and B are said to be* **equivalent** *iff there exists a one-one correspondence between them. In the case that there exists a bijection from A to B we say that $A \approx B$.*

We can easily show that $\approx$ forms an *equivalence relation* on the ”class” of all sets. Notice we are careful not say ”set of all sets”. We discussed why in our conversation about axiomatic set theory. We avoid the tiresome question: ”does the set of all sets contain itself?”.

Example 8.1.2. *Consider a set $A = \{1, \emptyset, dora\}$. This is equivalent to the set $\{1, 2, 3\}$. To prove this construct the mapping*

$$\Psi(1) = 1, \quad \Psi(\emptyset) = 2, \quad \Psi(3) = dora$$

it is clear this is both one-one and onto $\{1, 2, 3\}$. You might object that these are not the ”same” sets. I agree, but I didn't say they were the same, I said they were **equivalent** *or perhaps it is even better to say that the sets are in* **one-one correspondence***.*

Definition 8.1.3. $\mathbb{N}_k = \{1, 2, \dots, k\}$ *for any $k \in \mathbb{N}$. Here $\mathbb{N}_1 = \{1\}$ and $\mathbb{N}_2 = \{1, 2\}$ etc.*

Example 8.1.4. *Now I repeat the same idea as the previous example for an arbitrary finite set which has k things in it. Let $\mathbb{N}_k = \{1, 2, \dots, k\}$. If a set A has k distinct objects in it then it is easy to prove it is equivalent to $\mathbb{N}_k = \{1, 2, \dots, k\}$. Lable these k objects $A = \{a_1, a_2, \dots a_k\}$ then there is an obvious bijection,*

$$\Psi(a_j) = j \textit{ for each } j \in \mathbb{N}_k$$

The mapping Ψ is one-one since for $a_j, a_l \in \mathbb{N}_k$ we find $\Psi(a_j) = \Psi(a_l)$ implies $j = l$ implies $a_j = a_l$.

I claim the mapping Ψ is also onto. Let $y \in \mathbb{N}$ then by definition of $\mathbb{N}_k$ we have $y = j$ for some $j \in \mathbb{N}$ with $1 \leq j \leq k$. Observe that $a_j \in A$ since $1 \leq j \leq k$, and $\Psi(a_j) = j$.

Given the last example, you can appreciate the following definition of **finite**[1]

Definition 8.1.5. *A set S is said to be* **finite** *iff it is empty $S = \emptyset$ or in one-one correspondence with $\mathbb{N}_k$ for some $k \in \mathbb{N}$. Moreover, if $S \approx \mathbb{N}_k$ we define the* **cardinality** *of A to be $\overline{\overline{A}} = k$. If $S = \emptyset$ then we define $\overline{\overline{A}} = 0$.*

To summarize, the cardinality of a finite set is the number of elements it contains. The nice thing about finite sets is that you can just count the elements in them.

Definition 8.1.6. *A set S is infinite if it is not finite.*

Proposition 8.1.7. *A finite set is not equivalent to any of its proper subsets.*

A proper subset $A \subset B$ will be missing something since a "proper subset" A is a subset which is not the whole set B. It follows that B must have more elements and consequently $A \approx \mathbb{N}_a$ and $B \approx \mathbb{N}_b$ where $a < b$. The contrapositive of the proposition above is more interesting.

Proposition 8.1.8. *A set which is equivalent to one or more of its proper subsets is infinite.*

So if you were counting, there are two nice ways to show a set is infinite. First, you could assume it was finite and then work towards a contradiction. Second, you could find a bijection from the set to some proper subset of itself.

Example 8.1.9 ($\mathbb{N}$ is infinite)**.** *Observe that the mapping $f : \mathbb{N} \rightarrow 2\mathbb{N}$ defined by $f(n) = 2n$ is a bijection. First, observe*

$$f(x) = f(y) \quad \Rightarrow \quad 2x = 2y \quad \Rightarrow \quad x = y$$

therefore f is injective. Next $2\mathbb{N} = \{2k \mid \exists k \in \mathbb{N}\}$. Let $y \in 2\mathbb{N}$ then there exists $k \in \mathbb{N}$ such that $y = 2k$. Observe that

$$f(k) = 2k = y$$

thus f is onto $2\mathbb{N}$. Therefore $\mathbb{N} \approx 2\mathbb{N}$ and since $2\mathbb{N}$ is a proper subset of $\mathbb{N}$ it follows that $\mathbb{N}$ is infinite.

8.2 countably infinite sets

Definition 8.2.1 (denumerable)**.** *Let S be a set, we say S is* **denumerable** *iff $S \approx \mathbb{N}$. The cardnality of $S \approx \mathbb{N}$ is said to be $\aleph_o$. We denote $\overline{\overline{S}} = \aleph_o$ iff $S \approx \mathbb{N}$.*

The following is a list of sets with cardnality $\aleph_o$,

$$\mathbb{N},\ 2\mathbb{N},\ 3\mathbb{N},\ \mathbb{Z},\ 2\mathbb{Z},\ \mathbb{N} \times \mathbb{N},\ \mathbb{N}^{123},\ \{x \in \mathbb{R} \mid \sin(x) = 0\}, \left\{\frac{2}{n} \mid n \in \mathbb{N}\right\}$$

[1] my apologies I am shifting notation at this point, before we used $\#(S)$ for the number of things in S, but now I am adopting the notation $\overline{\overline{S}}$ for this chapter.

I don't find any of the examples above too surprising. These are all manifestly discrete sets. If you visualize them there is clearly gaps between adjacent values in the sets. In contrast, think about the rational numbers. Given any two rational numbers we can always find another in between them: given $p/q, m/n \in \mathbb{Q}$ we find

$$\frac{1}{2}\left(\frac{p}{q}+\frac{m}{n}\right)=\frac{1}{2}\left(\frac{pn+qm}{nq}\right)\in\mathbb{Q}$$

at the midpoint between p/q and m/n on the number line. It would seem there are more rational numbers then natural numbers. However, things are not always what they "seem". Cantor gave a bijection between $\mathbb{N}$ and postive rational numbers (there is likely a diagram of this in your text, I will explain more in lecture). Once you have that it's not hard to prove

$$\boxed{\overline{\overline{\mathbb{Q}}}=\aleph_o.}$$

Sometimes we also call a denumerable set a "countably infinite" set, here is why:

Definition 8.2.2 (countable)**.** *A set S is said to be* **countable** *iff S is finite or denumerable. If a set S is not countable then it is said to be* **uncountable***.*

8.3 uncountably infinite sets

The title of this section is somewhat superfluous since every uncountable set is necessarily infinite. Uncountable sets are quite common.

Theorem 8.3.1. *The open interval $(0,1)$ is uncountable.*

We might prove this in lecture, there is a proof which basically stems from the decimal expansion of the real numbers. The theorem above assures us the following definition is worthwhile:

Definition 8.3.2. *We define the cardnality of the open interval $(0,1)$ to be c (for* **continuum***).*

The proof $(0,1)$ is uncountable is not too easy, but once you have the unit interval it's easy to get other subsets of $\mathbb{R}$.

Example 8.3.3. *Show $(0,1)\approx(5,8)$. To do this we want a one-one mapping that takes $(0,1)$ as its domain and $(5,8)$ as its range. A line segment will do quite nicely. Let $f(x)=mx+b$ and fit the points*

$$f(0)=5=b, \quad f(5)=5m+5=8$$

Clearly $f(x)=\frac{3}{5}x+5$ will provide a bijection of the open intervals. Its not hard to see this construction works just the same for any open interval (a,b). Thus the cardnality of any open interval is c.

There are bijections from the open interval to closed intervals and half-open half-closed intervals not too mention unions of such things. These mappings are not always as easy to find. The text shows how to dodge the construction through a series of insightful theorems which we are skipping.

Example 8.3.4. *Show $(0,1)\approx\mathbb{R}$. First observe that $(0,1)\approx(-\frac{\pi}{2},\frac{\pi}{2})$ thus by transitivity of $\approx$ is suffices to show that $(-\frac{\pi}{2},\frac{\pi}{2})\approx\mathbb{R}$. The graph of inverse tangent comes to mind, it suggests we use*

$$f(x)=\tan^{-1}(x)$$

This mapping has dom$(f) = \mathbb{R}$ *and range*$(f) = (-\frac{\pi}{2}, \frac{\pi}{2})$. *This can be gleaned from the relation between a function and its inverse. The vertical asymptotes of tangent flip to become horizontal tangents of the inverse function. Notice that*

$$f(a) = f(b) \;\Rightarrow\; \tan^{-1}(a) = \tan^{-1}(b) \;\Rightarrow\; a = b$$

by the graph and definition of inverse tangent. Also, if $y \in (-\frac{\pi}{2}, \frac{\pi}{2})$ *then clearly* $f(\tan(y)) = y$ *hence* f *is onto.*

Example 8.3.5. *Show that* $[0,1] \approx (0,1)$. *Well, we already have that* $(0,1) \approx \mathbb{R}$ *so if I can find a mapping from* $[0,1]$ *to* $\mathbb{R}$ *which is a bijection then we're done. Let's think. If* f *is a bijection which is continuous with continuous inverse then* f *maps open sets to open sets and* f *maps closed sets to closed sets. This means the construction of the function showing equivalence of* $(0,1)$ *and* $[0,1]$ *cannot be a continuous function. In other words, whatever map shows* $(0,1) \approx [0,1]$, *it's not as easy as our previous examples. We have two choices then (1.) construct the technical bijection between these sets (2.) take the much easier route of applying the CSB Theorem to show their equivalence. But, since we don't know that theorem yet we proceed with (1.).*

Here is a rather ingenious construction I found on the Mathematics Stack Exchange by Asaf Karagila see here (I changed it to make it a bit easier to follow). Define $f : [0,1] \to (0,1)$ *by*

$$f(x) = \begin{cases} \frac{1}{2} & \text{if } x = 0 \\ \frac{1}{2^2} & \text{if } x = 1 \\ \frac{1}{2^{n+2}} & \text{if } x = \frac{1}{2^n} \text{ for some } n \in \mathbb{N} \\ x & \text{otherwise} \end{cases}.$$

This map has infinitely many points of discontinuity since $f(x) \to \frac{1}{2^n}$ *as* $x \to \frac{1}{2^n}$ *yet* $f\left(\frac{1}{2^n}\right) = \frac{1}{2^{n+2}}$ *by construction. Injectivity is not too hard to check, I leave that to the reader. Surjectivity might be a bit trickier. Suppose* $x \in (0,1)$ *and* $x \neq \frac{1}{2^n}$ *for some* $n \in \mathbb{N}$. *Then* $f(x) = x$. *If* $x = 1/2$ *then note* $f(0) = 1/2$. *If* $x = 1/2^2$ *then note* $f(1) = 1/2^2$. *Finally, if* $x = 1/2^{n+2}$ *for some* $n \in \mathbb{N}$ *then* $f(1/2^n) = 1/2^{n+2}$. *Thus* f *is onto* $(0,1)$. *Hence* $f : [0,1] \to (0,1)$ *is a bijection and* $[0,1] \approx (0,1)$.

8.4 Cantor's Theorem and transfinite arithmetic

Definition 8.4.1. *Let* A *and* B *be sets. Then*

- **(1.)** $\overline{\overline{A}} = \overline{\overline{B}}$ *iff* $A \approx B$, *otherwise* $\overline{\overline{A}} \neq \overline{\overline{B}}$
- **(2.)** $\overline{\overline{A}} \leq \overline{\overline{B}}$ *iff there exists an injection* $f : A \to B$
- **(3.)** $\overline{\overline{A}} < \overline{\overline{B}}$ *iff* $\overline{\overline{A}} \leq \overline{\overline{B}}$ *and* $\overline{\overline{A}} \neq \overline{\overline{B}}$

Notice that the injection took A as its domain. The direction is important here, it is not assumed that $f(A) = B$ in part (2.). Thus, while we can form an inverse function from *range*(f) to A that will not be a bijection from B to A since *range*(f) may not equal B in general. Transfinite arithmetic enjoys many of the same rules as ordinary arithmetic, see your text for proof, or perhaps we'll argue this in lecture.

Theorem 8.4.2 (Cantor's Theorem)**.** *For every set* A, $\overline{\overline{A}} < \overline{\overline{\mathcal{P}(A)}}$.

It then follows that we have an unending string of infinities:

$$\aleph_o = \overline{\overline{\mathbb{N}}} < \overline{\overline{\mathcal{P}(\mathbb{N})}} < \overline{\overline{\mathcal{P}(\mathcal{P}(\mathbb{N}))}} < \overline{\overline{\mathcal{P}(\mathcal{P}(\mathcal{P}(\mathbb{N})))}} < \cdots$$

An obvious question to ask is "where does the continuum c fit into this picture? It can be shown that $\aleph_o < c$. To see this, note $\aleph_o \leq c$ since $\mathbb{N} \subseteq \mathbb{R}$ we can restrict the identity function to an injection from $\mathbb{N}$ into $\mathbb{R}$ and since $\mathbb{R}$ is not equivalent to $\mathbb{N}$ we have that $\aleph_o < c$.

Theorem 8.4.3 (Cantor-Schröder-Bernstein Theorem)**.** *If $\overline{\overline{A}} \leq \overline{\overline{B}}$ and $\overline{\overline{B}} \leq \overline{\overline{A}}$, then $\overline{\overline{A}} = \overline{\overline{B}}$.*

This is a non-trivial Theorem despite it's humble appearance.

Example 8.4.4. *Return to Example 8.3.5 once more. To show $(0,1) \approx [0,1]$ we note $f : (0,1) \rightarrow [0,1]$ defined by $f(x) = x$ for $x \in (0,1)$ is an injection thus $\overline{\overline{(0,1)}} \leq \overline{\overline{[0,1]}}$. Likewise, $g : [0,1] \rightarrow (0,1)$ given by $g(x) = x/2 + 1/4$ is an injection hence $\overline{\overline{[0,1]}} \leq \overline{\overline{(0,1)}}$. Thus, by the CSB Theorem, $(0,1) \approx [0,1]$.*

Example 8.4.5. *It can be shown that $\overline{\overline{\mathcal{P}(\mathbb{N})}} \leq \overline{\overline{(0,1)}}$ and $\overline{\overline{\mathcal{P}(\mathbb{N})}} \geq \overline{\overline{(0,1)}}$[2]. Thus $\overline{\overline{\mathcal{P}(\mathbb{N})}} = \overline{\overline{(0,1)}} = c$.*

Definition 8.4.6 (trichotomy property of $\mathbb{N}$)**.** *If $m, n \in NN$ then $m > n$, $m = n$, or $m < n$*

The theorem below is called the **Comparability Theorem**,

Theorem 8.4.7. *If A and B are any two sets, then $\overline{\overline{A}} > \overline{\overline{B}}$, $\overline{\overline{A}} = \overline{\overline{B}}$, or $\overline{\overline{A}} < \overline{\overline{B}}$.*

It turns out that it is impossible to prove this Theorem in the Zermelo Fraenkel set theory unless we assume the Axiom of Choice is true.

Theorem 8.4.8. *If $\mathcal{A}$ is a collection of non-empty sets, then there exists a function F (the* **choice** *function) from $\mathcal{A}$ to $\cup_{A \in \mathcal{A}} A$ such that for every $A \in \mathcal{A}$ we have $F(A) \in A$.*

This axiom does lead to some unusual results. For example, the Banach-Tariski paradox which says that a ball can be cut into pieces and reassembled into two balls such that the total volume is doubled. (don't worry these "cuts" are not physically reasonable). Or the weird result that every subset of $\mathbb{R}$ can be reordered such that it has a smallest element.

Theorem 8.4.9. *If there exists a function from a set A onto a set B, then $\overline{\overline{B}} \leq \overline{\overline{A}}$.*

Notice surjectivity suggests that there is at least one thing in the domain to map to each element in the range B. It could be the case that more than one thing maps to each element in B, but certainly at least one thing in A maps to a given element in B. If the fibers in A are really "big" then inequality in the Theorem would become a strict $<$. The proof of this Theorem given in the text involves choosing something in the fiber.

Remark 8.4.10 (Continuum Hypothesis)**.** *The* **Continuum Hypothesis** *states that c is the next transfinite number beyond $\aleph_o$. There is no other infinite set between the rationals and the reals. This was conjectured by Cantor, but only later did the work of Godel(1930's) and Cohen(1960's) elucidate the issue. Godel showed that the Continuum Hypothesis was* **undecidable** *but relatively consistent in Zermelo Frankael set-theory. Then later Paul Cohen showed that the Continuum Hypothesis was independent of the Axiom of Choice relative to Zermelo-Frankael set theory modulo the Axiom of Choice. The Continuum Hypothesis and the Axiom of Choice continue to be widely believed since they are important "big guns" for certain crucial steps in hard theorems.*

[2] see pg. 250 of Smith, Eggen and St. Andre's *Transition to Advanced Mathematics*

Chapter 9

Analysis

Calculus is usually the first place students are exposed to analysis. Roughly, analysis is mathematics which involves using estimates and inequalities to quantify the existence and structure of limits. This is already far too limiting. Analysis also includes things like measure theory, the theory of differentiation, asymptotics and much much more. In some sense, the topology (which I introduced briefly in the early story arc of this course) is abtract analysis. But, then again, the study of metric spaces and Hilbert spaces are likewise of great importance to the overall story of mathematics as well as its application in physics. Practicing mathematicians who know more than me (not hard) object to this demarcation of algebra vs. analysis. The lines cannot so clearly be drawn, mathematics cannot be compartmentalized without damaging its ultimate progress. All of that said, I've found the following simplistic rule to be pretty accurate:

> Algebra is the study of equality and structure whereas Analysis is the study of inequality and existence.

Ok, sometimes I leave off the ”structure” and ”existence” because truthfully all of mathematics is about both structure and existence of abstract mathematical concepts.

I make no effort to be abstract in this chapter. Instead we will focus on single variable calculus and the theory of limits and convergence. There are great problems where we can test our understanding of quantifiers and our ability work with definition. The study of asymptotic behavior is also introduced, we discuss the little and big $\mathcal{O}$ notation and how it gives an intuitive guide to deciding absolute or relative growth in given functions on $\mathbb{R}$.

Time permitting, we review proofs of some of the more delicate theorems of calculus. Some of these proofs should have been given in Calculus I and II, but I do not expect previous knowledge of the proof itself. This should give us a chance to study several proofs which build off existing theory. Often in higher math we have to learn to use theorems to prove additional theorems. There is a danger in undergraduate math, sometimes we give the impression that you are not allowed to use theorems for proofs. It may seem that everything has to be done from the definition and logic alone. This is false. Context matters, the context of being asked a definition plus logic proof is that you are in the midst of an introductory course where we're probably asking you to do the proof to understand the definition. This phase will pass, in the next story arc you will have to learn many theorems and do **the weave** as you use multiple theorems in concert to prove more complicated assertions. That is not this course. We don't have such toys to play with here.

