MAT 200: Logic, Language and Proof
Spring 2014

Welcome to MAT 200 : Logic, Language and Proof

MAT 200 : Logic, Language and Proof
Instructor : Jaepil Lee (jefflee@math.sunysb.edu), Math Tower 3-117,
Office hour : Mon 1:00 - 2:00
Grader : Holly Chen(holly@math.sunysb.edu)
Math Tower 5-125B, Office Hour : Thur 10:00 - 11:30

Announcements

Announcements are listed in reverse choronological order: most recent announcement at the top.

5/15/2014
Expected letter grades have been posted in Blackboard.

5/9/2014
The final exam will be given on Tuesday, 5/13/14 8:30 PM to 11:00 PM(finalized). Location is Frey Hall 217.

5/8/2014
Practice exam solution for final is uploaded.

5/3/2014
Practice exam for final is uploaded.

5/3/2014
The final exam will be given on Tuesday, 5/13/14 8:30 PM to 11:00 PM. Location is TBA.

4/26/2014
Homework 8 updated.

4/16/2014
Homework 7 is also used to boost one of your midterm grade. You will need to specify which exam you want to be boosted. The grade boost will be computed as follows.
- If your grade is less than average, then ((average) - (your current grade)) * 0.75
- If your grade is above than average, then plus two points.

4/16/2014

Current averages of exams and homework
Exam 1 : 28.92, Exam 2 : 39.22, HW1 : 5, HW2 : 4.43, HW3 : 3.46, HW4 : 8.54, HW5 : 10.89

4/01/2014
Midterm 2 will be given on April 9, on class.

4/01/2014
Practice exam for midterm 2 updated(you can find it from "Exams" on your left). No homework on this week. Prepare for the exam.

3/26/2014
Homework 6 updated.

3/19/2014
Homework 5 updated. Sorry for the delay!

3/10/2014
Stony Brook Geometry Notes updated. You may find it from syllabus page.

3/10/2014
Exam 1 statistics : Average 28.62, Standard Deviation 15.75

3/5/2014
Homework 4 updated.

3/3/2014
Practice exam solution uploaded.

2/26/2014
Midterm 1 will be on Mar 5, Wednesday, 4:00 - 5:20pm, at Frey Hall 217

2/26/2014
A readable note on Zermelo-Fraenkel axiomatic set theory from University of Chicago.

2/25/2014
Practice exam for midterm 1 updated(you can find it from "Exams" on your left). No homework on this week.

2/19/2014
Homework 3 updated.

2/11/2014
Homework 2 updated.

2/5/2014
Due to the severe weather condition, all classes on this week have been canceled. Due date of Homework is also extended to Feb 10(Mon), in class.

1/28/2014

First Homework updated. You may find it from "Syllabus".

1/23/2014

Web page created. Syllabus uploaded.

General Information

Information for students with disabilities

If you have a physical, psychological, medical, or learning disability that may impact your course work, please contact Disability Support Services at (631) 632-6748 or http://studentaffairs.stonybrook.edu/dss/. They will determine with you what accommodations are necessary and appropriate. All information and documentation is confidential.

Students who require assistance during emergency evacuation are encouraged to discuss their needs with their professors and Disability Support Services. For procedures and information go to the following website: http://www.sunysb.edu/ehs/fire/disabilities.shtml

MAT 200: Logic, Language and Proof
Spring 2014

Syllabus

Textbook : *Peter J. Eccles: An Introduction to Mathematical Reasoning: numbers, sets and functions* and *Stony Brook's own* ***Geometry Notes***.

Schedule and classroom : MW 4:00 - 5:20pm, Frey Hall 217

Course Description : This course will provide skills to argue rigorous reasonings and proofs used in upper-division mathematics course. We will begin with basic logical language and general usage of it. Then we move on fundamental objects of mathematics - sets and functions between them. Later part of the course will be dedicated to application of mathematical logics to Euclidean geometry and number theory.