9.1 definitions

9.1.1 limits

Before we can define the limit we must define the sort of points where we can reasonably take limits for functions on $\mathbb{R}$.

Definition 9.1.1. *limit point*

Let $U \subseteq \mathbb{R}$. We say p is a **limit point** of U if for every $\delta > 0$ we have $B_\delta(p)_o \cap U \neq \emptyset$. We say p is a limit point of a function f on $\mathbb{R}$ if and only if p is a limit point of $dom(f)$. If there exists $\eta > 0$ for which $B_\eta(p)_o \subseteq dom(f)$ then p is an **interior limit point** of f.

Recall $B_\delta(p)_o = (p-\delta, p) \cup (p, p+\delta)$ thus the definition above simply reduces to the condition that for p to be a limit point of U there must be at least one other point in U near p no matter how small we make δ. In fact, we see a limit point p for a function f is a point at which there are infinitely many points in $dom(f)$ near p. Not every function has a limit point:

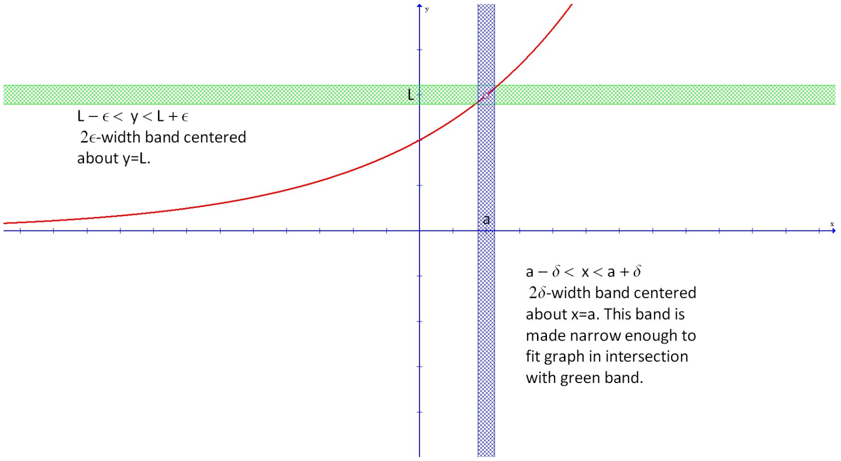
Example 9.1.2. *Sequences on $\mathbb{R}$ are functions $a : \mathbb{N} \to \mathbb{R}$ where we usually denote $a(n) = a_n$. In this case, no point in $\mathbb{N}$ is a limit point since $(n-1/2, n+1/2) \cap \mathbb{N} = \{n\}$ hence $B_{1/2}(n)_o \cap \mathbb{N} = \emptyset$. Every point in the domain of a sequence is called an* **isolated point***.*

Sequences are important, we will see them again when we study the area problem later in this course. For now though, we will focus on functions where there are more than just isolated points:

Definition 9.1.3. *limit or double-sided limit*

Let f be a function with interior limit point a and suppose $L \in \mathbb{R}$. We say that $f(x) \to L$ as $x \to a$ if and only if for each $\varepsilon > 0$ there exists $\delta > 0$ such that for all $x \in \mathbb{R}$ with $0 < |x-a| < \delta$ it follows $|f(x) - L| < \varepsilon$. In the case that the condition above is met we say that the limit exists and denote this by $\lim\limits_{x \to a} f(x) = L$.

Basically the idea is just that if we zoom in on an ϵ-band centered about L then the limit exists if we can find a δ-band centered about a such that the box made from the intersection of these bands captures the graph of the function for all the values in $(a-\delta, a) \cup (a, a+\delta)$



It is useful to have langauge to distinguish between left and right limits.

Definition 9.1.4. *one-sided limits*

If f is a function with limit point a.

1.) Assume there exists $\eta > 0$ for which $(a - \eta, a) \cap dom(f) \neq \emptyset$. If for each $\varepsilon > 0$ there exists $\delta > 0$ for which $x \in \mathbb{R}$ with $a < x < a + \delta$ implies $|f(x) - L| < \varepsilon$ then we write $\displaystyle\lim_{x \to a^+} f(x) = L$ and call this the **right-limit** at $x = a$ of f.

2.) Assume there exists $\eta > 0$ for which $(a, a + \eta) \cap dom(f) \neq \emptyset$. If for each $\varepsilon > 0$ there exists $\delta > 0$ for which $x \in \mathbb{R}$ with $a - \delta < x < a$ implies $|f(x) - L| < \varepsilon$ then we write $\displaystyle\lim_{x \to a^-} f(x) = L$ and call this the **left-limit** at $x = a$ of f.

If $(a - \eta, a) \cap dom(f)$ and $(a, a + \eta) \cap dom(f)$ then $B_\eta(a)_o \subseteq dom(f)$ and a is an interior limit point. Interior limit points allow for the calculation of left, right and double-sided limits. In contrast, if the domain of f was $[0, 1)$ then I would not consider $\lim_{x \to 0^-} f(x)$ or $\lim_{x \to 1^+} f(x)$ to be a well-defined limits. However, $\lim_{x \to 0^+} f(x)$ or $\lim_{x \to 1^-} f(x)$ would be well-defined limits (which may or may not exist).

Definition 9.1.5. *limits which diverge to ∞*

Let f be a function and $a \in \mathbb{R}$.

- We say that $f(x) \to \infty$ as $x \to a$ if and only if for each $M > 0$ there exists $\delta > 0$ such that $f(x) > M$ whenever $0 < |x - a| < \delta$. In the case that the condition above is met we say that the limit **diverges to** ∞ and denote this by $\displaystyle\lim_{x \to a} f(x) = \infty$.
- If for each $M > 0$ there exists $\delta > 0$ such that $f(x) > M$ whenever $a < x < a + \delta$ then we say $f(x) \to \infty$ as $x \to a^+$ and write $\displaystyle\lim_{x \to a^+} f(x) = \infty$
- Likewise, if for each $M > 0$ there exists $\delta > 0$ such that $f(x) > M$ whenever $a - \delta < x < a$ then we say $f(x) \to \infty$ as $x \to a^-$ and write $\displaystyle\lim_{x \to a^-} f(x) = \infty$.

One satisfying aspect of carefully defining divergent limits is that we can give a concrete definition of a vertical asymptote. In fact, we should pause and note that we now have a non-graphical method of distinguishing between vertical asymptotes, holes in the graph and jump-discontinuities of a function. All three can arise from formulas which fail if evaluated at the point in question. The concept of a limit helps us to carefully distinguish what algebra alone cannot hope to detect.

Definition 9.1.6. *vertical asymptotes (VA), holes and jumps.*

Let f be a function and $a \in \mathbb{R}$.

1. We say that f has a **vertical asymptote** $x = a$ if and only if either of the left or right limits diverge to $\pm\infty$. That is, $x = a$ is a VA if and only if $\lim_{x \to a^\pm} f(x) = \pm\infty$.
2. We say that f has a **hole in the graph** at (a, L) iff $a \notin dom(f)$ and $\lim_{x \to a} f(x) = L$
3. We say that f has a **finite jump-discontinuity** at $x = a$ if and only if both the left and right limits of $f(x)$ exist in $\mathbb{R}$ and do not agree; $\lim_{x \to a^+} f(x) = L_+ \in \mathbb{R}$ and $\lim_{x \to a^-} f(x) = L_-$ and $L_+ \neq L_-$.

The behavior a function for $x >> 0$ or for $x << 0$ is captured by the limit of the function at $\pm\infty$,

Definition 9.1.7. *limits at ∞ or $-\infty$.*

> We say $\lim\limits_{x\to\infty} f(x) = L$ if and only if for each $\varepsilon > 0$ there exists $N \in \mathbb{R}$ with $N > 0$ such that if $x > N$ then $|f(x) - L| < \varepsilon$. Likewise, $\lim\limits_{x\to-\infty} f(x) = L$ if and only if for each $\varepsilon > 0$ there exists $M \in \mathbb{R}$ with $M < 0$ such that if $x < M$ then $|f(x) - L| < \varepsilon$.

Definition 9.1.8. *horizontal asymptotes.*

> If $\lim_{x\to\infty} f(x) = L$ then the function f is said to have a **horizontal asymptote of $y = L$ at** ∞. If $\lim_{x\to-\infty} f(x) = L$ then the function f is said to have a **horizontal asymptote of $y = L$ at** $-\infty$.

Vertical asymptotes of the function correspond to horizontal asymptotes for the inverse function. We can also discuss limits which go to infinity at infinity. It's just the natural merger of both definitions but I state it here for completeness.

Definition 9.1.9. *infinite limits at infinity.*

> The limit at ∞ for a function f is ∞ iff for each $M > 0$ there exists $N > 0$ such that for $x > N$ we find $f(x) > M$. We denote $\lim\limits_{x\to\infty} f(x) = \infty$ in this case. Likewise, the limit at $-\infty$ for a function f is ∞ iff for each $M > 0$ there exists $N < 0$ such that if $x < N$ then $f(x) > M$. We denote this by $\lim\limits_{x\to-\infty} f(x) = \infty$. Similarly, if for each $M < 0$ there exists $N > 0$ such that $x > N$ implies $f(x) < M$ we say $\lim\limits_{x\to-\infty} f(x) = -\infty$. Finally, if for each $M < 0$ there exists $N < 0$ such that $x < N$ implies $f(x) < M$ we say $\lim\limits_{x\to-\infty} f(x) = -\infty$.

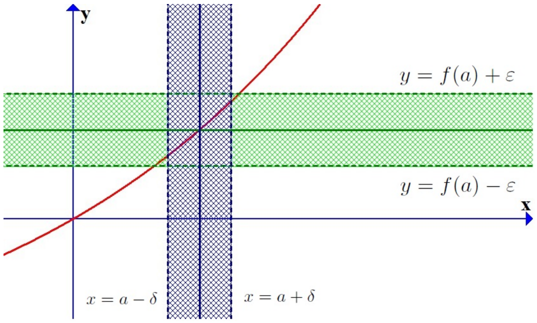
9.1.2 continuity of functions

Definition 9.1.10. *continuity.*

> Let f be a function and $a \in dom(f)$ then f is **continuous at** a if and only if for each $\varepsilon > 0$ there exists $\delta > 0$ for which $|x - a| < \delta$ implies $|f(x) - f(a)| < \varepsilon$. If f is continuous for each $x \in U$ then f is **continuous on** U. If f is continuous on its domain then f is **continuous**.

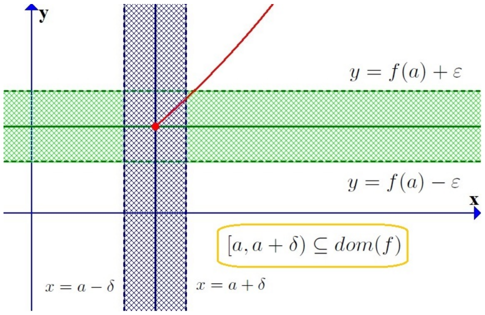
Let us picture the different cases which the above definition captures.

1. If there exists $\eta > 0$ for which $B_\eta(a) \subseteq dom(f)$ then continuity of f at a implies for each $\pm\varepsilon$-band centered about $y = f(a)$ we can select the blue $\pm\delta$-band centered at $x = a$ for which the outputs of f fit within the pictured green band:



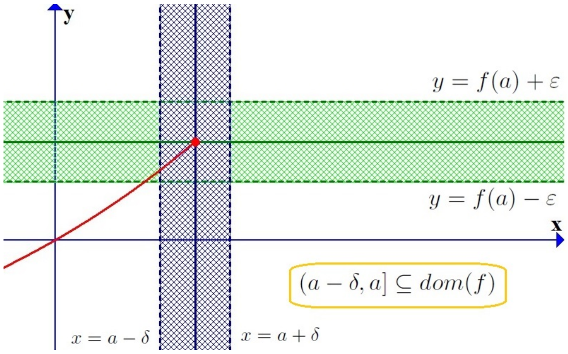
We should recognize that $\lim\limits_{x \to a} f(x) = f(a)$.

2. If $a \in dom(f)$ is a **left boundary point** of $dom(f)$ the continuity of f at $x = a$ indicates for each $\pm\varepsilon$-band about $y = f(a)$ there exists a blue $\pm\delta$-band about $x = a$ whose intersection with $dom(f)$ returns values for $f(x)$ which fit within the green band:



In this case we have $\lim\limits_{x \to a^-} f(x) = f(a)$.

3. If $a \in dom(f)$ is a **right boundary point** of $dom(f)$ the continuity of f at $x = a$ indicates for each $\pm\varepsilon$-band about $y = f(a)$ there exists a blue $\pm\delta$-band about $x = a$ whose intersection with $dom(f)$ returns values for $f(x)$ which fit within the green band:



In this case we have $\lim\limits_{x \to a^+} f(x) = f(a)$.

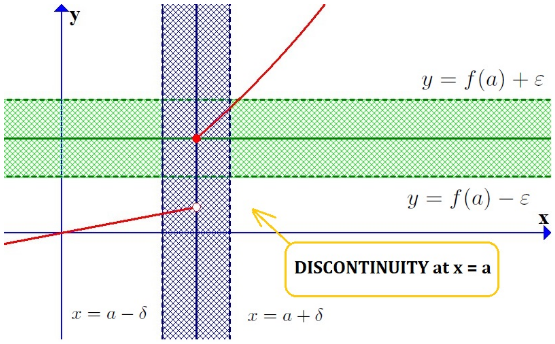
In summary, a function is continuous at $x = a$ if and only if the limit of the function as x approaches a within $dom(f)$ is given by evaluating f at $x = a$.

Theorem 9.1.11. *Characterizing continuity via limits: f is continuous at $a \in dom(f)$ if*

1. *$a \in int(dom(f))$ and $\lim_{x \to a} f(x) = f(a)$.*
2. *a is a left boundary point and $\lim_{x \to a^+} f(x) = f(a)$.*
3. *a is a right boundary point and $\lim_{x \to a^-} f(x) = f(a)$.*
4. *a is an isolated point in $dom(f)$.*

Another useful visualization is given below.

4. If we find a single $\pm\varepsilon$-band centered about $y = f(a)$ fow which it is impossible to contain the values $y = f(x)$ for $x \in (a - \delta, a + \delta)$ then this shows that $\lim_{x \to a} f(x)$ does not exist. For example:



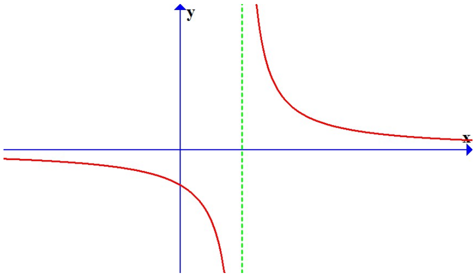
Discontinuity can also arise from just a single point moving off the graph. The key idea is that continuous functions have graphs where the values adhere to one another locally. However, logically, our definition also means sequences are continuous since the continuity criterion is automatically satisfied at isolated points. Every point in the domain of a sequence is isolated.

I should caution the reader who remembers the definition of continuity from their previous course work. Often in precalculus the description of a continuous function is give by the following slogan:

> *A continuous function is one whose graph is drawn without lifting your pen.*

Unfortunately, this slogan does not work unless the domain of the function is **connected**. If the domain is not connected then graph of the function is likewise disconnected.

For example, consider $f(x) = \frac{1}{x}$ the graph $y = \frac{1}{x}$ cannot be drawn unless we lift our pen at the vertical asymptote $x = 0$:



Notice that $dom(f) = (-\infty, 0) \cup (0, \infty)$ and for $a \neq 0$ we have $\lim_{x \to a} \frac{1}{x} = \frac{1}{a}$. Thus f is continuous at each point in its domain. Hence f is a continuous function.

9.2 limit proofs

Theorem 9.2.1. *two-sided limit holds if and only if both left and right limits hold.*

Let f be a function with interior limit point a. Let $L \in \mathbb{R}$,

$$\lim_{x \to a} f(x) = L \qquad \Leftrightarrow \qquad \left\{ \lim_{x \to a^+} f(x) = L \quad \text{and} \quad \lim_{x \to a^-} f(x) = L \right\}$$

Proof: to prove $\Leftrightarrow$ we must show both $\Rightarrow$ and $\Leftarrow$.

($\Rightarrow$) Begin by assuming $\lim_{x\to a} f(x) = L$ then for each $\varepsilon > 0$ there exists $\delta > 0$ such that $0 < |x-a| < \delta$ implies $|f(x) - L| < \varepsilon$. Note for each $\varepsilon > 0$ that if $0 < x - a < \delta$ it follows $0 < |x-a| < \delta$ so $|f(x) - L| < \varepsilon$ hence $\lim_{x\to a^+} f(x) = L$. Likewise, note for each $\varepsilon > 0$ that if $-\delta < x - a < 0$ it follows $0 < |x-a| < \delta$ so $|f(x) - L| < \varepsilon$ hence $\lim_{x\to a^-} f(x) = L$.

($\Leftarrow$) We assume that both $\lim_{x\to a^+} f(x) = L$ and $\lim_{x\to a^-} f(x) = L$. Let $\varepsilon > 0$ and choose $\delta = min(\delta_+, \delta_-)$ where we use the givens to choose $\delta_+, \delta_- > 0$ such that

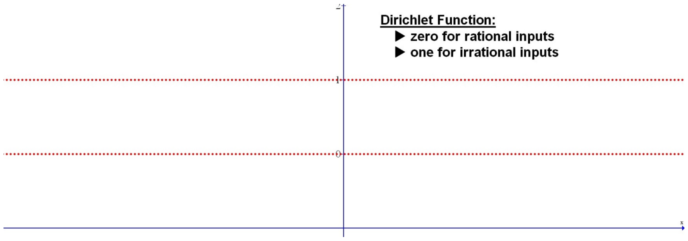
1. $0 < x - a < \delta_+$ implies $|f(x) - L| < \varepsilon$,
2. $-\delta_- < x - a < 0$ implies $|f(x) - L| < \varepsilon$

Therefore, if $x \in \mathbb{R}$ such that $0 < |x-a| < \delta \leq \delta_+, \delta_-$ then either $0 < x - a < \delta < \delta_+$ or $-\delta_- < -\delta < x - a < 0$ so by (1.) or (2.) it follows $|f(x) - L| < \varepsilon$. Therefore, the two-sided limit exists and $f(x) \to L$ as $x \to a$. $\square$.

Half the reason I include this proof is to get the math majors thinking about how to unfold the logic of the symbol $\Leftrightarrow$.

Limits work out well until mathematicians do weird stuff. For example, the function below has domain $\mathbb{R}$ hence every point is a limit point for the function, yet, there is not even one point where the limit exists.

Example 9.2.2. *The* **Dirichlet function***;* $f(x) = \begin{cases} 1 & if\ x \in \mathbb{Q} \\ 0 & if\ x \in \mathbb{J} = \mathbb{R} - \mathbb{Q} \end{cases}$. *The best I can do to the limit of the resolution is as follows:*



This function misbehaves! Think about $f(x) \to L$ as $x \to 0$. Should we expect that $L = 1$ or $L = -1$? No matter how close you get to $x = 0$ there are both rational and irrational numbers closer to $x = 0$.

9.2.1 proofs from the definition

Example 9.2.3. Problem: prove $\lim\limits_{x\to 2}(3x+2) = 8$ via the $\varepsilon\delta$-definition of the limit.

Preparatory calculations: *We need to show that $|x-2| < \delta$ implies $|f(x) - L| < \varepsilon$ for $f(x) = 3x+2$ and $L = 8$ and a particular choice of δ. Consider then*

$$|f(x) - L| = |3x + 2 - 8| = |3x - 6| = |3(x-2)| = 3|x-2| < 3\delta = \varepsilon.$$

So, we should choose $\delta = \varepsilon/3$ since $\varepsilon > 0$ it is clear that $\delta = \varepsilon/3 > 0$. In view of these calculations we are ready to state the proof.

Proof: *Let* $\varepsilon > 0$ *and choose* $\delta = \varepsilon/3$. *Suppose* $x \in \mathbb{R}$ *such that* $0 < |x-2| < \delta$. *Observe that*

$$|3x + 2 - 8| = |3(x-2)| = 3|x-2| < 3\delta = \varepsilon.$$

Thus $0 < |x-2| < \delta$ *implies* $|3x+2-8| < \varepsilon$ *and it follows by the definition of the limit that* $\lim\limits_{x\to 2}(3x+2) = 8$. □

Students sometimes ask me which part is the answer. My answer is that the whole proof is the answer. It is important that it contains all the proper logical statements put in the logical order. Basically, a "proof" is simply a complete explanation of why some statement is true. I will admit there is ambiguity as to what constitutes a "complete" proof in general.

Example 9.2.4. Problem: prove $\lim\limits_{x\to 3}(2-x) = -1$ **via the** $\varepsilon\delta$**-definition of the limit**.

Preparatory calculations: *We need to show that* $|x-3| < \delta$ *implies* $|f(x)-L| < \varepsilon$ *for* $f(x) = 2-x$ *and* $L = -1$ *and a particular choice of* δ. *Consider then*

$$|f(x) - L| = |2 - x - (-1)| = |-x+3| = |-1(x-3)| = |x-3| < \delta = \varepsilon.$$

So, we should choose $\delta = \varepsilon$.

Proof: *Let* $\varepsilon > 0$ *and choose* $\delta = \varepsilon$. *Suppose* $x \in \mathbb{R}$ *such that* $0 < |x-3| < \delta$. *Observe that*

$$|2 - x - (-1)| = |-x+3)| = |x-3| < \delta = \varepsilon.$$

Thus $0 < |x-3| < \delta$ *implies* $|2-x-(-1)| < \varepsilon$ *and it follows by the definition of the limit that* $\lim\limits_{x\to 3}(2-x) = -1$. □

Example 9.2.5. Problem: prove $\lim\limits_{x\to 0}(x^2) = 0$ **via the** $\varepsilon\delta$**-definition of the limit**.

Preparatory calculations: *We need to show that* $|x-0| < \delta$ *implies* $|f(x)-L| < \varepsilon$ *for* $f(x) = x^2$ *and* $L = 0$ *and a particular choice of* δ. *Consider then*

$$|f(x) - L| = |x^2 - 0| = |x|^2 < \delta^2 = \varepsilon.$$

So, we should choose $\delta = \sqrt{\varepsilon}$. *Since* $\varepsilon > 0$ *we can be assured that the squareroot gives* $\delta > 0$.

Proof: *Let* $\varepsilon > 0$ *and choose* $\delta = \sqrt{\varepsilon}$. *Suppose* $x \in \mathbb{R}$ *such that* $0 < |x-0| < \delta$. *Observe that*

$$|x^2 - 0| = |x|^2 < (\sqrt{\varepsilon})^2 = \varepsilon.$$

Thus $0 < |x-0| < \delta$ *implies* $|x^2 - 0| < \varepsilon$ *and it follows by the definition of the limit that* $\lim_{x\to 0}(x^2) = 0$. □

Example 9.2.6. Problem: prove $\lim\limits_{x\to 3}(x^2) = 9$ **via the** $\varepsilon\delta$**-definition of the limit**.

Preparatory calculations: *We need to show that* $|x-3| < \delta$ *implies* $|f(x)-L| < \varepsilon$ *for* $f(x) = x^2$ *and* $L = 9$ *and a particular choice of* δ. *Consider then*

$$|f(x) - L| = |x^2 - 9| = |(x-3)(x+3)| < \delta|x+3|$$

Ok, so $|x+3|$ is annoying. But, have no fear, we control the δ. Note that $0 < |x-3| < \delta$ gives $3-\delta < x < 3+\delta$ so $6-\delta < x+3 < 6+\delta$. Suppose $\delta < 1$ then we certainly have that $5 < x+3 < 7$ which gives $-7 < 5 < x+3 < 7$ so $|x+3| < 7$ which is very nice because, given our assumption $\delta < 1$ we find:

$$|f(x) - L| =< \delta|x+3| < 7\delta.$$

now the choice should be clear, we use $\delta = \varepsilon/7$. However, we do need that $\varepsilon/7 < 1$, remember we don't control ε, all we know is that $\varepsilon > 0$. The solution is simple, to be careful about the possibility of large ε we choose $\delta = min(\varepsilon/7, 1)$. If $\delta = 1$ then we still find $|x+3| \leq 7$ and so $|f(x)-L| \leq 7\delta < \varepsilon$ provide that $\delta = min(\varepsilon/7, 1)$ so we knew $\delta < \varepsilon/7$ hence $7\delta < \varepsilon$.

Proof: *Let $\varepsilon > 0$ and choose $\delta = min(\varepsilon/7, 1)$. Suppose $x \in \mathbb{R}$ such that $0 < |x-3| < \delta$. Observe that $\delta \leq 1$ thus $0 < |x-3| < \delta \leq 1$ yields $-1 \leq x-3 \leq 1$ from which it follows $5 < x+3 \leq 7$ hence $-7 < x+3 \leq 7$ so $|x+3| \leq 7$. Therefore,*

$$|x^2 - 9| = |(x-3)(x+3)| = |x-3||x+3| < \delta|x+3| < 7\delta$$

Moreover, as $\delta \leq \varepsilon/7$ we have $7\delta \leq \varepsilon$. Thus, $0 < |x-3| < \delta$ implies that $|x^2 - 9| < \varepsilon$ and it follows by the definition of the limit that $\lim_{x\to 3}(x^2) = 9$. □

Sometimes we are called upon to calculate a limit which has an arbitrary limit point. In the example below the limit point is denoted by "a". We must make arguments which hold for all possible values of a since no particular restriction on a is offered.

Example 9.2.7. Problem: prove $\lim_{x\to a}(3x+2) = 3a+2$ via the $\varepsilon\delta$-definition of the limit.

Preparatory calculations: *We need to show that $|x-a| < \delta$ implies $|f(x) - L| < \varepsilon$ for $f(x) = 3x+2$ and $L = 3a+2$ and a particular choice of δ. Consider then*

$$|f(x) - L| = |3x+2-(3a+2)| = |3(x-a)| = 3|x-a| < 3\delta = \varepsilon.$$

So, we should choose $\delta = \varepsilon/3$ since $\varepsilon > 0$ it is clear that $\delta = \varepsilon/3 > 0$. In view of these calculations we are ready to state the proof.

Proof: *Let $\varepsilon > 0$ and choose $\delta = \varepsilon/3$. Suppose $x \in \mathbb{R}$ such that $0 < |x-a| < \delta$. Observe that*

$$|3x+2-(3a+2)| = |3(x-a)| = 3|x-a| < 3\delta = \varepsilon.$$

Thus $0 < |x-a| < \delta$ implies $|3x+2-(3a+2)| < \varepsilon$ and it follows by the definition of the limit that $\lim_{x\to a}(3x+2) = 3a+2$. □

Example 9.2.8. Problem: prove $\lim_{x\to 1^+}(\sqrt{x-1}) = 0$ via the $\varepsilon\delta$-definition of the limit.

Preparatory calculations: *We need to show that $1 < x < 1+\delta$ implies $|f(x) - L| < \varepsilon$ for $f(x) = \sqrt{x-1}$ and $L = 0$ and a particular choice of δ. Consider then*

$$|f(x) - L| = |\sqrt{x-1} - 0| = |\sqrt{x-1}| = \sqrt{|x-1|}.$$

where we used $1 < x < 1+\delta$ to deduce $0 < x-1$ hence $|x-1| = x-1$. We should choose $\delta = \varepsilon^2$.

Proof: *Let $\varepsilon > 0$ and choose $\delta = \varepsilon^2$. Suppose $x \in \mathbb{R}$ such that $0 < x - 1 < \delta$. Observe that*

$$|\sqrt{x-1}| = \sqrt{|x-1|} < \sqrt{\delta} = \sqrt{\varepsilon^2} = \varepsilon.$$

Thus $0 < x - 1 < \delta$ implies $|\sqrt{x-1}| < \varepsilon$ and it follows by the definition of the right-sided limit that $\lim\limits_{x \to 1^+} \sqrt{x-1} = 0$. □

Notice $f(x) = \sqrt{x-1}$ has $dom(f) = [1, \infty)$ and $x = 1$ is the boundary point of the domain. The two-sided limit is not defined at one because the function is not real-valued for $x < 1$.

Example 9.2.9. Problem: prove $\lim_{x \to 0} \frac{1}{x} \notin \mathbb{R}$ via the $\varepsilon\delta$-definition of the limit.

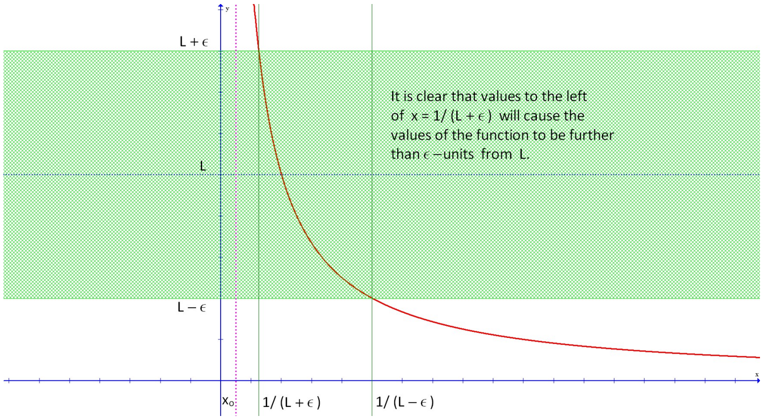
Preparatory calculations: *think about it. What do we need to show to show it is impossible for any real number to be the limit of $\frac{1}{x}$ as $x \to 0$?. By the proposition we just proved it would suffice to show that the right-limit failed to exist no matter what our choice of L is. Let's proceed from that angle. We want to show that $\lim_{x \to 0^+} \frac{1}{x}$ cannot be a real number. The natural thing to try here is contradiction, we suppose that there does exist $L \in \mathbb{R}$ such that $\lim_{x \to 0^+} \frac{1}{x} = L$ and then we hunt for something insane. Once we find the insanity we see that believing in the existence of $L \in \mathbb{R}$ is madness so we can safely assume $L \notin \mathbb{R}$. This is the outline of the logic. Let's get into the details:*

Proof: *assume that $L \in \mathbb{R}$ such that $\frac{1}{x} \to L$ as $x \to 0^+$. This means that for each $\varepsilon > 0$ there exists $\delta > 0$ such that $0 < x < \delta$ implies $\left|\frac{1}{x} - L\right| < \varepsilon$. We seek a contradiction, suppose $\varepsilon = L$ and let $\delta > 0$ be some number such that all $x \in \mathbb{R}$ satisfying $0 < x < \delta$ force $\left|\frac{1}{x} - L\right| < \varepsilon$. Define $x_o = min\left(\frac{1}{2(L+\varepsilon)}, \frac{\delta}{2}\right)$ thus $x_o \leq \frac{1}{2(L+\varepsilon)}$ and $x_o < \delta$. Clearly $0 < x_o < \delta$ so it follows that*

$$-\varepsilon < \frac{1}{x_o} - L < \varepsilon$$

and as $\varepsilon = L$ we add ε to find $0 < \frac{1}{x_o} < 2\varepsilon$. On the other hand, we have constructed x_o to satisfy the inequality $x_o \leq \frac{1}{2(L+\varepsilon)} = \frac{1}{4\varepsilon}$ thus $\frac{1}{x_o} \geq 4\varepsilon$. But, this is a contradiction since we cannot have both $\frac{1}{x_o} < 2\varepsilon$ and $\frac{1}{x_o} \geq 4\varepsilon$. Therefore, be proof by contradiction, there does not exist such an $L \in \mathbb{R}$ and we conclude that the $\lim_{x \to 0^+} \frac{1}{x}$ does not exist, hence $\lim_{x \to 0} \frac{1}{x}$ does not exist. These limits **diverge**. □

If you're wondering how I thought of the argument in the last example then perhaps the following picture will help you understand why I chose x_o as I did. In fact, the picture is what I used to think of the proof. Pictures are often helpful, you ought not forget that graphing can be a powerful tool for analysis.



Example 9.2.10. Problem: prove $\lim_{x\to 0^+} \frac{1}{x} = \infty$..

Preparatory calculations: *we need to find δ such that $M > \frac{1}{x}$ for all $x \in \mathbb{R}$ such that $0 < x < \delta$. Note $M > \frac{1}{x}$ implies $\frac{1}{M} < x$. Looks like $\delta = \frac{1}{2M}$ will do nicely.*

Proof: *suppose $M > 0$ and let $\delta = \frac{1}{2M}$. If $0 < x < \delta = \frac{1}{2M}$ then $\frac{1}{x} > 2M > M$. Therefore, for each $M > 0$ there exists $\delta > 0$ such that $\frac{1}{x} > M$ whenever $0 < x < \delta$. It follows by definition that $\lim_{x\to 0^+} \frac{1}{x} = \infty$.* □

We learned in Example 9.2.9 this limit does not exist in $\mathbb{R}$. Now we have shown that it actually diverges to ∞. Notice that $\infty \notin \mathbb{R}$, rather, ∞ is simply a notation to indicate a function has a particular behavior at a point.

9.3 limit laws

We assume $a \in \mathbb{R}$ and f, g are functions with limit point a throughout this section unless otherwise explicitly stated. Let us begin by proving a limit has a single value.

Proposition 9.3.1. *limit is unique.*

If $\lim\limits_{x\to a} f(x) = L_1$ and $\lim\limits_{x\to a} f(x) = L_1$ then $L_1 = L_2$.

Proof: let $\varepsilon > 0$. Suppose $\lim\limits_{x\to a} f(x) = L_1$ and $\lim\limits_{x\to a} f(x) = L_1$. Choose $\delta_1 > 0$ for which $0 < |x-a| < \delta_1$ implies $|f(x) - L_1| < \varepsilon/2$. Likewise, choose $\delta_2 > 0$ for which $0 < |x-a| < \delta_2$ implies $|f(x) - L_2| < \varepsilon/2$. Let $\delta = min(\delta_1, \delta_2)$ and suppose $0 < |x-a| < \delta \leq \delta_1, \delta_2$ hence

$$\begin{aligned} |L_1 - L_2| &= |L_1 - f(x) + f(x) - L_2| \\ &\leq |L_1 - f(x)| + |f(x) - L_2| \\ &= |f(x) - L_1| + |f(x) - L_2| \\ &< \varepsilon/2 + \varepsilon/2 = \varepsilon. \end{aligned} \tag{9.1}$$

Thus $|L_1 - L_2| < \varepsilon$ for arbitary $\varepsilon > 0$ and that implies $|L_1 - L_2| = 0$ hence $L_1 = L_2|$. □

Very similar arguments can be used to show right and left limits which exist in $\mathbb{R}$ are unique. It is very amusing that the proof of Proposition 9.3.4 rests on nearly the same calculation as the uniqueness result above.

Proposition 9.3.2. *limit of identity function.*

$$\lim_{x\to a} x = a.$$

Proof: Fix $a \in \mathbb{R}$. Let $f(x) = x$ for all $x \in \mathbb{R}$. Let $\varepsilon > 0$ and choose $\delta = \varepsilon$. If $0 < |x-a| < \delta$ then $|f(x) - a| = |x - a| < \varepsilon$ thus $\lim_{x\to a} f(x) = a$ which is to say $\lim_{x\to a} x = a$. □

Proposition 9.3.3. *limit of constant function.*

$$\lim_{x\to a} c = c.$$

Proof: Fix $a \in \mathbb{R}$ and define $f(x) = c$ for all $x \in \mathbb{R}$. Suppose $\varepsilon > 0$ and choose $\delta = 42$. If $x \in \mathbb{R}$ with $0 < |x-a| < 42$ then $|f(x) - c| = |c - c| = 0 < \varepsilon$ thus $\lim_{x \to a} f(x) = c$ by the definition of the limit. Thus $\lim_{x\to a} c = c$. □

Proposition 9.3.4. *additivity of the limit.*

Suppose $\lim_{x\to a} f(x) = L_f \in \mathbb{R}$ and $\lim_{x \to a} g(x) = L_g \in \mathbb{R}$ then

$$\lim_{x\to a}[f(x) + g(x)] = \lim_{x\to a} f(x) + \lim_{x \to a} g(x).$$

Proof: we are given that $\lim\limits_{x\to a} f(x) = L_f$ and $\lim\limits_{x \to a} g(x) = L_g$. Let $\varepsilon > 0$ and choose $\delta_f > 0$ such that $0 < |x-a| < \delta_f$ implies $|f(x) - L_f| < \frac{\varepsilon}{2}$. Likewise, choose $\delta_g > 0$ for which $0 < |x - a| < \delta_g$ implies $|g(x) - L_g| < \frac{\varepsilon}{2}$. Let $\delta = min(\delta_f, \delta_g)$ then $\delta \leq \delta_f$ and $\delta \leq \delta_g$. Suppose $x \in \mathbb{R}$ and $0 < |x - a| < \delta$ then $|f(x) - L_f| < \frac{\varepsilon}{2}$ and $|g(x) - L_g| < \frac{\varepsilon}{2}$. Consider that

$$\begin{aligned} |f(x) + g(x) - (L_f + L_g)| &= |f(x) - L_f + g(x) - L_g| \\ &\leq |f(x) - L_f| + |g(x) - L_g| \\ &< \varepsilon/2 + \varepsilon/2 = \varepsilon. \end{aligned} \tag{9.2}$$

Therefore, by the definition of the limit, $\lim\limits_{x\to a}[f(x) + g(x)] = \lim\limits_{x\to a} f(x) + \lim\limits_{x\to a} g(x)$. □.