Homework : Homework will be assigned in weekly basis. We will put emphasis on written argument or proof, so try to give your own argument with clear and legit reasoning. Sometimes homework problems whose solution may be found in your textbook may be assigned. Although such problems may not be graded, but students should put same emphasis on them.

Exams and Grading : Final grading will be given based on following criteria.

Exam 1	25%
Exam 2	25%
Final	30%
Homework	20%

Information for students with disabilities : If you have a physical, psychological, medical, or learning disability that may impact your course work, please contact Disability Support Services at **http://studentaffairs.stonybrook.edu/dss/** or (631) 632-6748. They will determine with you what accommodations are necessary and appropriate. All information and documentation is confidential.

Students who require assistance during emergency evacuation are encouraged to discuss their needs with their professors and Disability Support Services. For procedures and information go to the following website:

http://www.stonybrook.edu/ehs/fire/disabilities.shtml

Academic Integrity : Each student must pursue his or her academic goals honestly and be personally accountable for all submitted work. Representing another person's work as your own is always wrong. Faculty are required to report any suspected instances of academic dishonesty to the Academic Judiciary. For more comprehensive information on academic integrity, including categories of academic dishonesty, please refer to the academic judiciary website at
http://www.stonybrook.edu/uaa/academicjudiciary/

Schedule
This is the brief course plan. Since the schedule is tentative and subject to change, so make sure to visit the course web page in regular basis.

Week of Jan 27 : Language of mathematics, Implications
Exercise 1.2, 1.3, 1.4, 2.1, 2.3, 2.4, 2.5, Due on Feb 5, in class.

Week of Feb 3 : All classes has been canceled due to severe weather condition. Keep watching Stony Brook weather announcement.

Week of Feb 10 : Proofs, Proof by contradiction, Induction principle
*Homework of this week can be found **here**. Due on Feb 19, in class.*

Week of Feb 17 : Induction Principle(continued), Language of set theory
*Homework of this week can be found **here**. Due on Feb 26, in class.*

Week of Feb 24 : quantifiers, Functions, Injections, surjections and bijections
There is no homework on this week.

Week of Mar 3 : Review, Midterm I
*Homework of this week can be found **here**. Due on Mar 12, in class.*

Week of Mar 10 : Geometry note 1-4(introduction, axioms)
***Geometry note**.*

Week of Mar 17 : Spring recess
*Homework of this week can be found **here**. Due on Mar 26, in class.*

Week of Mar 24 : Geometry note 5(triangles)
*Homework of this week can be found **here**. Due on Apr 2, in class.*

Week of Mar 31 : Geometry note 6, 7(parallels, similarity and Pythagoras)
Week of Apr 7 : Midterm II, Counting
Week of Apr 14 : Properties of finite set, Counting functions and subset
*Homework of this week can be found **here**. Due on Apr 23, in class.*

Week of Apr 21 : Number system, Modular arithmetic
*Homework of this week can be found **here**. Due on May 5, in class.*

Week of Apr 28 : Linear congruence, Congruence classes
Week of May 5 : Partitions and equivalence relations

MAT 200
COURSE NOTES ON GEOMETRY

STONY BROOK MATHEMATICS DEPARTMENT

Revised: Spring, 2008

Contents

1. Introduction

The treatment of Euclidean geometry you will find presented in these notes is loosely based[1] on an approach proposed by Garrett Birkhoff in 1932. Birkhoff, in turn, was heavily influenced by earlier work of David Hilbert (1899) and Morris Pasch (1882). However, all of these approaches — and indeed, virtually all other approaches to axiomatic plane geometry — are essentially refinements of Euclid's classical treatise, the *Elements*. The latter text, written about 300 BC, provided such a beautifully logical development of plane geometry that its absolute authority remained essentially unchallenged for well over 2000 years.