Proposition 9.3.5. *homogeneity of the limit.*

Suppose $c \in \mathbb{R}$ and $\lim_{x\to a} f(x) = L \in \mathbb{R}$ then $\lim\limits_{x\to a} cf(x) = c \lim\limits_{x\to a} f(x)$.

Proof: Suppose $c \in \mathbb{R}$ and $\lim_{x\to a} f(x) = L \in \mathbb{R}$. Let $\varepsilon > 0$. If $c \neq 0$ then choose $\delta > 0$ for which $0 < |x - a| < \delta$ implies $|f(x) - L| < \frac{\varepsilon}{|c|}$. Observe

$$|cf(x) - cL| = |c||f(x) - L| < |c|\frac{\varepsilon}{|c|} = \varepsilon \tag{9.3}$$

If $c = 0$ then $|cf(x) - cL| = 0 < \varepsilon$ for all $x \in dom(f)$. Thus, by the definition of the limit, $\lim\limits_{x\to a} cf(x) = c \lim\limits_{x\to a} f(x)$. □

I often collectively refer to the previous two theorems as the *linearity* of the limit. In calculus we will learn that most major constructions obey the linearity rules. We can also extend the rules to give the limit law for a finite linear combination of convergent functions.

Proposition 9.3.6. *limit of linear combination of convergent functions.*

Suppose $a \in \mathbb{R}$ and $f_i(x) \to L_i \in \mathbb{R}$ as $x \to a$ for $i = 1, 2, \dots, n$. Then,

$$\lim_{x\to a}\left(c_1f_1(x) + c_2f_2(x) + \cdots + c_nf_n(x)\right) = c_1\lim_{x\to a} f_1(x) + c_2\lim_{x\to a} f_2(x) + \cdots + c_n\lim_{x\to a} f_n(x).$$

Proof: Suppose $f_i(x) \to L_i \in \mathbb{R}$ as $x \to a$ for $i = 1, 2, \dots, n$. We claim

$$\lim_{x\to a}\left(c_1f_1(x) + c_2f_2(x) + \cdots + c_nf_n(x)\right) = c_1\lim_{x\to a} f_1(x) + c_2\lim_{x\to a} f_2(x) + \cdots + c_n\lim_{x\to a} f_n(x)$$

for all $n \in \mathbb{N}$. We will prove this claim by induction on n. Notice the claim is true for $n = 1$ since Proposition 9.3.5 provides that $\lim\limits_{x\to a}(c_1 f_1(x)) = c_1 \lim\limits_{x\to a} f_1(x)$. Inductively suppose the claim is true for some $n \in \mathbb{N}$. Consider the linear combination of $n+1$ functions,

$$\begin{aligned}
&\lim_{x\to a}\big(c_1 f_1(x) + c_2 f_2(x) + \cdots + c_n f_n(x) + c_{n+1} f_{n+1}(x)\big) = \\
&\qquad = \lim_{x\to a}\big(c_1 f_1(x) + c_2 f_2(x) + \cdots + c_n f_n(x)\big) + \lim_{x\to a}\big(c_{n+1} f_{n+1}(x)\big) && (9.4)\\
&\qquad = c_1 \lim_{x\to a} f_1(x) + c_2 \lim_{x\to a} f_2(x) + \cdots + c_n \lim_{x\to a} f_n(x) + c_{n+1} \lim_{x\to a} f_{n+1}(x) && (9.5)
\end{aligned}$$

We used Proposition 9.3.4 for Equation 9.4 and we applied the induction hypothesis and Proposition 9.3.5 for Equation 9.5. Thus we have shown the claim holds for $n+1$ and it follows the result is true for all $n \in \mathbb{N}$ by induction on n. $\square$

Proposition 9.3.7. *limit of product is product of limits.*

If $\lim_{x\to a} f(x) = L_f \in \mathbb{R}$ and $\lim_{x\to a} g(x) = L_g \in \mathbb{R}$ then

$$\lim_{x\to a}[f(x)g(x)] = \left(\lim_{x\to a} f(x)\right)\left(\lim_{x\to a} g(x)\right).$$

Preparing for Proof: Consider that we wish to find $\delta > 0$ that forces $x \in B_\delta(a)_o$ to satisfy

$$|f(x)g(x) - L_f L_g| < \varepsilon \tag{9.6}$$

we have control over $|f(x) - L_f|$ and $|g(x) - L_g|$. If we can somehow factor these out then we have something to work with. Add and subtract $L_f g(x)$ towards that goal:

$$\begin{aligned}
|f(x)g(x) - L_f L_g| &= |f(x)g(x) - L_f g(x) + L_f g(x) - L_f L_g| && (9.7)\\
&\le |f(x) - L_f||g(x)| + |L_f||g(x) - L_g|
\end{aligned}$$

Proof: let $\varepsilon > 0$ and suppose $f(x) \to L_f$ and $g(x) \to L_g$ as $x \to a$. Observe we may select positive constants δ_1, δ_2 and δ_3 for which:

(i.) $0 < |x - a| < \delta_1$ implies $|f(x) - L_f| < \dfrac{\varepsilon}{2(1 + |L_g|)}$,

(ii.) $0 < |x - a| < \delta_2$ implies $|g(x) - L_g| < \dfrac{\varepsilon}{2(1 + |L_f|)}$,

(iii.) $0 < |x - a| < \delta_3$ implies $|g(x) - L_g| < 1$.

Observe, from (iii.) we also have the bound below:

$$|g(x)| = |g(x) - L_g + L_g| \le |g(x) - L_g| + |L_g| < 1 + |L_g| \tag{9.8}$$

Let $\delta = \min(\delta_1, \delta_2, \delta_3)$ and suppose $0 < |x - a| < \delta$ thus (i.), (ii.) and (iii.) hold true and $|g(x)| < 1 + |L_g|$. Thus calculate:

$$\begin{aligned}
|f(x)g(x) - L_f L_g| &= |f(x)g(x) - L_f g(x) + L_f g(x) - L_f L_g| && (9.9)\\
&\le |f(x) - L_f||g(x)| + |L_f||g(x) - L_g| \\
&\le \frac{\varepsilon}{2(1 + |L_g|)}(1 + |L_g|) + |L_f|\frac{\varepsilon}{2(1 + |L_f|)} \\
&< \varepsilon
\end{aligned}$$

where the last inequality stems from the observation that $|L_f|/(1+|L_f|) < 1$. Therefore, we have shown $f(x)g(x) \to L_f L_g$ as $x \to a$ and this completes the proof. □

The proof given above is fairly standard. I found the argument in this Wikibook.

Proposition 9.3.8. *power function limit (for powers $n \in \mathbb{N}$).*

Let $a \in \mathbb{R}$ and $n \in \mathbb{N} \cup \{0\}$, $\lim_{x\to a} x^n = a^n$.

Proof: is by induction on n. Observe $n = 0$ is true by Proposition 9.3.3. Inductively suppose $\lim\limits_{x\to a} x^n = a^n$ for some $n \in \mathbb{N}$. Consider the $(n+1)$ case,

$$\lim_{x\to a} x^{n+1} = \lim_{x\to a} x^n x = \left(\lim_{x\to a} x^n\right)\left(\lim_{x\to a} x\right) = a^n a = a^{n+1}$$

where I used the Proposition 9.3.7 based on the induction hypothesis and Proposition 9.3.2. We find the statement true for n implies it is likewise true for $n+1$ hence the theorem is true for all $n \in \mathbb{N}$ by proof by mathematical induction. □

Proposition 9.3.9. *polynomial function limit.*

Suppose $c_n, \dots, c_1, c_0 \in \mathbb{R}$ and $p(x) = c_n x^n + \cdots + c_1 x + c_0$ then $\lim\limits_{x\to a} p(x) = p(a)$.

Proof: by Proposition 9.3.8 we note $f_i(x) = x^i$ has $\lim\limits_{x\to a} f_i(x) = a^i$ for $i = 0, 1, 2, \dots, n$. Changing numbering slightly on Proposition 9.3.6 with $f_i(x) = x^i$ for $i = 0, 1, \dots, n$ we obtain:

$$\lim_{x\to a} (c_n x^n + \cdots + c_1 x + c_0) = c_n a^n + \cdots + c_1 a + c_0 = p(a). \quad \square$$

Proposition 9.3.10. *limit of composite. Suppose f has limit point a and g has limit point L_1,*

If $\lim\limits_{x\to a} f(x) = L_1$ and $\lim\limits_{y\to L_1} g(y) = L_2$ then $\lim_{x\to a} g(f(x)) = L_2$.

Proof: let $\varepsilon > 0$. Since $\lim_{y\to L_1} g(y) = L_2$ we may choose $\delta_g > 0$ such that $0 < |y - L_1| < \delta_g$ implies $|g(y) - L_2| < \varepsilon$. Likewise, since $\lim\limits_{x\to a} f(x) = L_1$ we may select $\delta_f > 0$ for which $0 < |x - a| < \delta_f$ implies $|f(x) - L_1| < \delta_g$. Suppose $0 < |x - a| < \delta_f$ and let $y = f(x)$ then $|y - L_1| = |f(x) - L_1| < \delta_g$ hence $|g(y) - L_2| < \varepsilon$. Thus $|g(f(x)) - L_2| < \varepsilon$. Therefore, by definition of limit, $\lim_{x\to a} g(f(x)) = L_2$. □

This proposition can be written without use of L_1 and L_2 but the statement is a bit clunky:

$$\lim_{x\to a} [g(f(x))] = \lim_{y\to \lim_{x\to a} f(x)} [g(y)]. \tag{9.10}$$

Notice the proof and application of the composite limit rule both rest on the substitution $y = f(x)$. When we make the subsitution of $y = f(x)$ we have to swap $f(x)$ for y as we trade $g(f(x))$ for $g(y)$. Likewise, we exchange $x \to a$ for the corresponding limit in y of $y \to \lim_{x\to a} f(x)$.

Proposition 9.3.11. *reciprocal function limit.*

If $a \neq 0$ then $\lim_{x \to a} \frac{1}{x} = \frac{1}{a}$.

Proof: Suppose $a > 0$. Let $\varepsilon > 0$ and choose $\delta = min\left(\frac{a}{2}, \frac{a^2\varepsilon}{2}\right) > 0$. Observe $\delta \leq a/2$ then $|x-a| < \delta \leq \frac{a}{2}$ implies $-\frac{a}{2} < x - a$ hence $\frac{a}{2} < x = |x|$. Therefore, $\frac{1}{|x|} < \frac{2}{a}$. Consequently, if $x \in \mathbb{R}$ with $0 < |x-a| < \delta$ we find:

$$\left|\frac{1}{x} - \frac{1}{a}\right| = \left|\frac{a-x}{ax}\right| = \frac{|x-a|}{a|x|} < \frac{2|x-a|}{a^2} < \frac{2}{a^2}\delta \leq \frac{2}{a^2}\frac{a^2\varepsilon}{2} = \varepsilon. \tag{9.11}$$

Thus, by the definition of the limit, $\displaystyle\lim_{x \to a} \frac{1}{x} = \frac{1}{a}$. The proof in the case $a < 0$ is similar and we leave it as an exercise for the reader. □

Proposition 9.3.12. *limit of quotient is quotient of limits.*

Suppose $\lim_{x \to a} f(x) = L_f \in \mathbb{R}$ and $\lim_{x \to a} g(x) = L_g \in \mathbb{R}$ with $L_g \neq 0$ then

$$\lim_{x \to a} \frac{f(x)}{g(x)} = \frac{\lim_{x \to a} f(x)}{\lim_{x \to a} g(x)}.$$

Proof: Let $h(y) = \frac{1}{y}$ and note Proposition 9.3.11 provides $\lim_{y \to L_g} h(y) = \frac{1}{L_g}$ since $L_g \neq 0$. Furthermore, by Proposition 9.3.10 we find the limit of the composite function $h(g(x)) = \frac{1}{g(x)}$ is given by $\lim_{y \to L_g} h(y) = \frac{1}{L_g}$. Proposition 9.3.7 completes the proof since:

$$\lim_{x \to a} \frac{f(x)}{g(x)} = \lim_{x \to a} \left[f(x) \cdot \frac{1}{g(x)}\right] = \left(\lim_{x \to a} f(x)\right)\left(\lim_{x \to a} \frac{1}{g(x)}\right) = L_f \cdot \frac{1}{L_g} = \frac{\lim_{x \to a} f(x)}{\lim_{x \to a} g(x)}. \ \square$$

Beyond these rules you will find a number of other "limit laws" in various texts. In one way or another they boil down to proving a particular function has a natural limit then you combine that data together with the composite limit law. So, to complete our catalog of basic limit math we ought to calculate limits of the elementary functions.

Proposition 9.3.13. *limit of square root function.*

If $a > 0$ then $\lim_{x \to a} \sqrt{x} = \sqrt{a}$. In addition, $\lim_{x \to 0^+} \sqrt{x} = 0$.

Proof: Notice the following algebraic identity for $a > 0$,

$$\left|\sqrt{x} - \sqrt{a}\right| = \frac{|\sqrt{x} - \sqrt{a}||\sqrt{x} + \sqrt{a}|}{|\sqrt{x} + \sqrt{a}|} = \frac{|(\sqrt{x} - \sqrt{a})(\sqrt{x} + \sqrt{a})|}{|\sqrt{x} + \sqrt{a}|} = \frac{|x-a|}{|\sqrt{x} + \sqrt{a}|} \tag{9.12}$$

Let $\varepsilon > 0$ and choose $\delta = \varepsilon\sqrt{a} > 0$. If $0 < |x-a| < \delta = \varepsilon\sqrt{a}$ then following Equation 9.12 we find

$$\left|\sqrt{x} - \sqrt{a}\right| = \frac{|x-a|}{|\sqrt{x} + \sqrt{a}|} < \frac{|x-a|}{\sqrt{a}} < \frac{\varepsilon\sqrt{a}}{\sqrt{a}} = \varepsilon.$$

Therefore, by the definition of the limit we find $\lim_{x \to a} \sqrt{x} = \sqrt{a}$. We leave the proof of $\lim_{x \to 0^+} \sqrt{x} = 0$ to the reader □

9.4 intermediate value theorem

Proposition 9.4.1.

> Let f be continuous at c such that $f(c) \neq 0$ then there exists $\delta > 0$ such that either $f(x) > 0$ or $f(x) < 0$ for all $x \in (c-\delta, c+\delta)$.

Proof: we are given that $\lim_{x\to c} f(x) = f(a) \neq 0$.

1.) Assume that $f(a) > 0$. Choose $\varepsilon = \frac{f(a)}{2}$ and use existence of the limit $\lim_{x\to c} f(x) = f(a)$ to select $\delta > 0$ such that $0 < |x-c| < \delta$ implies $|f(x) - f(a)| < \frac{f(a)}{2}$ hence $-\frac{f(a)}{2} < f(x) - f(a) < \frac{f(a)}{2}$. Adding $f(a)$ across the inequality yields $0 < \frac{f(a)}{2} < f(x) < \frac{3f(a)}{2}$.

2.) If $f(a) < 0$ then we can choose $\varepsilon = -\frac{f(a)}{2} > 0$ and select $\delta > 0$ such that $0 < |x-c| < \delta$ implies $|f(x) - f(a)| < -\frac{f(a)}{2}$ hence $\frac{f(a)}{2} < f(x) - f(a) < -\frac{f(a)}{2}$. It follows that $\frac{3f(a)}{2} < f(x) < \frac{f(a)}{2} < 0$.

The proposition follows. □

Bolzano understood there was a gap in the arguments of the founders of calculus. Often, theorems like those stated in this section would merely be claimed without proof. The work of Bolzano and others like him ultimately gave rise to the careful rigorous study of the real numbers and more generally the study of *real analysis* [1]

Proposition 9.4.1 is clearly extended to sets which have boundary points. If we know a function is continuous on $[a, b)$ and $f(a) \neq 0$ then we can find $\delta > 0$ such that $f([a, a+\delta)) > 0$. (*This is needed in the proof below in the special case that $c = a$ and a similar comment applies to $c = b$.*)

Theorem 9.4.2. *Bolzano's theorem*

> Let f be continuous on $[a.b]$ such that $f(a)f(b) < 0$ then there exists $c \in (a, b)$ such that $f(c) = 0$.

Proof: suppose $f(a) < f(b)$ then $f(a)f(b) < 0$ implies $f(a) < 0$ and $f(b) > 0$. We can use axiom A11 for the heart of this proof. Our goal is to find a nonempty subset $S \subseteq \mathbb{R}$ which has an upper bound. Axiom A11 will then provides the existence of the least upper bound. We should like to construct a set which has the property desired in this theorem. Define $S = \{x \in [a, b] \mid f(x) < 0\}$. Notice that $a \in S$ since $f(a) < 0$ thus $S \neq \emptyset$. Moreover, it is clear that $x \leq b$ for all $x \in S$ thus S is bounded above. Axiom A11 states that there exists a least upper bound $c \in S$. To say c is the least upper bound means that any other upperbound of S is larger than c.

We now seek to show that $f(c) = 0$. Consider that there exist three possibilities:

1. if $f(c) < 0$ then the continuous function f has $f(c) \neq 0$ so by prop. 9.4.1 there exists $\delta > 0$ such that $x \in (c-\delta, c+\delta) \cap [a, b]$ implies $f(x) < 0$. However, this implies there is a value $x \in [c, c+\delta)$ such that $f(x) < 0$ and $x > c$ which means x is in S and is larger than the upper bound c. Therefore, c is not an upper bound of S. Obviously this is a contradiction therefore $f(c) \not< 0$.

[1] the Bolzano-Weierstrauss theorem is one of the central theorems of real analysis, in 1817 Bolzano used it to prove the IVT. It states every bounded sequence contains a convergent subsequence. Sequences can also be used to formulate limits and continuity. Sequential convergence is dealt with properly in undergraduate real analysis.

2. if $f(c) > 0$ then the continuous function f has $f(c) \neq 0$ so by prop. 9.4.1 there exists $\delta > 0$ such that $x \in (c-\delta, c+\delta) \cap [a,b]$ implies $f(x) > 0$. However, this implies that all values $x \in (c-\delta, c]$ have $f(x) > 0$ and thus $x \notin S$ which means $x = c - \delta/2 < c$ is an upper bound of S which is smaller than the least upper bound c. Therefore, c is not the least upper bound of S. Obviously this is a contradiction therefore $f(c) \not> 0$.

3. if $f(c) = 0$ then no contradiction is found. The theorem follows. □

My proof here essentially follows the argument in CALCULUS, Volume 1 by Apostol[2] However I suspect this argument in one form or another can be found in many serious calculus texts. With Bolzano's theorem settled we can prove the IVT without much difficulty.

(IVT): Suppose that f is continuous on an interval $[a,b]$ with $f(a) \neq f(b)$ and let N be a number such that N is between $f(a)$ and $f(b)$ then there exists $c \in (a,b)$ such that $f(c) = N$.

Proof: let N be as described above and define $g(x) = f(x) - N$. Note that g is clearly continuous. Suppose that $f(a) < f(b)$ then we must have $f(a) < N < f(b)$ which gives $f(a) - N \leq 0 \leq f(b) - N$ hence $g(a) < 0 < g(b)$. Applying Bolzano's theorem to g gives $c \in (a,b)$ such that $g(c) = 0$. But, $g(c) = f(c) - N = 0$ therefore $f(c) = N$. If $f(a) > f(b)$ then a similar argument applies. □.

9.5 application of mean value theorem

The following theorem should be proved in Calculus I. Let me state it for reference.

Proposition 9.5.1. *Mean Value Theorem (MVT).*

Suppose that f is a function such that

1. f is continuous on $[a,b]$,
2. f is differentiable on (a,b),

Then there exists $c \in (a,b)$ such that $f'(c) = \frac{f(b)-f(a)}{b-a}$. That is, there exists $c \in (a,b)$ such that $f(b) - f(a) = f'(c)(b-a)$.

Proposition 9.5.2. *sign of the derivative function f' indicates strict increase or decrease of f.*

Suppose that f is a function and J is a connected subset of $dom(f)$

1. if $f'(x) > 0$ for all $x \in J$ then f is strictly increasing on J
2. if $f'(x) < 0$ for all $x \in J$ then f is strictly decreasing on J.

Proof: suppose $f'(x) > 0$ for all $x \in J$. Let $[a,b] \subseteq J$ and note f is continuous on $[a,b]$ since it is given to be differentiable on a superset of $[a,b]$. The MVT applied to f with respect to $[a,b]$

[2] CALCULUS Volumes 1 and 2 are a worthy resource for any math major, I highly recomend reading them as a follow-up to calculus. Those volumes capture a time when we were much more serious about math at the undergraduate level. Much of the rest of the world still uses Apostol for the text in the university calculus course. International editions of the text are inexpensive and a pdf is freely available online.

implies there exists $c \in [a,b]$ such that

$$\frac{f(b)-f(a)}{b-a} = f'(c).$$

Notice that $f(b)-f(a) = (b-a)f'(c)$ but $b-a > 0$ and $f'(c) > 0$ hence $f(b)-f(a) > 0$. Therefore, for each pair $a, b \in J$ with $a < b$ we find $f(a) < f(b)$ which means f is strictly increasing on J. Likewise, if $f'(c) < 0$ then almost the same argument applies to show $a < b$ implies $f(a) > f(b)$. □

Theorem 9.5.3. *derivative zero implies constant function.*

> If $f'(x) = 0$ for each $x \in (a,b)$ then f is a constant function on (a,b).

Proof: apply the Mean Value Theorem. We know we can because the derivative exists at each point on the interval and this implies the function is continuous on the open interval, so it is continuous on any closed subinterval of (a,b). Let us denote this closed subinterval by $J = [a_o, b_o] \subset (a,b)$. We have to apply the Mean Value Theorem to $J = [a_o, b_o]$ because we do not know for certain that the function is continuous on the endpoints. We find,

$$0 = \frac{f(b_o)-f(a_o)}{b_o-a_o} \quad \Longrightarrow \quad f(b_o) = f(a_o)$$

But this is for an arbitrary closed subinterval hence the function is constant on (a,b). □

Caution: we cannot say the function is constant beyond the interval (a,b). It could do many different things beyond the interval in consideration. Piecewise continuous functions are such examples, they can be constant on the pieces yet at the points of discontinuity the function can jump from one constant to another.

In-Class Example 9.5.4. *Let* $f(x) = \dfrac{\sqrt{x^2}}{x}$ *show* $f'(x) = 0$ *for all* $x \neq 0$*. Is* f *constant ?*

Theorem 9.5.5. *if derivatives of two functions agree then the functions have same shaped graph.*

> If $f'(x) = g'(x)$ for each $x \in (a,b)$ then $f(x) = g(x) + c$ for some constant $c \in \mathbb{R}$.

Proof: Apply Proposition 9.5.3 to $h(x) = f(x) - g(x)$. Notice $h'(x) = f'(x) - g'(x) = 0$ hence $h(x) = c$ and thus $c = f(x) - g(x)$. The proposition follows. □

Notice that the assumption is that they are equal on an open interval. If we had that the derivatives of two functions were equal over some set which consisted of disconnected pieces then we could apply Theorem 9.5.5 to each piece separately then we would need to check that those constants from different components matched up. (for example if $\frac{df}{dx} = \frac{dg}{dx}$ on $(0,1) \cup (2,3)$ then we could have that $f(x) = g(x) + 1$ on (0,1) whereas $f(x) = g(x) + 2$ on $(2,3)$).

9.6 application of extreme value theorem

The following theorem details how to actually find the extrema the Extreme Value Theorem indicated exist. If f is continuous on $[a,b]$ then the Extreme Value Theorem says there exist global extrema with respect to $[a,b]$. If an extrema are in the interior then it must also be a local extrema thus by Fermat's theorem it will occur at a critical number. Otherwise, the extrema are at the endpoints. Therefore, if we check endpoints and critical points we will find the extrema.

Theorem 9.6.1. *closed interval method.*

If we are given function f which is continuous on a closed interval $[a,b]$ the we can find the absolute minimum and maximum values of the function over the interval $[a,b]$ as follows:

1. Locate all critical numbers $x = c$ in (a,b) and calculate $f(c)$.
2. Calculate $f(a)$ and $f(b)$.
3. Compare values from steps 1. and 2. the largest of these values is the absolute maximum, the smallest (or largest negative) value is the absolute minimum of f on $[a,b]$.

I state this theorem here as a reminder of its importance towards finding extreme values of a given function on some closed interval. It is likely I assign some homework to help us mature in our application of calculus to create inequalities for a given function. This tends to be underemphasized in the calculus sequence.

Example 9.6.2. *Let $f(x) = (x-3)(x-4)$ find absolute extrema of f on $[0,1]$. Calculate $f'(x) = (x-4)+(x-3) = 2x-7$ thus $c = -\frac{7}{2}$ is a critical point. Compute the values of $f(x)$ at the critical points inside $[0,1]$ and the endpoints (there are no critical points in $[0,1]$):*

$$f(0) = 12, \quad f(1) = 6.$$

Therefore, $f(0) = 12$ is the absolute maximum and $f(1) = 6$ is the absolute minimum of $f(x) = (x-3)(x-4)$ on $[0,1]$. That is, $6 \leq (x-3)(x-4) \leq 12$ for all $x \in [0,1]$.

Example 9.6.3. *Let $f(x) = x^4 - 2x^2 + 3$ find absolute extrema of f on $[0,2]$. Note that $f'(x) = 4x^3 - 4x = 4x(x^2-1) = 4x(x+1)(x-1)$ thus $c = 0, -1, 1$ are critical points for f. Only $0, 1 \in [0,2]$. Calculate the values of the potential extrema:*

$$f(0) = 3, \quad f(1) = 2$$

Thus, $f(1) = 2$ is the minimum and $f(0) = 3$ is the maximum of f on $[0,2]$. Therefore, $2 \leq x^4 - 2x^2 + 3 \leq 3$ for all $x \in [0,2]$.

9.7 Landau's growth notation

Definition 9.7.1. *Big O-notation ($x \to \infty$) .*

Let f,g be non-negative functions on some unbounded subset of positive real numbers then we write $f(x) = O(g(x))$ as $x \to \infty$ which is read "$f(x)$ is big O of $g(x)$" if there exists $M > 0$ and $x_0 \in \mathbb{R}$ for which $|f(x)| \leq M|g(x)|$ for all $x \geq x_0$. .

When the context is clear, we simply write $f(x) = O(g(x))$. This notation is often applied to sequences which arise in computer science in the study of algorithmics. It gives a quick notation to capture the idea of the largest term.

Example 9.7.2. *Consider $f(x) = 3x^3 - 2x^2 + 7$ then we argue $f(x) = O(x^3)$. Suppose $x \geq 1$,*

$$|f(x)| = |3x^3 - 2x^2 + 7| \leq |3x^3| + |-2x^2| + |7| \leq 3x^3 + 2x^3 + 7x^3 = 12x^3.$$

Hence $|f(x)| \leq 13|x^3|$ for $x \geq 1$. Hence $3x^3 - 2x^2 + 7 = O(x^3)$.

Example 9.7.3. *Consider $f(x) = \frac{1}{x^2+4x+5}$ then we argue $f(x) = O(1/x^2)$. Suppose $x \geq 1$,*

$$|f(x)| = \frac{1}{x^2 + 4x + 5} \leq \frac{1}{x^2}.$$

Hence $|f(x)| \leq |1/x^2|$ for $x \geq 1$. Hence $\dfrac{1}{x^2 + 4x + 5} = O\left(\dfrac{1}{x^2}\right)$.

Example 9.7.4. *Consider $f(x) = \frac{1}{x^2} - \frac{1}{x^2+2x+1}$ then we argue $f(x) = O(1/x^3)$. Observe*

$$f(x) = \frac{1}{x^2} - \frac{1}{x^2 + 2x + 1} = \frac{x^2 + 2x + 1 - x^2}{x^2(x^2 + 2x + 1)} = \frac{2x + 1}{x^4 + 2x^3 + x^2}.$$

Suppose $x \geq 1$, then since $x^4 + 2x^3 + x^2 \geq x^4$ we deduce

$$|f(x)| = \left|\frac{2x + 1}{x^4 + 2x^3 + x^2}\right| \leq \frac{2x + 1}{x^4} \leq \frac{3x}{x^4} = \frac{3}{x^3}.$$

Hence $|f(x)| \leq 3|1/x^3|$ for $x \geq 1$. Hence $\dfrac{1}{x^2} - \dfrac{1}{x^2 + 2x + 1} = O\left(\dfrac{1}{x^3}\right)$.

Definition 9.7.5. *Big O-notation ($x \to 0$).*

Let f, g be non-negative functions near zero then we write $f(x) = O(g(x))$ as $x \to 0$ which is read "$f(x)$ is big O of $g(x)$" as $x \to 0$ if there exists $M > 0$ and $\delta > 0$ for which $|f(x)| \leq M|g(x)|$ for all $x \in (-\delta, \delta)$. .

The idea is that the order O captures the dominant term near $x = 0$. Naturally we could write a similar definition for $x \to a$ or $x \to a^{\pm}$, but we will be content to study O only for the $x \to \infty$ and $x \to 0$ cases.

Example 9.7.6. *Consider $f(x) = e^x - 1 - x$ then we argue $f(x) = O(x^2)$ as $x \to 0$. Recall,*

$$e^x = 1 + x + x^2/2 + x^3/3! + \cdots$$

Thus,

$$e^x - 1 - x = x^2/2 + x^3/3! + \cdots$$

For $|x| < 1$ notice $|x^n| < |x|^n < x^2$

$$|e^x - 1 - x| = |x^2/2 + x^3/3! + \cdots| \leq x^2/2 + x^2/3! + x^2/4! + \cdots \leq (1/2 + 1/3! + 1/4! + \cdots)x^2$$

Consequently, for $x \in (-1, 1)$ we find

$$|e^x - 1 - x| \leq (e - 2)x^2$$

thus $e^x - 1 - x = O(x^2)$ as $x \to 0$. Therefore, as $x \to 0$,

$$e^x = 1 + x + O(x^2)$$

I'll forego the details, but the claims below follow from inequality work similar to that given above. To understand these you need to use the known power series from Calculus II.

Example 9.7.7.

$$\cos(x) = 1 - x^2/2 + O(x^4)$$

$$\cos(x^3) = 1 - x^6/2 + O(x^{12})$$

$$\frac{1}{1-x} = 1 + x + x^3 + O(x^4)$$

$$\frac{1}{1-x} = 1 + x + x^3 + x^4 + O(x^5)$$

$$\frac{1}{1-x^2} = 1 + x^2 + O(x^6)$$

$$\ln(1+x) = x - x^2/2 + x^3/3 + O(x^4)$$

9.8 sequences

We begin by defining sequences of real numbers. Many texts define a real sequence as a function from $\mathbb{N} = \{1, 2, 3, \dots\}$ to $\mathbb{R}$. I'll give a slightly less elegant definition which reflects our actual practice; the sequence can start at any $n_o \in \mathbb{N}$.

Definition 9.8.1. *Sequences*

Let $S = \{n_o, n_o + 1, \dots\} \subseteq \mathbb{Z}$. A function $a : S \to \mathbb{R}$ is called a **sequence**. We denote $a(n) = a_n$ and we refer to a_n as the **n-th term in the sequence**. Alternatively, we also denote the sequence by $\{a_n\}$ or by an explicit list of values:

$$\{a_n\}_{n=n_o}^{\infty} = \{a_{n_o}, a_{n_o+1}, \dots\}.$$

There are various ways to define a sequence. I'll illustrate with a few examples.

Example 9.8.2. *If $a_n = n^2$ for $n \in \mathbb{N}$ then $\{a_n\} = \{1, 4, 9, 16, \dots\}$*

Example 9.8.3. *If $\{a_n\}_{n=1}^{\infty} = \{3, 4, 5, 6, \dots\}$ then $a_n = n + 2$ for $n = 1, 2, \dots$. Alternatively, we can write $\{b_k\}_{k=3}^{\infty} = \{3, 4, 5, 6, \dots\}$ then $b_k = k$ for $k = 3, 4, \dots$.*

Example 9.8.4. *Let a_n for $n = 0, 1, \dots$ be defined* **recursively** *as follows $a_0 = 1$, $a_1 = 1$ and $a_{n+1} = na_n$ for $n = 1, 2, \dots$. The standard notation for this sequence is $a_n = n!$, which is read as* **n-factorial**. *This sequence is grows very large very quickly:*

$$0! = 1,\ \ 1! = 1,\ \ 2! = 2,\ \ 3! = 6,\ \ 4! = 24,\ \ 5! = 120,\ \ 6! = 720,\ \ 7! = 5,040,\ \ 8! = 40,320$$

$$50! = 30414093201713378043612608166064768844377641568960512000000000000$$

Example 9.8.5. *Let $a_n = cr^n$ for $n = 0, 1, \dots$ where r, c are nonzero constants; $\{a_n\} = \{c, cr, cr^2, \dots\}$. Such a sequence is called a* **geometric sequence**. *Notice $a_{n+1}/a_n = (cr^{n+1})/(cr^n) = r$. Infact, it is possible to define the geometric sequence recursively; $a_0 = c$ and $a_n = ra_{n-1}$ for all $n \geq 1$.*

Example 9.8.6. *Consider,* $\{3, 6, 12, 24, 48, \dots\}$ *is geometric with* $c = 3$ *and* $r = 2$ *since*

$$2 = 6/3 = 12/6 = 24/12 = 48/24$$

and the first term is $c = 3$.

Example 9.8.7. *Let* a_n *be given by the decimal representation of* π *given to the* n*-th decimal place for* $n = 1, 2 \dots$. *Then* $\{a_n\} = \{3.1, 3.14, 3.141, 3.1415, 3.14159, 3.141592, \dots\}$

In the example above, the limit of the sequence is simply π and we can write $a_n \to \pi$ as $n \to \infty$. We should define the limit of a sequence carefully:

Definition 9.8.8. *Limits of Sequences*

If for each $\varepsilon > 0$ there exists $N \in \mathbb{N}$ for which $n > N$ implies $|a_n - L| < \varepsilon$ then we say the limit of a_n is L and we denote this by $a_n \to L$ as $n \to \infty$. Equivalently, we write $\lim_{n\to\infty} a_n = L$. A sequence which has a limit is known as a **convergent sequence**. If the sequence does not converge then the sequence is said to **diverge**.

What this definition is saying is that a sequence converges to L then all the terms in the sequence get close to L if we go far enough out in the sequence.

Example 9.8.9. *Let's prove* $\lim_{n\to\infty} \frac{1}{n^2} = 0$. *Let* $\varepsilon > 0$ *and choose* $N \in \mathbb{N}$ *for which* $N > \frac{1}{\sqrt{\varepsilon}}$. *If* $n \in \mathbb{N}$ *and* $n > N > \frac{1}{\sqrt{\varepsilon}}$ *then* $n^2 > \frac{1}{\varepsilon}$ *implies* $\frac{1}{n^2} < \varepsilon$. *Thus*

$$\left| \frac{1}{n^2} - 0 \right| = \frac{1}{n^2} < \varepsilon.$$

Therefore, $\frac{1}{n^2} \to 0$ *as* $n \to \infty$.

If $p > 0$ then we could make a similar argument to that given above to prove $\lim_{n\to\infty} \frac{1}{n^p} = 0$. Convergent sequences are necessarily **bounded**. To say $\{a_n\}_{n=n_o}^{\infty}$ is bounded means there exists $m, M \in \mathbb{R}$ for which $m \leq a_n \leq M$ for all $n \geq n_o$. Equivalently, $\{a_n\}$ is bounded if and only if there exists M for which $|a_n| \leq M$ for all n.

Theorem 9.8.10. *convergent sequences are bounded*

If $\{a_n\}$ is a convergent sequence then $\{a_n\}$ is bounded.

Proof: Consider the sequence $\{a_n\}_{n=n_o}^{\infty}$ for which $a_n \to L$ as $n \to \infty$. Let $\varepsilon = 1$ then note there exists $N \in \mathbb{N}$ for which $|a_n - L| < 1$ whenever $n > N$. Thus,

$$-1 < a_n - L < 1 \quad \Rightarrow \quad L - 1 < a_n < L + 1.$$

for each $n \in \mathbb{N}$ with $n > N$. Define

$$m = min(L - 1, a_{n_o}, a_{n_o+1}, \dots, a_N)$$

$$M = max(L - 1, a_{n_o}, a_{n_o+1}, \dots, a_N)$$

then we find $m \leq a_n \leq M$ for all $n \in \mathbb{N}$ with $n \geq n_o$. $\square$

Logically, if a sequence is not bounded then it cannot be convergent. However, there are sequences which are bounded and yet do not converge.

Example 9.8.11. *Let $a_n = (-1)^{n+1}$ for $n \in \mathbb{N}$. Notice $-1 \leq a_n \leq 1$ for all n, hence this is a bounded sequence. Note $a_{2k} = (-1)^{2k+1} = -1$ whereas $a_{2k-1} = (-1)^{2k-1+1} = (-1)^{2k} = 1$. For this sequence the* **even subsequence** *is the constant sequence $-1, -1, \dots$ whereas the* **odd subsequence** *is the constant sequence $1, 1, \dots$. Naturally $a_{2k} \to -1$ whereas $a_{2k-1} \to 1$ as $k \to \infty$. It follows the limit of a_n does not exist.*

A useful strategy for showing a sequence diverges is illustrated by the example above; if we can find two subsequences which converge to different values then it follows that the given sequence diverges. On the other hand, if the bounded sequence is also *monotonic* then convergence of the sequence is inevitable.