1.1. Euclidean geometry as an axiomatic theory.

Euclidean geometry tries to describe geometric properties of various subsets of *the plane*. The geometric figures we will discuss should be understood to be sets of points; we will use capital letters for points and write $P \in m$ for "the point P belongs to the figure m," or "the figure m contains the point P." The notion of "point" is taken to be fundamental, and we will not attempt to explain it in terms of simpler notions. There are some other basic notions (line, distance, angle measure) that are also left undefined. Instead, we will simply postulate some *rules* which these objects obey; these "postulates" are usually called the "axioms of Euclidean geometry." **All results in Euclidean geometry should be proved by deducing them from the axioms**; justifications such as, "it is obvious," "it is well-known," or "it is clear from the figure" are not acceptable. We allow use of all tautologies and laws of logic. We also assume standard facts about the real numbers and their properties.

Although a monumental achievement of classical civilization, Euclid's *Elements* must unfortunately be judged to be somewhat deficient by current mathematical standards of clarity and rigor. For this reason, various modern authors have developed their own systematic ways of remedying the limitations of Euclid's framework. As there are, however, several different but equally satisfactory ways of accomplishing this, different modern books on geometry typically use slighlty different sets of axioms. For this reason, you are advised to exercise considerable care when comparing these notes to any other treatment of the subject.

1.2. Basic objects.

The following concepts are the bedrock on which we will build our theory. No attempt will be made to define or explain them in terms of anything simpler. However, everything else in these notes will be defined in terms of these basic notions.

- Points: the *plane* is assumed to consist of elements, called points.
- Lines: certain special subsets of the plane will be called lines;
- Distances: for any two points A and B, it is assumed that there is a real number $|AB|$, called the *distance* between A and B.
- Angle measures: we will eventually introduce some special geometric figures, called *angles*. For every angle $\angle ABC$, it will be assumed that there there is an associated real number $m\angle ABC$, called the *measure* of the angle.

[1] In writing these notes, Stony Brook faculty members made use of numerous secondary sources, including textbooks by G. E. Martin, by E. G. Golos, and by C. R. Wylie, Jr.

2. Incidence Axioms

In this section, we introduce the first axioms which deal with lines, points, and the relation that "the point P lies on the line l." This relation is often called an *incidence* relation; hence the name of this section. We will not discuss distances or angles yet; they will be treated later by other axioms.

2.1. First Concepts.

Definition 2.1. Two lines l, m are said to be transverse if they are *distinct* ($l \neq m$) and have at least one point in common. When this is true, we will write $l \pitchfork m$.

This is slightly different from saying that l and m intersect as point sets. (Why?) Nonetheless, the word intersecting is often used to mean "transverse" in contexts where this is unlikely to cause any confusion.

Definition 2.2. Two lines l and m are called parallel if they are not transverse. When this is true, we will write $l \| m$.

Notice that, by this definition, any line is parallel to itself.

Exercise 2.1: Show that two lines l and m are parallel iff either

- $l \cap m = \emptyset$; or
- $l = m$.

Exercise 2.2: Show that $l \| m \iff m \| l$.

2.2. Incidence and Parallel lines Axioms.

Incidence Axiom.

1. *There are at least two distinct points.*
2. *For any two distinct points, there is a unique line that contains these two points.*
3. *For any line, there exists a point not on this line.*

We will denote the unique line containing points A, B by $\overleftrightarrow{AB}$.

Parallel Axiom. *For any line l and a point P not on l, there exists a unique line containing P and parallel to l.*

2.3. First theorems.

Theorem 2.1. *The intersection of two transverse lines consists of exactly one point.*

Exercise 2.3: Prove this theorem.

Definition 2.3. Two transverse lines are said to meet at their unique point of intersection.

Theorem 2.2. *For any lines l, m, n, if $l \| m$ and $m \| n$, then $l \| n$.*

Exercise 2.4: Prove this theorem.

Exercise 2.5: Let A, B, C be distinct points such that C lies on the line $\overleftrightarrow{AB}$. Show that then A lies on the line $\overleftrightarrow{BC}$.

Exercise 2.6: Lel l, m, n be lines such that $l \| m$ and $n \pitchfork l$. Show that $n \pitchfork m$.

2.4. Historical remarks. Our Parallel Axiom corresponds to the Fifth Postulate in Euclid's classical treatment. Starting in the Middle Ages, some scholars wondered whether it was redundant, in the sense that it might actually be a logical consequence of Euclid's other postulates. In the 1830's, however, Bolyai and Lobachevsky independently became convinced that this could *not* be the case, and proposed a conjectural alternative geometry, in which the Parallel Axiom fails, but all the other axioms of Euclidean geometry still hold. Half a century later, the logical consistency of this alternative geometry was definitively proved by Klein and Poincaré, who constructed explicit coordinate models of the so-called "non-Euclidean plane" or "hyperbolic plane". For a wonderfully readable, yet mathematically precise account, see Hilbert and Cohn-Vossen, **Geometry and the Imagination**, §§34-35.

3. Ruler Axiom

In this section we impose a new axiom which describes properties of distance and order relation for points on a line.

3.1. Ruler Axiom.

Ruler Axiom. *Let l be any line. Then there is a one-to-one correspondence $f: l \to \mathbb{R}$ such that, for any two points A, B on l, $|AB| = |f(A) - f(B)|$.*

Here the statement that f is a one-to-one correspondence means that for every $t \in \mathbb{R}$, there is exactly one point $P \in l$ such that $f(P) = t$. In particular, we must have $f(P) \neq f(Q)$ whenever $P \neq Q$.

This axiom roughly says that any line "looks like" the usual number line $\mathbb{R}$. This allows us to use known properties of $\mathbb{R}$ to prove many results about points on lines.

A one-to-one correspondence $f: l \to \mathbb{R}$ with the distance property stipulated by the Ruler Axiom is called a coordinate system on l. It is not unique: there are many coordinate systems on a given line.

Exercise 3.1: Suppose that $f: l \to \mathbb{R}$ is a coordinate system on the line l, and let $c \in \mathbb{R}$ be any real constant. Define $g: l \to \mathbb{R}$ and $h: l \to \mathbb{R}$ by

$$\begin{aligned} g(A) &= c + f(A) \\ h(A) &= c - f(A) \end{aligned}$$

for all $A \in l$. Show that g and h are also coordinate systems on l.

Theorem 3.1. *Let P and Q be distinct points. Then there exists a coordinate system f on the line $\overleftrightarrow{PQ}$ such that $f(P) = 0$ and $f(Q) > 0$.*

Exercise 3.2: Prove this theorem, using Exercise 3.1.

Exercise 3.3: Let f be a coordinate system on $\overleftrightarrow{PQ}$ which satisfies the conditions of Theorem 3.1. For every $A \in \overleftrightarrow{PQ}$, show that

$$f(A) = \begin{cases} |PA|, & \text{if } |QA| < |QP| \text{ or } |QA| < |PA| \\ -|PA|, & \text{otherwise.} \end{cases}$$

(Hint: if c is a positive constant, first show that a real number x is positive iff either $|x-c| < c$ or $|x-c| < |x|$.) Then use this to show that the added conditions stipulated by Theorem 3.1 in fact determine a **unique** coordinate system on $\overleftrightarrow{PQ}$.

Exercise 3.4: Let f be the coordinate system on $\overleftrightarrow{PQ}$ given by Theorem 3.1. If g is any coordinate system on $\overleftrightarrow{PQ}$ for which $g(P) < g(Q)$, use Exercise 3.3 to show that

$$g(A) = c + f(A),$$

where $c = g(P)$. Similarly, if h is any coordinate system on $\overleftrightarrow{PQ}$ for which $h(P) > h(Q)$, show that

$$h(A) = c - f(A),$$

where $c = h(P)$.

3.2. Order on a line.

Definition 3.1. Let A, B, C be points on a line l. We say that B is between A and C if there is a coordinate system f on l such that $f(A) < f(B) < f(C)$. When this is true, we write $A - B - C$.

Exercise 3.5: Show that $A - B - C$ iff $C - B - A$.

Exercise 3.6: Let g be *any* coordinate system on a line l. If A, B, C are three points of l, use Exercise 3.4 to show that $A - B - C$ iff either $g(A) < g(B) < g(C)$ or $g(A) > g(B) > g(C)$.