Definition 9.8.12. *Monotonic Sequences*

We say the sequence $\{a_n\}_{n=n_o}^{\infty}$ is strictly increasing if $n_o \leq n < m$ implies $a_n < a_m$. We say the sequence $\{a_n\}_{n=n_o}^{\infty}$ is strictly decreasing if $n_o \leq n < m$ implies $a_n > a_m$. If a sequence is strictly increasing or strictly decreasing then the sequence is said to be **monotonic**.

The proof of this theorem belongs to real analysis[3], but we will apply it in this course.

Theorem 9.8.13. *Bounded Monotonic Sequence Theorem*

A bounded monotonic sequence converges. Furthermore,

(1.) if $\{a_n\}$ is increasing and $a_n \leq M$, then $\{a_n\}$ converges and $\lim_{n\to\infty} a_n \leq M$,

(2.) if $\{a_n\}$ is decreasing and $a_n \geq m$, then $\{a_n\}$ converges and $\lim_{n\to\infty} a_n \geq m$.

Let us see how this helps us find limits of recursively defined sequences.

Example 9.8.14. *Consider the geometric sequence with $0 < r < 1$ and $c = 1$. In particular, we define a_n recursively by $a_0 = 1$ and $a_n = ra_{n-1}$ for $n \geq 1$. Notice $a_n = ra_{n-1} < a_{n-1}$ implies $a_n < a_m$ whenever $m > n$. It is clear the sequence is strictly decreasing. We note $0 < cr^n < c$ for all $n \geq 0$ thus $\{a_n\}$ is bounded. Thus $a_n \to L \in \mathbb{R}$ by the Bounded Monotonic Sequence Theorem. To find the value of L we take the limit[4] of the recursion rule which defined the sequence:*

$$\lim_{n\to\infty}(a_n) = \lim_{n\to\infty}(ra_{n-1}) = r\lim_{n\to\infty} a_{n-1} \quad \Rightarrow \quad L = rL \quad \Rightarrow \quad L(r-1) = 0$$

thus $L = 0$ since $r \neq 1$.

Example 9.8.15. *Let $a_1 = \sqrt{2}$ and define $a_n = \sqrt{2a_{n-1}}$ for $n = 2, 3, \dots$.*

$$a_2 = \sqrt{2\sqrt{2}} = 1.6818, \ a_3 = \sqrt{2\sqrt{2\sqrt{2}}} = 1.8340, \ a_4 = \sqrt{2\sqrt{2\sqrt{2\sqrt{2}}}} = 1.9152$$

continuing in this fashion we can approximate

$$a_5 = 1.9571, \ a_6 = 1.9785, \ a_7 = 1.9892, \ a_8 = 1.9946$$

[3] the proof of this relies on the completeness of the real numbers. Moreover, this is an abbreviation of the full theorem which also claims the limit is given by the supremum or infimum of the set of upper or lower bounds for the sequence.

[4] forgive me for using limit law **(2.)** before its official announcement in this article, look ahead to Theorem **??**

We can guess $a_n \to 2$ from the data we've collected so far. We argue 2 serves as an upper bound for a_n. Observe $a_1 = \sqrt{2} < 2$. Suppose $a_n < 2$ and observe

$$a_{n+1} = \sqrt{2a_n} < \sqrt{2(2)} = 2$$

thus $a_n < 2$ for each $n \in \mathbb{N}$ by mathematical induction[5]*. If $\lim_{n\to\infty} a_n = L$ then we also know $\lim_{n\to\infty} a_{n-1} = L$. Hence, as $n \to \infty$,*

$$a_n = \sqrt{2a_{n-1}} \to L = \sqrt{2L}.$$

Algebra finishes the job here, $L^2 = 2L$ gives $L(L-2) = 0$ hence either $L = 0$ or $L = 2$. But, since the terms in the sequence are increasing and positive we find $L = 2$.

Sometimes we can use calculus to help verify a bound for a given sequence, the next example illustrates such a technique.

Example 9.8.16. *Consider $a_n = \sqrt{n+1} - \sqrt{n}$. Let $f(x) = \sqrt{x+1} - \sqrt{x}$. Observe for $x \geq 1$ we find:*

$$\frac{df}{dx} = \frac{1}{2\sqrt{x+1}} - \frac{1}{2\sqrt{x}} < 0$$

Therefore, if $n < m$ then $f(n) > f(m)$ and hence $a_n > a_m$. Thus $\{a_n\}$ is strictly decreasing. Furthermore, since $g(x) = \sqrt{x}$ has $g'(x) = \frac{1}{2\sqrt{x}} > 0$ for $x > 0$ we likewise find the squareroot function is a strictly increasing function. Note $n < n+1$ thus implies $\sqrt{n} < \sqrt{n+1}$ which means $0 < a_n = \sqrt{n+1} - \sqrt{n}$. Thus $\{a_n\}$ is a bounded monotonic sequence which must converge.
In fact, a bit more algebra would have already revealed the limit is exactly 0:

$$a_n = \sqrt{n+1} - \sqrt{n} = \frac{(\sqrt{n+1} - \sqrt{n})(\sqrt{n+1} + \sqrt{n})}{\sqrt{n+1} + \sqrt{n}} = \frac{1}{\sqrt{n+1} + \sqrt{n}} \to 0$$

I should admit, unlike the last example, the Bounded Monotonic Sequence Theorem is not really needed to solve this limit. The purpose of this example is to explore the ideas, not to coach you in optimally efficient calculation.

Often the divergence fits into the categories defined below:

Definition 9.8.17. *Sequences diverging to $\pm\infty$*

If for each $M > 0$ there exists $N \in \mathbb{N}$ for which $a_n > M$ for all $n > N$ then we write $a_n \to \infty$ as $n \to \infty$ or $\lim_{n\to\infty} a_n = \infty$. If for each $M < 0$ there exists $N \in \mathbb{N}$ for which $a_n < M$ for all $n > N$ then we write $a_n \to -\infty$ as $n \to \infty$ or $\lim_{n\to\infty} a_n = -\infty$.

Example 9.8.18. *Let's prove $\lim_{n\to\infty} n^2 = \infty$. Suppose $M > 0$ and let $N \in \mathbb{N}$ be the next integer after $\sqrt{M}$. By construction, $N \geq \sqrt{M}$. If $n > N$ then $n > \sqrt{M}$ thus $n^2 > M$ and we conclude $\lim_{n\to\infty} n^2 = \infty$.*

If $p > 0$ then we could make a similar argument to that given above to prove $\lim_{n\to\infty} n^p = \infty$.

[5] proof by mathematical induction requires we verify the base-step is true and that if the claim is true for n then the claim likewise follows for $n+1$. The claim in this example was $a_n < 2$. Anytime we want to prove something for all $n \in \mathbb{N}$ it is likely that a proof by induction is technically required.

9.9 series

Let us begin by carefully defining summability or convergence of a series:

Definition 9.9.1. *series*

The series $\displaystyle\sum_{k=n_o}^{\infty} a_k = a_{n_o}+a_{n_o+1}+\cdots$ has n-th partial sum $\displaystyle\sum_{k=n_o}^{n} a_k = a_{n_o}+a_{n_o+1}+\cdots+a_n$. We say the series $\displaystyle\sum_{k=n_o}^{\infty} a_k$ **converges** or is **summable** if its sequence of partial sums converges. The limit of the sequence of partial sums is known as the **sum** of the series and we write

$$\sum_{k=n_o}^{\infty} a_k = \lim_{n\to\infty} \sum_{k=n_o}^{n} a_k.$$

If the series is not convergent then we say the series is **divergent**. If the sequence of partial sums diverges to ±∞ then we write $\displaystyle\sum_{k=n_o}^{\infty} a_k = \pm\infty$.

Let me express the sequence of partial sums in the case $n_o = 1$,

$$\left\{\sum_{k=1}^{n} a_k\right\} = \{a_1,\ a_1+a_2,\ a_1+a_2+a_3,\ \dots\}$$

Example 9.9.2. *Consider $\sum_{k=1}^{\infty} 1 = 1+1+\cdots$. In this case the n-th partial sum is simply*

$$\sum_{k=1}^{n} 1 = \underbrace{1+1+\cdots+1}_{n\text{-}summands} = n$$

Thus $\displaystyle\sum_{k=1}^{\infty} 1 = \lim_{n\to\infty}\sum_{k=1}^{n} 1 = \lim_{n\to\infty} n = \infty.$

Example 9.9.3. *Observe* $\displaystyle\sum_{k=1}^{n} 0 = 0+0+\cdots+0 = 0$ *thus* $\displaystyle\sum_{k=0}^{\infty} 0 = \lim_{n\to\infty} 0 = 0.$

Theorem 9.9.4. *n-th term test for divergence*

If $\displaystyle\sum_{k=n_o}^{\infty} a_k$ converges then $\lim_{n\to\infty} a_n = 0$. If $\lim_{n\to\infty} a_n \neq 0$ then $\displaystyle\sum_{k=n_o}^{\infty} a_k$ diverges.

Proof: Let $S_n = \sum_{k=n_o}^{n} a_k$ and suppose $S_n \to S$ as $n \to \infty$. Notice that the n-term in the series can be written as the difference of partial sums $S_n - S_{n-1} = \sum_{k=n_o}^{n} a_k - \sum_{k=n_o}^{n-1} a_k = a_n$. Thus,

$$a_n = S_n - S_{n-1} \to S - S = 0.$$

Therefore, if $\displaystyle\sum_{k=n_o}^{\infty} a_k$ converges then $\lim_{n\to\infty} a_n = 0$. Notice the second sentence in the Theorem follows by logic from the first. □

Example 9.9.5. *Consider the series* $\tan^{-1}(1)+\tan^{-1}(2)+\dots$. *Observe the* n*-th term in the series is* $\tan^{-1}(n)$. *Therefore this series diverges by the* n*-th term test since* $\tan^{-1}(n) \to \frac{\pi}{4}$ *as* $n \to \infty$.

I should mention now that the converse to the n-th term test does not hold. In particular, it is possible to have a series with n-term $a_n \to 0$ as $n \to \infty$, yet the series still diverges. The most famous example of this is the harmonic series:

$$\sum_{n=1}^{\infty} \frac{1}{n} = 1 + \frac{1}{2} + \frac{1}{3} + \cdots = \infty.$$

I will withold proof of the claim above until a later section. I just want you to understand why I include the term *divergence* in heading for the n-th term test. It is a test which only gives certitude of divergence. The n-th term test does not prove summability of the series.

Definition 9.9.6. *geometric series*

Let $c, r \in \mathbb{R}$ then $\sum_{k=0}^{\infty} cr^k = c + cr + cr^2 + \cdots$ is a **geometric series**.

Geometric series are everywhere if you look for them. It is very simple to decide whether a given geometric series is convergent or divergent.

Theorem 9.9.7. *geometric series*

The geometric series $c + cr + cr^2 + \cdots$ is summable with sum $\frac{c}{1-r}$ if and only if $|r| < 1$. If $|r| \geq 1$ then the geometric series is divergent.

Proof: let $S_n = c + cr + cr^2 + \cdots + cr^{n-1} + cr^n$ be the n-th partial sum of the geometric series. Observe $rS_n = r(c + cr + cr^2 + \cdots + cr^{n-1} + cr^n) = cr + cr^2 + cr^3 + \cdots + cr^n + cr^{n+1}$. Therefore,

$$\begin{aligned} S_n - rS_n &= cr + cr^2 + cr^3 + \cdots + cr^n + cr^{n+1} - \big(c + cr + cr^2 + \cdots + cr^{n-1} + cr^n\big) \\ &= cr^{n+1} - c \end{aligned}$$

Algebra yields $(1-r)S_n = c(r^{n+1}-1)$. Hence, $S_n = \dfrac{c(r^{n+1}-1)}{1-r}$. If $|r| < 1$ then $S_n \to \frac{c}{1-r}$ since $r^{n+1} \to 0$ as $n \to \infty$. If $|r| \geq 1$ then $\lim_{n\to\infty}(cr^n) \neq 0$ thus the geometric series diverges by the n-th term test. □

Example 9.9.8. *Whenever we have a number with a repeating decimal expansion we can use the geometric series to convert the number to an explicit fraction.*

$$2.577777\cdots = 2.5 + 0.07777\cdots = 2.5 + \underbrace{\frac{7}{100} + \frac{1}{10}\frac{7}{100} + \frac{1}{10^2}\frac{7}{100} + \cdots}_{\text{geometric with } c = 7/100 \text{ and } r = 1/10}$$

thus,

$$2.5777\cdots = 2.5 + \frac{7/100}{1-1/10} = \frac{5}{2} + \frac{7/100}{9/10} = \frac{5}{2} + \frac{7}{90} = \frac{5(90)+7(2)}{180} = \frac{464}{180} = \frac{116}{45}.$$

Chapter 10

Algebra

Typically I expect the students in this course to memorize and understand all the definitions we discuss in these notes. This chapter is an exception to that rule. Basically, this chapter is a survey of higher algebra courses and concepts. I will tell you explicitly which definitions or proofs I expect you to be able to recreate for tests and the exam. I would like you to read this chapter, it is my hope this helps prepare you for future courses.

10.1 history, scope, motivations

Algebra is a general term which encompasses a very wide section of modern mathematics. There are hundereds if not thousands of subfields of study in algebra. Almost all of these are born from the desire to solve equations.

Polynomial equations are a central motivating example. Linear equations $ax + b = 0$ are easy to solve. Quadratics $ax^2 + bx + c = 0$ are solved without exception by the quadratic formula (*which you should be able to derive at this point in your mathematical journey, just saying*). Cubics, well those are a little harder, however it is known that $ax^3 + bx^2 + cx + d = 0$ has a solution which is given by a closed form algebraic formula. The same holds for quartics. You might be tempted to hope there is always some "n-order quadratic formula" which gives the general solutions for $p(x) = 0$ where $deg(p) = n \in \mathbb{N}$. You would be wrong. It turns out that the 5-th order equation, called a **quintic equation**, does not have a general closed form solution.

Each step in the preceding paragraph has all sorts of algebra tied to it. Linear equations are the first example in study of linear algebra, although I should emphasize that linear algebra is motivated by a myriad of applications. The linear equation also leads you to consider negative numbers; what is the solution to $x + 2 = 0$? If you were born several centuries ago you might have said there was no solution, the concept of negative numbers has only become mainstream relatively recently. Quadratic equations force you to consider numbers beyond fractions of integers, the equation $x^2 - 2 = 0$ has a solution which is not rational. Quadratic equations encourage you to think about complex numbers; what is the solution to $x^2 + 1 = 0$? The same is true for cubic equations whose solution was given by Cardano in 1545. In 1572 Bombelli pointed out that the cubic $x^3 - 15x - 4 = 0$ has three real solutions yet the Cardona formula has complex numbers (which somehow cancel out to give a three real solutions). This goes to show that imaginary numbers are not really that "imaginary". In my humble opinion this is why it is high time we taught complex numbers early and often in mathematics, but don't get me started...

The quintic equation was shown to be insolvable by a formula like the quadratic formula by Abel and Ruffini in the early nineteenth century. (this is the Abel for which Abelian groups get there name). However, this is not to say that **all** quintics cannot be solved by a closed-form formula using a finite series of algebraic operations. For example, $x^5 = 0$ is pretty easy to solve in terms of radicals; $\sqrt[5]{x^5} = \sqrt[5]{0^5}$ thus $x = 0$. There is an obvious question to ask: *When does a quintic have a nice algebraic solution?*. Galois answered this question by studying the *group* of symmetries for roots to a polynomial equations. This group is now known as the Galois group. Incidentally, the history of Galois is rather fascinating, he died at age 20 (in 1832) after getting shot in a duel. He pioneered much of basic group theory and is apparently the first to call a group a group (although, the precise definition of a *group* we consider in these notes wasn't settled until much later). Galois apparently feared his death was likely since he wrote a letter trying to preserve his work just before the duel. There are stories that he worked late into the night so that his mathematical works would not be lost with his death.

It turns out that the very construction of rational numbers, real numbers and complex numbers is provided by in large by techniques in abstract algebra. The natural numbers come from set theory. The integers are constructed by adjoining negatives and zero. Then the rational numbers are constructed as the *field of quotients* of the integers. Then, one can adjoin algebraic numbers using something called an *extension field.* The rational numbers adjoined with all possible algebraic numbers form the set of *algebraic numbers.* For example, $\sqrt{2}$ and $\sqrt{1 + \frac{1}{1+\sqrt[5]{3}}}$ are algebraic numbers. It turns out that the cardnality of the algebraic numbers is $\aleph_o$. To obtain the *transcendental* numbers something beyond algebra has to enter the discussion. Analysis, in particular the careful study of sequences and their limits, allows us to adjoin the transcendental numbers. In a nutshell, that is how to construct the real numbers. The construction I just outlined will generate all the properties of real numbers which we have been taught to take for granted since our elementary school days. Algebra (and analysis) is used to construct our number system.

Algebra goes far beyond the history I just outlined. I'll throw in more comments as I develope the material. My goal in this Chapter is simply to equip you with the basic definitions and some familarity with basic examples. Hopefully Math 421 will seem less bizarre if we at see the basics here. Customarily a math major will have two serious courses in abstract algebra as an undergraduate then another pair of graduate abstract algebra courses as a graduate student. For a pure mathematician it is not unusual to take upwards of a dozen courses in algebra.

10.2 algebraic structures

There are many examples of binary operations:

$$\text{Function Composition: } (f, g) \mapsto f \circ g$$
$$\text{Addition of Numbers: } (a, b) \mapsto a + b$$
$$\text{Multiplication of Numbers } (a, b) \mapsto ab$$
$$\text{Matrix Addition } (A, B) \mapsto A + B$$
$$\text{Matrix Multiplication } (A, B) \mapsto AB$$

Cross Product on 3-vectors $(\vec{v}, \vec{w}) \mapsto \vec{v} \times \vec{w}$

A binary operation on a set S is a rule which takes **two** things from the set and outputs another. We can be precise about this:

Definition 10.2.1. *A* **binary operation** *on A is a function from $A \times A$ to A. We say that a binary relation on A is* **closed on A**. *Moreover, if we denote the operation by $*$ such that $(a, b) \mapsto a * b$ then we say that $(A, *)$ is a set A with an operation $*$.*

The notation $(A, *)$ is nice because it pairs the set with the operation. Clearly there can be many operations on a particular set. When we have one or more operations on a set A it is called an **algebraic system**.

Definition 10.2.2. *Given a set A and operations $*$ and $\circ$ we say that $(A, *, \circ)$ is a set with two operations $*$ and $\circ$. If a set A has has one or more operations and possibly several relations then we say A is an* **algebraic system**

Example 10.2.3. *Let $\mathbb{R}$ be the real numbers. We have two natural operations, addition $+$ and multiplication $\cdot$. We also have an order relation on $\mathbb{R}$; we say $(x, y) \in R_< \subset \mathbb{R} \times \mathbb{R}$ iff $x < y$. Collecting these together, $(\mathbb{R}, +, \cdot, <)$ is an algebraic system with operations $+$ and $\cdot$.*

Almost always given a particular set you can add further structure. For example, we could adjoin the relation $R_>$ (where $(x, y) \in R_> \subset \mathbb{R} \times \mathbb{R}$ iff $x > y$) to the algebraic system above; $(\mathbb{R}, +, \cdot, <, >)$. You should understand that when we give a description of a set in algebra we are trying to give a minimal description. The goal is to obtain the desired conclusion with a minimal set of assumptions. As a student this is a change of culture, in calculus we have been in the practice of admonishing you for forgetting things from years and years ago. In algebra, and abstract math in general, we ask you to forget what you know and work with just what you are given and can prove. This is quite a change in thinking. Almost everyone struggles at first, so if first you don't succeed then don't be too discouraged. Remember, at least for this course the most critical thing is definitions. You have to know the definitions, you should *own* them.

Example 10.2.4. *Let $\mathbb{Z}$ be the integers. We have two natural operations, addition $+$ and multiplication $\cdot$. Thus $(\mathbb{Z}, +, \cdot)$ is an algebraic system.*

Example 10.2.5. *Let $\mathbb{Z}_n$ be the integers mod $n \in \mathbb{N}$. We have two natural operations, addition $+_n$ and multiplication $\cdot_n$. Thus $(\mathbb{Z}_n, +_n, \cdot_n)$ is an algebraic system.*

Given an operation on a set A we can sometimes induce an operation on a subset $B \subseteq A$. Let $(A, *)$ be a set with operation $*$ then we say that $B \subseteq A$ is **closed under** $*$ iff $*$ restricted to B is a binary operation.

Example 10.2.6. *Let $\mathbb{Z}$ be the integers. Notice $2\mathbb{Z} = \{2k \mid k \in \mathbb{Z}\}$ is a subset of $\mathbb{Z}$. We proved that the sum and product of even integers is even thus the two natural operations, addition $+$ and multiplication $\cdot$, are closed on $2\mathbb{Z}$. Therefore $(2\mathbb{Z}, +, \cdot)$ is an algebraic system.*

If you want to be really pedantic (as is sometimes my custom), the $+$ and $\cdot$ on $2\mathbb{Z}$ and those on $\mathbb{Z}$ are technically different functions since they have different domains. Hence, you could say that they are different operations. However, I find it more productive to say that the operations on $2\mathbb{Z}$ are *inherited* or *induced* from $\mathbb{Z}$.

Example 10.2.7. *Let $\mathbb{Z}$ be the integers. Notice $2\mathbb{Z}+1 = \{2k+1 \mid k \in \mathbb{Z}\}$ is a subset of $\mathbb{Z}$. We proved that the product of odd integers is odd thus the natural operation of multiplication $\cdot$ is closed on $2\mathbb{Z}+1$. Therefore $(2\mathbb{Z}+1, \cdot)$ is an algebraic system. Notice, in contrast, $+$ is* **not** *an operation on $2\mathbb{Z}+1$ since $1, 3 \in 2\mathbb{Z}+1$ yet $1+3 = 4 \notin 2\mathbb{Z}+1$. We see that $\cdot$ is not closed on the set of odd integers.*

The examples that follow go beyond the mainline of the text and homework, but I thought they might help bring context to the earlier discussion. I now give examples of things which are **not** binary operations. But, first a definition:

Definition 10.2.8. *Suppose A is a set and $n \in \mathbb{N}$. We define an n-ary operation on A to be a function $f : \underbrace{A \times A \times \cdots \times A}_{n\ copies} \to A$. If $n = 1$ we say it is a* **unary** *operation on A, if $n = 2$ it's a* **binary** *operation on A, if $n = 3$ its called a* **ternary** *operation.*

Example 10.2.9. *Let $f : \mathbb{R} \to \mathbb{R}$ be defined by $f(x) = -x$. This describes a unary operation on $\mathbb{R}$ called the* **additive inverse operation***. Likewise, $g(x) : \mathbb{R} - \{0\} \to \mathbb{R} - \{0\}$ defined by $g(x) = \frac{1}{x}$ is the* **multiplicative inverse operation***.*

Example 10.2.10. *The dot product on $\mathbb{R}^n$ is defined as follows: let $n \in \mathbb{N}$ and $\vec{x} =< x_1, x_2, \dots, x_n >$ and $\vec{y} =< y_1, y_2, \dots, y_n >$ then*

$$\vec{x} \cdot \vec{y} = x_1y_1 + x_2y_2 + \cdots + x_ny_n$$

This is a function from $\mathbb{R}^n \times \mathbb{R}^n$ to $\mathbb{R}$ thus the dot-product is **not** *a binary operation on vectors.*

Example 10.2.11. *(concerning crossproducts in dimension $n \neq 3$) The crossproduct is sometimes said to only exist in $\mathbb{R}^3$. In other words, there is no crossproduct in 2 or 4 dimensions. I usually adopt this viewpoint. However, it does depend on what you mean by "crossproduct in other dimensions". Let me remind you that*

$$(\vec{A} \times \vec{B}) \cdot \vec{A} = 0 \quad \textit{and} \quad (\vec{A} \times \vec{B}) \cdot \vec{B} = 0$$

essentially describe what the crossproduct does; the crossproduct picks out a vector which is perpendicular to both of the given vectors. If we characterize the crossproduct to simply be the operation which produces a new vector which is orthogonal to its input vectors then you can construct "crossproducts" in any dimension. However, the "crossproduct" on $\mathbb{R}^n$ will be a $(n-1)$-ary operation on $\mathbb{R}$. Let me show you the "crossproduct" on $\mathbb{R}^2$,

$$f(< a, b >) =< b, -a >$$

Notice $f(< a, b >) \cdot < a, b >= ab - ba = 0$ thus $f(< a, b >)$ is orthogonal to its input $< a, b >$. For $\mathbb{R}^4$ you could define the "crossproduct" of $\vec{x}, \vec{y}, \vec{z}$ to be

$$\vec{x} \times \vec{y} \times \vec{z} = det \begin{pmatrix} e_1 & e_2 & e_3 & e_4 \\ x_1 & x_2 & x_3 & x_4 \\ y_1 & y_2 & y_3 & y_4 \\ z_1 & z_2 & z_3 & z_4 \end{pmatrix}$$

where this is a mneumonic just as is the case with $n = 3$ since the first row is made of vectors $e_1 =< 1, 0, 0, 0 >$ and $e_2 =< 0, 1, 0, 0 >$ etc.. so technically this is not a determinant.[1]

[1] the best way to generalize the cross product is with the wedge product. In Math 332 (Advanced Calculus) we explore the wedge product and the exterior calculus which generalizes vector calculus seen in Math 231.

The Point? *only in $\mathbb{R}^3$ is the crossproduct a* **binary** *operation on vectors. So, if you insist that the crossproduct is a binary operation then you have a pretty good case that it only exists for $\mathbb{R}^3$.*

That said, the other "crossproducts" I have described are important to higher dimensional integration and so forth. We use the crossproduct to pick out the normal to a surface. The "crossproduct" in $n = 4$ could pick out the normal to a volume. In fact, the theory of integration in n-dimensions is most elegantly phrased in terms of the wedge product which gives differential forms a natural **exterior algebra***. If you want to see an elementary introduction to exterior calculus, just ask I can point you to a few videos.*

10.3 algebraic properties

Algebraic systems often obey certain rules or properties.

Definition 10.3.1. *Let $(A, *)$ be an algebraic system. Then*

1. *commutative property* *We say $*$ is* **commutative** *iff for all $a, b \in A$, $a * b = b * a$.*
2. *associative property* *We say $*$ is* **associative** *iff for all $a, b, c \in A$, $(a * b) * c = a * (b * c)$.*
3. *unital* *We say that A has an* **identity** *$e \in A$ iff for all $a \in A$, $e * a = a$ and $a * e = a$. If A has an identity then it is said to be* **unital***.*
4. *invertibility* *Let A be unital with identity element e. Let $a \in A$, we say a is* **invertible** *iff there exists $b \in A$ such that $a * b = e$ and $b * a = e$. In this case, we say b is the* **inverse of** *a* **with respect to** *$*$. If every element of A is invertible then we say that $*$ is* **closed under inverses***.*

If a set A is closed under inverses then we could say that the inverse operation is unary on A. Usually $*$ is either addition, multiplication or function composition. In those cases there are standard notations and terminologies for the inverse operation:

1. multiplicative inverse of a: we denote by a^{-1}; we have $a * a^{-1} = 1$ and $a^{-1} * a = 1$.

2. additive inverse of b: we denote by $-b$; we have $b + (-b) = 0$ and $-b + b = 0$.

3. inverse function of f: we denote by f^{-1}; we have $f \circ f^{-1} = id_{range(f)}$ and $f^{-1} \circ f = id_{dom(f)}$.

Notice that e can be many things depending on context. In the list just above we saw that $e = 1$ for multiplication, $e = 0$ for addition and $e = id$ the identity function for function composition.

Example 10.3.2. $(\mathbb{R}, +, \cdot)$ *is commutative, associative and unital with respect to both $+$ and $\cdot$. Moreover, $\mathbb{R}$ is closed under additive inverses. In contrast, $\mathbb{R}$ is not closed under multiplicative inverses since the additive inverse 0 does not have a multiplicative inverse (cannot divide by zero).*

Example 10.3.3. *A nice example of a nonassociative operation is the crossproduct. Notice*

$$[(i + j) \times j] \times k = k \times k = 0$$

yet

$$(i + j) \times (j \times k) = (i + j) \times i = -k$$

Example 10.3.4. *Matrix multiplication is associative: let A, B, C be multipliable matrices then $(AB)C = A(BC)$. This follows directly from the definition of matrix multiplication and the associativity of the numbers which fill the matrices.*

Example 10.3.5. Lie Algebras *have an operation which is typically nonassociative. The operation on a Lie algebra is called the* **Lie bracket** *and it is denoted by $[A, B]$. The bracket has to satisfy the Jacobi Identity which is a sort of weakened associativity condition:*

$$[[A, B], C] + [[B, C], A] + [[C, A], B] = 0$$

In the case that the Lie algebra arises from an associative algebra the Lie bracket is just the **commutator bracket** *which is defined by $[A, B] = AB - BA$.*

Lie Algebras play an important role in classical and quantum mechanics because the generators of symmetry groups typically obey some sort of Lie algebraic structure. As I understand it, the original goal of Sophius Lie was to find solutions to differential equations. Perhaps you have seen that many differential equations reduce to a problem in algebra. If you study physics you'll learn that many of the hardest physics problems are solved through making a clever change of coordinates. The coordinate change always reflects a deeper symmetry of the problem and usually it makes the differential equations for the problem decouple so that elegant solutions are possible. Lie was trying to generalize this idea from classical mechanics to the solution of arbitrary differential equations, not necessarily stemming from physics. I don't think the complete goal has been realized even at this time, however work on Lie theory continues. I have a textbook which explains the idea of solving differential equations by symmetry methods for one independent variable, I'll show you if you're interested.

Definition 10.3.6. *A* **Cayley Table** *for an algebraic structure $(A, *)$ is a square table which lists all possible operations for the structure.*

Example 10.3.7. *We have already discussed many Cayley tables for $\mathbb{Z}_n$. For example, we wrote all possible additions and multiplications in $\mathbb{Z}_3$ in the last chapter. These are the Cayley tables for $(\mathbb{Z}_3, +_3)$ and $(\mathbb{Z}_3, \cdot_3)$ respectively:*

$+_3$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\cdot_3$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

Example 10.3.8. *Suppose that $A = \{x, y\}$ such that $(A, *)$ is an algebraic structure on A which is commutative and $x * y = x$. Moreover, suppose that $a * a = a$ for all $a \in A$. Find the Cayley table and identify the identity if possible. Use the given assumptions to deduce that*

$$x * x = x, \qquad y * y = y, \qquad x * y = y * x = x.$$

We can write these results in a Cayley table:

$*$	x	y
x	x	x
y	x	y

Is x is the identity for $*$? Consider

$$x * x = x, \qquad \text{but } y * x = x \neq y.$$

Is y is the identity for $*$? Consider

$$x * y = x, \qquad \text{and } y * y = y$$

It follows $y * a = a * y = a$ for all $a \in A$ hence y is the identity element for A. Moreover, we can see x is not invertible while $y^{-1} = y$. In order for x to be invertible we need there to be some element x^{-1} such that $x * x^{-1} = y$ but there is no such element.

Theorem 10.3.9. *Let $(A, *)$ be an algebraic structure. Then A has at most one identity element. In addition, if A is associative and unital then each invertible element has a unique inverse.*

Proof: Suppose that $(A, *)$ has two identity elements $e_1, e_2 \in A$. Since e_1 is an identity element we have $a * e_1 = e_1 * a = a$ for all $a \in A$. Notice that $e_2 \in A$ thus $e_2 * e_1 = e_2$. Likewise, since e_2 is an identity element, $a * e_2 = e_2 * a = a$ for all $a \in A$. Hence, as $e_1 \in A$, we also have $e_2 * e_1 = e_1$. Therefore, $e_1 = e_2$. We can speak of **the** identity for an associative algebraic system.

Next, suppose that A is an associative, unital algebra with identity e. Use multiplicative notation and let $a \in A$ such that b_1 and b_2 are both inverses of a. That is, assume $ab_1 = b_1a = e$ and $ab_2 = b_2a = e$. We seek to show that $b_1 = b_2$. Multiply the first equation by b_2 on the left,

$$b_2ab_1 = b_2b_1a = b_2e = b_2$$

Multiply the second equation by b_1 on the right,

$$ab_2b_1 = b_2ab_1 = eb_1 = b_1$$

Comparing these equations we see $b_2ab_1 = b_2 = b_1$. Therefore, the inverse of $a \in A$ (when it exists) is unique. It is hence unambiguous to denote **the** inverse of a by $a^{-1} = b_1 = b_2$.

Question: where did we assume associativity in the proof above?

Remark 10.3.10. *(fruits of associativity) Let $(A, \cdot)$ be an associative algebraic system. Furthermore, let us use* **juxtaposition** *as a notation for the operation; $a \cdot b = ab$. In this notation, associativity simply means that certain parentheses can be dropped. For all $a, b, c \in A$,*

$$(ab)c = a(bc) = abc,$$

the parentheses can be dropped without ambiguity. In contrast, we cannot drop parentheses in $(\vec{A} \times \vec{B}) \times \vec{C}$ since this not equal to $\vec{A} \times (\vec{B} \times \vec{C})$. If we just write $\vec{A} \times \vec{B} \times \vec{C}$ then what is meant? Associative products allow for nonnegative **power notation**

$$aa = a^2, \qquad aaa = a^3, \qquad a^n = a^{n-1}a$$

Be careful though, generally

$$(ab)^2 \neq a^2b^2.$$

Instead, $(ab)^2 = abab$. If the algebraic stucture is also **commutative** *then we can rearrange those terms to get $(ab)^2 = aabb = a^2b^2$. Matrix multiplication is a popular example of an operation which is associative but* **not** *commutative.*

Theorem 10.3.11. *(algebraic system of bijections on a set A) Let $A \neq \emptyset$ and let $\mathcal{F}(A)$ be the set of all bijections on A. If $\circ$ denotes function composition then $(\mathcal{F}(A), \circ)$ is an associative, unital algebraic system which is closed under inverses. In particular the identity element of $\mathcal{F}(A)$ is the identity function I_A and the inverse of $f \in \mathcal{F}(A)$ is f^{-1}.*

Proof: See theorems in in Chapter 4. In short, the composite of bijections is again a bijection to the operation of function composition is closed on $\mathcal{F}(A)$. Moreover, we the inverse of a bijection exists and the identity function does satisfy the needed identities.

10.3.1 groups

Definition 10.3.12. *(group) We say $(G, *)$ is a* **group** *iff $(G, *)$ is an algebraic system which is associative, unital and closed under inverses. That is a set G is a group iff the following hold true:*

(1.) *if $g, h \in G$ then $*$ assigns one element $g * h \in G$,*

(2.) *if $a, b, c \in G$ then $(a * b) * c = a * (b * c)$,*

(3.) *there exists $e \in G$ such that for all $g \in G$, $g * e = e * g = g$.*

(4.) *for each $g \in G$ there exists $a^{-1} \in G$ such that $a * a^{-1} = a^{-1} * a = e$.*

Here (1.) is to insure that $*$ is a binary operation on G. Many of the examples we have so far discussed are in fact groups. Some are not. For example, $(\mathbb{Z}_n, +_n)$ forms a group with respect to $+$ however $(\mathbb{Z}_n, \cdot_n)$ does not form a group since 0^{-1} does not exist.

Definition 10.3.13. *(abelian group) An abelian group is a commuative group. That is, G is abelian iff $(G, *)$ is a group and for all $a, b \in G$, $a * b = b * a$.*

$(\mathbb{Z}_n, +_n)$, $(\mathbb{R}, +)$, $(\mathbb{C} - \{0\}, \cdot)$ are all abelian groups. In contrast, $\mathcal{F}(A)$ of Theorem 10.3.11 is **nonabelian**. In fact, the group $\mathcal{F}(A)$ is so special it gets a name:

Definition 10.3.14. *($\mathcal{F}(A)$; the group of permutations on A) Let A be a nonempty set. A* **permutation** *on A is a one-one and onto function on A. The set of all one-one and onto functions on A is a group called the* **permutation group on** *A which we denote $\mathcal{F}(A)$ in these notes (not a standard notation).*

When A is finite it turns out that $\mathcal{F}(A)$ is also finite. Counting will reveal that $\overline{\overline{\mathcal{F}(A)}} = (\overline{\overline{A}})!$. If A is infinite then there are more permutations than I can count.

Definition 10.3.15. *The* **symmetric group** *is the group of permuations on $\{1, 2, 3, \dots, n\} = \mathbb{N}_n$. We define $\mathcal{F}(\mathbb{N}_n) = S_n$.*

I refer you to the posted homework solutions for examples on how the notation for S_n works in this text. I would like to talk about *cycle notation* if there is time (unlikely). Permutation groups have played an important role in the historical developement of group theory. They are also very useful in the theory of determinants. In short, you can use permutations to encode all those funny signs in the determinant formula.