Definition 3.2. Let A, B be distinct points. Then the segment $\overline{AB}$ is the set of all points C on the line $\overleftrightarrow{AB}$ such that $A - C - B$.

Note that according to this definition, the endpoints A and B are not included in $\overline{AB}$.

Definition 3.3. Let A, B, C be points on a line l, where $A \neq C$ and $B \neq C$. Then we will say that A and B are on opposite sides of C if $A - C - B$. On the other hand, we will say that A and B are on the same side of C if they are **not** on opposite sides of C.

Exercise 3.7: Let A, B, C be points on a line l, where $A \neq C$ and $B \neq C$. Show that A and B are one the same side of C iff one of the following holds:

- $A = B$:
- $C - A - B$; or
- $C - B - A$.

Theorem 3.2.

(1) *Given three distinct points on a line, exactly one of them lies between the other two.*
(2) *Let A, B, C, D be points on a line l, and suppose that none of the other three points is equal to D. If A and B are on the same side of D, and if B and C are on the same side of D, then A and C are on the same side of D.*

Exercise 3.8: Prove this theorem.

Theorem 3.3. *Let V be a point on the line l. Then the complement of V in l is the union of two disjoint subsets $\mathcal{R}_1$ and $\mathcal{R}_2$, such that*

- *if $A, B \in \mathcal{R}_1$, then A and B are on the same side of V;*
- *if $A, B \in \mathcal{R}_2$, then A and B are on the same side of V; but*
- *if $A \in \mathcal{R}_1$ and $B \in \mathcal{R}_2$, then A and B are on opposite sides of V.*

The subsets $\mathcal{R}_1$ and $\mathcal{R}_2$ of l are called rays, or half-lines.

In other words, any point on a line "divides the line into two rays."

Proof. Choose a coordinate system on l such that $f(V) = 0$; by Theorem 3.1, such a coordinate system exists. Define $\mathcal{R}_1$ to consist of those points A with $f(A) > 0$, and define $\mathcal{R}_2$ to consist of those points A with $f(A) < 0$. The stated properties of $\mathcal{R}_1$ and $\mathcal{R}_2$ then follow from the fact that 0 lies between two real numbers iff one is positive and one is negative. □

Definition 3.4. Let V and A be distinct points. By Theorem 3.3, V then divides the line $\overleftrightarrow{VA}$ into two rays, and exactly one of these rays will contain A. We will denote this preferred ray by $\overrightarrow{VA}$.

Theorem 3.4. *Let $\overrightarrow{VA}$ be a ray, and suppose $B \in \overrightarrow{VA}$. Then $\overrightarrow{VB} = \overrightarrow{VA}$.*

Exercise 3.9: Prove this theorem.

3.3. PROPERTIES OF DISTANCE. Here are some easy but useful consequences of the Ruler Axiom.

Theorem 3.5. *For any A, B, $|AB| \geq 0$. Moreover, $|AB| = 0$ iff $A = B$.*

Exercise 3.10: Prove this theorem.

Theorem 3.6. *Let A, B, C be distinct points such that $B \in \overline{AC}$. Then*

$$|AB| + |BC| = |AC|.$$

Exercise 3.11: Prove this theorem.

Exercise 3.12: Let $\overrightarrow{VA}$ be a ray, and let r be a positive real number. Show that there is a unique point P on the ray $\overrightarrow{VA}$ such that $|VP| = r$.

Exercise 3.13: If $B \in \overrightarrow{VA}$ and $|VB| < |VA|$, then $V - B - A$.

Exercise 3.14: Let A and B be distinct points. Show there exists a unique point M on the segment $\overline{AB}$ such that $|AM| = |MB|$. (This point is called the midpoint of $\overline{AB}$.)

4. Protractor Axiom

The purpose of this section is to discuss angles and their measures. Before we can do so, however, we will first need to introduce the notion of a *half-plane*.

Definition 4.1. Let l be a line in the plane, and let P and Q be points which are not on l. Then we will say that P and Q are on opposite sides of l if $P \neq Q$ and the line segment $\overline{PQ}$ meets l. We will say that P and Q are on the same side of l if they are not on opposite sides of l.