Theorem 10.3.16. *(socks-shoes theorem) Let $(G, *)$ be a group then $(a * b)^{-1} = b^{-1} * a^{-1}$*

Proof: Let $a, b \in G$ notice since G is closed under inverses we know $a^{-1}, b^{-1} \in G$. Observe that

$$(a * b) * (b^{-1} * a^{-1}) = a * b * b^{-1} * a^{-1} = a * e * b^{-1} = b * b^{-1} = e$$

and,

$$(b^{-1} * a^{-1}) * (ab) = b^{-1} * a^{-1} * a * b = b^{-1} * e * b = b^{-1} * b = e.$$

Therefore, $(ab)^{-1} = b^{-1} * a^{-1}$. $\square$

Theorem 10.3.17. *(inverse operation is an involution) Let $(G, *)$ be a group then $(a^{-1})^{-1} = a$*

Proof: Let $a \in G$ notice since G is closed under inverses we know $a^{-1} \in G$ and $aa^{-1} = e$ and $a^{-1}a = e$. But then by definition of inverse we see a is the inverse of a^{-1}. Moreover, since the inverse is unique by Theorem 10.3.9 we conclude $(a^{-1})^{-1} = a$.

Theorem 10.3.18. *Let $x, y, z \in G$ and use juxtaposition to denote the operation then*

(1.) $xy = xz \implies y = z$

(2.) $yx = zx \implies y = z$

We call (1.) the **left cancellation law** *and (2.) the* **right cancellation law***.*

Proof: Let $x, y, z \in G$ notice that by definition of group x^{-1} exists. Suppose $xy = xz$ then multiply by x^{-1} on the left to obtain $x^{-1}xy = x^{-1}xz$ which implies $ey = ez$ thus $y = z$. Likewise, multiply by x^{-1} on the right to obtain the right cancellation law. □

Let me restate the cancellation laws and their proof in additive notation:

Theorem 10.3.19. *Let $x, y, z \in (G, +)$ and use additive notation to denote the operation then*

(1.) $x + y = x + z \implies y = z$

(2.) $y + x = z + x \implies y = z$

Proof: Let $x, y, z \in (G, +)$ notice that by definition of group $-x$ exists. Suppose $x + y = x + z$ then add by $-x$ on the left to obtain $-x + x + y = -x + x + z$ which implies $0 + y = 0 + z$ thus $y = z$. Likewise, add by $-x$ on the right to obtain the right cancellation law. □

Remark 10.3.20. *(additive verses multiplicative group notation) We can define integer powers of $a \in (G, \cdot)$ by repeated multiplication of a or a^{-1}, using the juxtaposition notation: for each $n \in \mathbb{N}$*

$$a^n = \underbrace{aa \cdots a}_{n} \qquad a^{-n} = \underbrace{a^{-1}a^{-1} \cdots a^{-1}}_{n}$$

finally we **define** *$a^0 = e$. It is straightforward to check that $a^s a^t = a^{s+t}$ for all $s, t \in \mathbb{Z}$. In the case the group is commutative we recover the usual laws of exponents.*

If $(G, +)$ is an additive group then we can define **multiples** *of a in terms of repeated addition of a or $-a$: for each $n \in \mathbb{N}$*

$$n \cdot a = \underbrace{a + a + \cdots + a}_{n} \qquad -n \cdot a = \underbrace{-a + (-a) + \cdots + (-a)}_{n}$$

and $0 \cdot a = 0$.

The notation $n \cdot a$ is not necessarily multiplication in the group. Your group might not even have integers in it. It is simply a notation, a shorthand, to express repeated addition.

10.3.2 subgroups

A subset of a group which is also a group is called a **subgroup**.

Definition 10.3.21. *(subgroup) Let $(G, *)$ be a group. If $H \subseteq G$ such that $*$ restricted to H gives H the structure of a group then we say that H is a* **subgroup** *of G. Equivalently, we can say H is a subgroup of G if it is a group with respect to the group operation inherited from G. If H is a subgroup of G then we denote this by writing $H < G$.*

Example 10.3.22. *$G = \mathbb{Z}_6$ is an additive group. We can show $H = \{0, 3\}$ is a subgroup of G. Notice that $0 + 0 = 0$ and $3 + 3 = 0$ thus H contains the identity and each element has an inverse. Moreover, it is clear that addition in H is commutative and associative. Thus $H < G$.*

Example 10.3.23. *Let G be a group with identity e. Observe that $H = G$ and $H = \{e\}$ form subgroups of G. The subgroup $H = \{e\}$ is called the* **trivial subgroup**. *A subgroup $H \neq G$ is called a* **proper subgroup**.

Theorem 10.3.24. *(subgroup test) Let $(G, *)$ be a group. A subset $H \subseteq G$ is a subgroup of G iff $H \neq \emptyset$ and for all $a, b \in H$, $a * b^{-1} \in H$.*

Cyclic groups are particularly simple to analyze.

Proposition 10.3.25. *(cyclic subgroup generated by a) Let G be a group with operation denoted by juxtaposition. Let $a \in G$ then*

$$< a >= \{a^n \mid n \in \mathbb{Z}\} = \{..., a^{-2}, a^{-1}, e, a, a^2, \dots\}$$

is an abelian subgroup of G.

Proof: Let G be a group and suppose $a \in G$. Observe that $a \in < a >$ thus $< a > \neq \emptyset$. Suppose that $x, y \in < a >$ then there exist $s, t \in \mathbb{Z}$ such that $x = a^s$ and $y = a^t$. Furthermore, $y^{-1} = a^{-t}$. Observe that $xy^{-1} = a^s a^{-t} = a^{s-t} \in < a >$ thus by the subgroup test we conclude that $< a >$ is a subgroup of G. Notice $< a >$ is abelian since for all $a^s, a^t \in < a >$, $a^s a^t = a^{s+t} = a^{t+s} = a^t a^s$. □

Definition 10.3.26. *Let G be a group then $< a >$ is the* **cyclic subgroup** *generated by $a \in G$. If there exists $b \in G$ such that $< b >= G$ then we say that G is a* **cyclic group** *with* **generator** *b.*

Example 10.3.27. *$(\mathbb{Z}_4, +)$ is a cyclic group with generator 1. Additionally, $(\mathbb{Z}_4, +)$ is a cyclic group with generator 3. Notice that, modulo 4 we calculate*

$$\{1, 1 + 1, 1 + 1 + 1, 1 + 1 + 1 + 1\} = \{3, 3 + 3, 3 + 3 + 3, 3 + 3 + 3 + 3\} = \{0, 1, 2, 3\}$$

In contrast, $2 \in \mathbb{Z}_4$ generates the subgroup $< 2 >= \{2, 2 + 2\} = \{0, 2\}$.

Example 10.3.28. *$(\mathbb{Z}_5 - \{0\}, \cdot)$ is a cyclic group which can be generatr. Additionally, $(\mathbb{Z}_4, +)$ is a cyclic group with generator 3. Notice that, modulo 4 we calculate*

$$\{1, 1 + 1, 1 + 1 + 1, 1 + 1 + 1 + 1\} = \{3, 3 + 3, 3 + 3 + 3, 3 + 3 + 3 + 3\} = \{0, 1, 2, 3\}$$

In contrast, $2 \in \mathbb{Z}_4$ only generates the subgroup $< 2 >= \{2, 2 + 2\} = \{0, 2\}$.

Definition 10.3.29. *The* **order** *of a group G is the cardinality of G. The order of an element $a \in G$ is the smallest $r \in \mathbb{N}$ for which $a^r = e$. If no such r exists then the order of a is infinite.*

It turns out that order of an element and the cardinality of the subgroup generated by the element are identical. This is proved in abstract algebra[2].

Theorem 10.3.30. *If the order of a is $r \in \mathbb{N}$ then $< a >= \{a, a^2, \dots, a^{r-1}, e\}$. Moreover, $\langle a \rangle$ is an infinite set if the order of a is infinite.*

Example 10.3.31. *In Example 10.3.28 we saw that the order of 1 and 3 was 4 since $< 1 >=< 3 >= \mathbb{Z}_4$. On the other hand, the order of 2 was 2 since $< 2 >= 2\mathbb{Z}_4 = \{0, 2\}$ has just two elements.*

Notice the identity has order 1 in any group since $< 0 >= \{0\}$. In other words, the cyclic subgroup generated by the identity element is just the trivial subgroup.

Example 10.3.32. *Consider $H = \{1, 2, 3, 4\} \subset \mathbb{Z}_5$. You can check that H is a group with respect to multiplication modulo 5. Moreover, $< 1 >= \{1\}$, $< 2 >=< 3 >=< 4 >= H$. In particular,*

$$2^2 = 4, \quad 2^3 = 3 \quad 2^4 = 1.$$

We see notice that the order of 2 is 4 and we also have $2^4 = 1$. This is no accident

10.3.3 operation perserving maps

Definition 10.3.33. *Let $(A, *)$ and $(B, \circ)$ be algebraic systems. A mapping $\phi : A \to B$ is an* **operation preserving map** *iff for all $x, y \in A$, $\phi(x * y) = \phi(x) \circ \phi(y)$. If $(A, *)$ and $(B, \circ)$ are groups then an operation preserving map is called a* **homomorphism** *and $(B, \circ)$ is said to be a* **homomorphic image** *of $(A, *)$.*

Example 10.3.34. *Consider the Cayley table for $(\mathbb{Z}_2, \cdot)$ and compare it to the $A = \{x, y\}$ with operation $*$ from Example 10.3.8. It is pretty clear that 0 is like x and 1 is like y. This suggests that $\phi(0) = x$ and $\phi(1) = y$ will make $\phi : \mathbb{Z}_2 \to \{x, y\}$ an operation preserving map.*

$$\phi(0 \cdot 0) = \phi(0) = x = x * x = \phi(0) * \phi(0)$$

$$\phi(0 \cdot 1) = \phi(0) = x = x * y = \phi(0) * \phi(1)$$

$$\phi(1 \cdot 0) = \phi(0) = x = y * x = \phi(1) * \phi(0)$$

$$\phi(1 \cdot 1) = \phi(1) = y = y * y = \phi(1) * \phi(1)$$

This is not a homomorphism since $(\mathbb{Z}_2, \cdot)$ is not a group.

Example 10.3.35. *Notice that $((0, \infty), \cdot)$ is a multiplicative group and $(\mathbb{R}, +)$ is and additive group. The exponential function provides a homomorphism of these groups. In particular, $exp : \mathbb{R} \to (0, \infty)$ satisfies*

$$exp(x + y) = exp(x) \cdot exp(y)$$

The operation of addition in the domain of exp is preserved to become multiplication in the range. In fact, exp is an **isomorphism***, see below:*

[2] that is Math 421 at Liberty University

Definition 10.3.36. *If $(A, *)$ and $(B, \circ)$ are groups then an* **isomorphism** *is a homomophism which is a bijection. That is $\phi : A \to B$ is an isomorphism iff it is a bijection and for all $x, y \in A$, $\phi(x * y) = \phi(x) \circ \phi(y)$. If there is an isomorphism from $(A, *)$ to $(B, \circ)$ then the groups are said to be* **isomorphic**.

Example 10.3.37. *Show that $3\mathbb{Z}_6$ is a homomorphic image of $\mathbb{Z}_6$ as additive groups. Define $f : \mathbb{Z}_6 \to 3\mathbb{Z}_6$ by $f(z) = 3z$ for each $z \in \mathbb{Z}_6$. Let $x, y \in \mathbb{Z}_6$,*

$$f(x + y) = 3(x + y) = 3x + 3y = f(x) + f(y)$$

We can compare the Cayley tables of $3\mathbb{Z}_6 = \{0, 3\}$ and that of $\mathbb{Z}_6$ to see that $3\mathbb{Z}_6$

$+_6$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

$+_6$	0	3
0	0	3
3	3	0

The way to understand this is that in $3\mathbb{Z}_6$ the elements $\{0, 2, 4\}$ in $\mathbb{Z}_6$ have been squished to 0 in $3\mathbb{Z}_6$. On the other hand $\{1, 3, 5\}$ in $\mathbb{Z}_6$ have been squished to 3 in $3\mathbb{Z}_6$. Perhaps I can illustrate it better in lecture with some colors. It helps to reorder the rows and columns so that the identified elements are next to each other.

Example 10.3.38. *Let $(\mathbb{R}^3, +)$ be 3-dimensional vectors with the usual vector addition. Likewise suppose $(\mathbb{R}^2, +)$ are 2-dimensional vectors with the usual addition. The projection $\pi : \mathbb{R}^3 \to \mathbb{R}^2$ defined by*

$$\pi(< a, b, c >) =< a, b >$$

is a homomorphism. Observe that for all $< a, b, c >, < x, y, z > \in \mathbb{R}^3$,

$$\begin{aligned} \pi(< a, b, c > + < x, y, z >) &= \pi(< a + x, b + y, c + z >) \\ &=< a + x, b + y > \\ &=< a, b > + < x, y > \\ &= \pi(< a, b, c >) + \pi(< x, y, z >). \end{aligned}$$

Thus 2-D vectors are a homomorphic image of 3-D vectors. When I think about a homomorphism I think of a sort of shadow of an object with more intricate structure. On the other hand, isomorphic sets are essentially the same thing perhaps cast in differing notation.

Remark 10.3.39. *If you look at the last example from the perspective of our discussion at the end of the functions chapter you could identify that the fibers of π are vertical vectors. Then the space of equivalence classes squishes those vertical vectors to a point. The resulting space of equivalence classes is 2 dimensional and the naturally induced bijection would be an isomophism from the equivalence classes to $\mathbb{R}^2$. Likewise, the sets I mentioned in the last example are the fibers of f and the space of fiber-equivalence classes is isomorphic to the range of f through the natural bijection we discussed at the end of the functions chapter.*

Theorem 10.3.40. *(fun facts about homomorphisms and isomorphisms) Let $(A, *)$ and $(B, \circ)$ be groups and $\phi : A \to B$ a homomorphism,*

1. $\phi(e_A) = e_B$ *where* e_G *is the identity in* $G = A, B$.
2. $\phi(a^{-1}) = (\phi(a))^{-1}$ *for each* $a \in A$.
3. *if* ϕ *is an isomorphism then* ϕ^{-1} *is an isomorphism.*
4. *The image* $\phi(A)$ *is a subgroup of* B.

Example 10.3.41. *(loop groups) Given a space S you can form a group from the closed paths (loops) in the space. The group operation is constructed from simply pasting the paths together. The structure of the loop group will reveal things the topology of the space S. This means that abstract algebra can be used to reveal things about topology. This general type of thinking forms a branch of mathematics called* **algebraic topology**.

Example 10.3.42. *(Lie groups) A manifold with a smooth group structure is called a* **Lie group**. *The Lie algebra is in one-one correspondence with the tangent space at the identity of the Lie group. For a silly example, $exp : \mathbb{R} \to (0, \infty)$ connects the Lie group $(0, \infty)$ and the Lie algebra $\mathbb{R}$. Lie groups formed from matrices have wide-spread application in theoretical and experimental physics. Rotation groups are Lie groups. The Lorentz group from special relativity contains rotations and velocity boosts on spacetime. I have hardly even touched on the geometrical motivations for group theory in these notes. Look up Klein's Erlanger Programm to see more about this.*

Example 10.3.43. *(representation theory) One interesting goal of representation theory is to find homomorphic images of certain abstract groups (or algebras) onto matrix groups(or algebras). This is interesting because the homorphic image will naturally act on a vector space. In physics, especially quantum mechanics, the vector space contains the physical states. The symmetry group acts on the states. It "rotates" the states amongst themselves. When a symmetry commutes with the Hamiltonian then the states that rotate amongst themselves form a set of equal energy states. Most of those funny magic rules in Chemistry actually can be* **derived** *from a careful study of group theory and its application to quantum atomic physics. In mathematics and physics the term* **representation theory** *goes far beyond what I have sketched here. (by the way a "group" in physics is sometimes not a group as mathematicians think of them)*

Example 10.3.44. *(local symmetry groups) If you want a theory in which a symmetry acts at one point in space at a time then a local symmetry group is what you want. In contrast to a rotation group, the local symmetry group acts locally. Special relativity motivates the desire to use local symmetries. It turns out that a local symmetry group is not just a group. In fact, it is better described by a principle fiber bundle where the symmetry group forms the fiber. This may sound esoteric to you, but you should know that electricity and magnetism is the quintessensial example of a physical model motivated from a local symmetry. Such theories are called* **gauge theories**. *Everytime you turn on a lightswitch or watch TV you reap the benefits of understanding gauge theory. Gauge theory has been a major player in theoretical physics since the late 1950's, although it was pioneered by Weyl in 1929 for Electromagnetism. Einstein discouraged Weyl's original attempt in 1919 because his original theory infringed on the standard view of space and time. Einstein's general theory of relativity can also be phrased as a gauge theory. These are the basics for a theoretical physicist. I think it is amazing how far God has allowed human thought to progress these past few centuries.*

10.3.4 rings, integral domains and fields

Definition 10.3.45. *A* **ring** $(R, +, \cdot)$ *is a set* R *togther with two binary operations called addition* $+$ *and multiplication* $\cdot$ *that satisfy the following axioms:*

1. $(R, +)$ *is an abelian group.*
2. $(R, \cdot)$ *is an associative algebraic system*
3. *The multiplication is left and right distributive over additon. That is for all* $a, b, c \in R$ *we have*

$$a \cdot (b + c) = a \cdot b + a \cdot c, \qquad (a + b) \cdot c = a \cdot c + b \cdot c$$

If R *has a multiplicative identity then we say that* R *is a ring with unity. If* R *has a commutative multiplication then we say that* R *is a commutative ring.*

Example 10.3.46. $\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$ *and* $\mathbb{Z}$ *are all rings with respect to the natural addition and multiplication. Also* $(\mathbb{Z}_n, +_n, \cdot_n)$ *is a ring.*

Definition 10.3.47. *An* **integral domain** *is a commutative ring with unity such that* $(R, +, \cdot)$ *has no* **zero divisors***; that is if* $a \cdot b = 0$ *then either* $a = 0$ *or* $b = 0$*.*

An integral domain is a set where factoring works.

Example 10.3.48. $\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$ *and* $\mathbb{Z}$ *are all integral domains with respect to the natural addition and multiplication. Also* $(\mathbb{Z}_p, +_p, \cdot_p)$ *for* p *prime is an integral domain.*

Example 10.3.49. *Notice that* $\mathbb{Z}_4$ *is not an integral domain since* $2 \cdot 2 = 0$ *yet* $2 \neq 0$*. If* n *is not prime you can find zero divisors for* $\mathbb{Z}_n$ *from the factors of* n*. For example, in* $\mathbb{Z}_6$ *we saw that* 2 *and* 3 *are zero divisors.*

Definition 10.3.50. *A* **field** F *is a integral domain such that the multiplication restricted to* $F - \{0\}$*is closed under inverses. In other words,* F *is an commuative ring with unity such that* $(F - \{0\}, \cdot)$ *is an abelian group.*

Example 10.3.51. $\mathbb{C}$, $\mathbb{R}$ *and* $\mathbb{Q}$ *are all fields with respect to the natural addition and multiplication. Also* $(\mathbb{Z}_p, +_p, \cdot_p)$ *for* p *prime is a field. Note that* $\mathbb{Z}$ *is not a field since* $2^{-1} \notin \mathbb{Z}$*.*