4.1. Plane separation axiom.

Plane Separation Axiom. *Let l be a line, and let P, Q, and R be three points which do not lie on l.*

1. *If P and Q are on the same side of l, and if Q and R are on the same side of l, then P and R are also on the same side of l.*
2. *If P and Q are on opposite sides of l, and if Q and R are on opposite sides of l, then P and R are both on the same side of l.*

Now, given a line l, the Incidence Axiom tells us that there is a point $P \notin l$. We can then also find a point R which is on the opposite side of l from P, for instance by choosing some point $A \in l$, and then using the ruler axiom to find a point $R \in \overleftrightarrow{PA}$ such that $P - A - R$. Thus, we can always find two points P and R on opposite sides of any line l.

Now, given two such points P and R on opposite sides of a line l, consider the *contrapositive* of the first part of the Plane Separation Axiom. This tells us that any third point $Q \notin l$ is either on the opposite side of l from P, or else on the opposite side of l from R. But the second part of the axiom, together with our assumption that P and R are on opposite sides, then tells us that either Q is on the same side of l as R, or else on the same side of l as P. And *both* cannot hold, since the first part of the axiom would otherwise allow us to conclude that P and R were on the same side, in contradiction with our assumption. Thus every point $Q \notin l$ must belong to one of the sets

$$\begin{aligned} \mathcal{H}_1 &= \{\text{points on same side of } l \text{ as } P\} \\ \mathcal{H}_2 &= \{\text{points on same side of } l \text{ as } R\} \end{aligned}$$

but no point can possibly belong to both. We have therefore proved the following result:

Theorem 4.1. *The complement of any line l is the union of two disjoint non-empty sets $\mathcal{H}_1$ and $\mathcal{H}_2$, such that*

- *If $A, B \in \mathcal{H}_1$, then A and B are on the same side of l;*
- *If $A, B \in \mathcal{H}_2$, then A and B are on the same side of l; and*
- *If $A \in \mathcal{H}_1$ and $B \in \mathcal{H}_2$, then A and B are on opposite sides of l.*

Definition 4.2. The two subsets $\mathcal{H}_1$ and $\mathcal{H}_2$ in the above theorem are called *half-planes*

Thus, the plane separation axiom essentially says that *any line divides the plane into two half-planes.*

4.2. Angles and their interiors.

Definition 4.3. An angle is the figure consisting of a point A and two *distinct* rays starting at A. The angle formed by rays $\overrightarrow{AB}$ and $\overrightarrow{AC}$ is denoted by $\angle BAC$.

Later in these notes, we will sometimes use the abbreviated notation $\angle A$ for $\angle BAC$ if it is absolutely clear from the context which rays form the sides of the angle.

Definition 4.4. We will say that $\angle BAC$ is a straight angle if $A \in \overline{BC}$.

Exercise 4.1: Show that an angle $\angle BAC$ is a straight angle iff there is a single line which contains all three of the points A, B, C.

Definition 4.5. Suppose that $\angle BAC$ is not a straight angle. Then the interior of $\angle BAC$ is the set of those points which are simultaneously

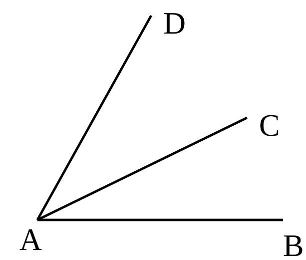
- on the same side of $\overleftrightarrow{AB}$ as C; and
- on the same side of $\overleftrightarrow{AC}$ as B.

By contrast, when $\angle BAC$ *is* a straight angle, we will allow ourselves to choose a half-plane on one side of $\overleftrightarrow{BC}$, and then refer to this chosen half-plane as the "interior" of $\angle BAC$. (Of course, however, the opposite half-plane would have made an equally valid choice).

Exercise 4.2: If $\angle BAC$ is not a straight angle, D lies in the interior of $\angle BAC$ iff

- $D \notin \overleftrightarrow{AB}$;
- $D \notin \overleftrightarrow{AC}$;
- $\overline{DB} \cap \overleftrightarrow{AC} = \emptyset$; and
- $\overline{DC} \cap \overleftrightarrow{AB} = \emptyset$.

Exercise 4.3: If C lies in the interior of $\angle BAD$, show that every other point of $\overrightarrow{AC}$ lies in the interior of $\angle BAD$, too. In this case, we will say that $\overrightarrow{AC}$ lies inside of $\angle BAD$.



4.3. Angle measure. One of the basic undefined notions of Euclidean geometry is that of *angle measure*: it is assumed that for each angle $\angle ABC$, there is an associated positive real number $m\angle ABC$ called the measure of $\angle ABC$. No attempt is made to give a definition of this measure. Instead, the Protractor Axiom below simply specifies some of its properties. It is common to use Greek letters $\alpha, \beta, \gamma, \ldots, \varphi, \theta$ for angle measures.

4.4. Historical note. The phrase "measure of an angle" is actually relatively modern. Up to about 50 years ago, the measure of the angle at A was simply denoted by A or $\angle A$, and it was left to the reader to distinguish between the angle and its measure. When convenient, we will follow this convention, and use the same notation for an angle and its measure.

4.5. The Protractor axiom.

Protractor Axiom.

(1) *For any angle $\angle BAC$, $0 < m\angle BAC \leq \pi$.*
(2) *If $\angle BAC$ is a straight angle, then $m\angle BAC = \pi$.*
(3) *Let A, B be distinct points, and let $\mathcal{H}$ be one of half-planes into which $\overleftrightarrow{AB}$ divides the plane. Then, for any $\alpha \in \mathbb{R}$ with $0 < \alpha < \pi$, there exists a unique ray $\overrightarrow{AC}$ in the half-plane $\mathcal{H}$ such that $m\angle BAC = \alpha$.*
(4) *If ray $\overrightarrow{AC}$ lies inside $\angle BAD$, then $m\angle BAD = m\angle BAC + m\angle CAD$.*

Note that we measure the angles in radians, so that the measure of straight angle is π rather than 180. Also, we always measure the smaller of the two sectors formed by two rays, so the measure of any angle is at most π.

Exercise 4.4: Let A, B be distinct points, and let $\mathcal{H}$ be one of the half-planes into which $\overleftrightarrow{AB}$ divides the plane. For any real numbers r and α such that $r > 0$ and $0 < \alpha < \pi$, show there exists a unique point C in $\mathcal{H}$ such that $|AC| = r$ and $m\angle BAC = \alpha$. (Please note that you can only use the results we have proved; in particular, we do not yet know anything about circles!)

4.6. When rays are inside an angle. We now come to two important results characterizing when a ray lies inside an angle. First of all, we have:

Theorem 4.2 (Monotonicity of angles). *Let A, B, C, D be distinct points such that C and D lie on the same side of the line $\overleftrightarrow{AB}$. Then $m\angle BAD < m\angle BAC$ iff $\overrightarrow{AD}$ is inside the angle $\angle BAC$.*

Exercise 4.5: Show that, without the assumption that C, D lie on the same side of $\overleftrightarrow{AB}$, Theorem 4.2 would be false.

Exercise 4.6: Prove Theorem 4.2.

The second result discussed in this section is much more subtle:

Theorem 4.3 (Crossbar Theorem). *Suppose that $\angle BAC$ is a non-straight angle. Then the ray $\overrightarrow{AD}$ is inside of $\angle BAC$ if and only if $\overrightarrow{AD}$ meets the segment $\overline{BC}$.*

In one direction, this is actually straightforward:

Exercise 4.7: Suppose the $\overrightarrow{AD}$ meets the segment $\overline{BC}$. Show that $\overrightarrow{AD}$ is inside of $\angle BAC$.

Part of the other direction is fairly manageable, too:

Exercise 4.8: Suppose that $\angle BAC$ is a non-straight angle, and that $\overrightarrow{AD}$ is inside of $\angle BAC$. Show that either

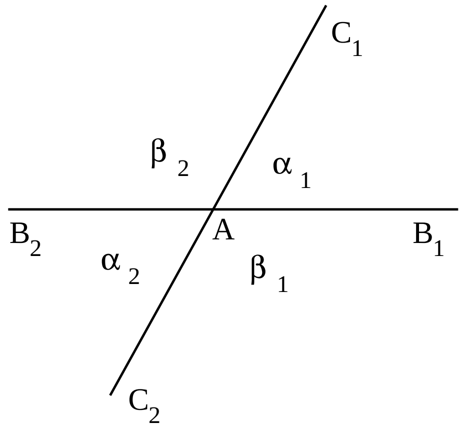
- the ray $\overrightarrow{AD}$ meets the segment $\overline{BC}$; or else
- the lines $\overleftrightarrow{AD}$ and $\overleftrightarrow{BC}$ are parallel.

(Use the fact that every point of $\overleftrightarrow{BC}$ is either on the same side of $\overleftrightarrow{AB}$ as D, or else on the same side of $\overleftrightarrow{AC}$ as D. Then show than any element of $\overleftrightarrow{AD}$ which has one of these properties actually has both.)

To prove Theorem 4.3, it therefore suffices to show that $\overleftrightarrow{AD}$ and $\overleftrightarrow{BC}$ cannot be parallel. In Exercise 6.1 below, you will be able to give a proof of this remaining fact, assuming the Parallel axiom. We remark in passing, however, that Theorem 4.3 can actually be shown to hold *without* assuming the Parallel axiom; it is true even in "non-Euclidean" geometry. Such a proof, however, is much more difficult, and lies beyond the scope of the present notes.

4.7. Vertical and supplementary angles. Let l, m be distinct lines intersecting at point A. Then these lines define four angles as shown in the figure below (again, this can be proved but we omit the proof). In this situation, two angles are called supplementary if they have a common side; otherwise, they are called vertical. Thus, in the figure below angles

$\angle B_1AC_1$ and $\angle C_1AB_2$ are supplementary, while $\angle B_1AC_1$ and $\angle B_2AC_2$ are vertical.



Theorem 4.4.

(1) *The sum of the measures of any two supplementary angles is* π.
(2) *Any two vertical angles have equal measure.*

Proof. (1) By part (4) of the Protractor Axiom, the sum of the measures of supplementary angles is equal to the measure of a straight angle. But by part (b) of the same axiom, the measure of the straight angle is π.

(2) Let α_1, α_2 and β_1, β_2 be the measures of two pairs of vertical angles, arranged as in the figure above. Then by part (a), $\alpha_1 + \beta_1 = \pi$. But also by part (a), $\alpha_2 + \beta_1 = \pi$. Subtracting these equalities, we get $\alpha_1 = \alpha_2$. In a similar way one proves that $\beta_1 = \beta_2$.

□

This result shows that when we have two intersecting lines, they define two different angle measures, α and $\beta = \pi - \alpha$. The "measure of the angle between two lines" is therefore ambiguous and undefined; one would need specify *which* of these is being used in order to give this phrase a precise meaning.

5. Triangles

5.1. Basics. A triangle is a figure consisting of three points, A, B, C, not lying on one line, and the three segments connecting them, $\overline{AB}$, $\overline{BC}$, $\overline{AC}$. The points A, B, C are called the vertices of the triangle, and the segments $\overline{AB}$, $\overline{BC}$, and $\overline{AC}$ are called its sides. A triangle with vertices A, B, C is denoted $\triangle ABC$.

Each triangle defines three angles, $\angle BAC, \angle ABC, \angle BCA$. In this context, it is common to use the abbreviated notation $\angle A, \angle B, \angle C$ if it is clear which triangle is being discussed.

Thus, every gives six real numbers: measures of the three angles and lengths of the three sides. It is common to denote $\alpha = m\angle A, \beta = m\angle B, \gamma = m\angle C$ and $a = |BC|, b = |AC|, c = |AB|$

This definition formalizes our intuitive picture of a triangle as something built out of three sticks joined together at the ends.

5.2. Congruence.

Definition 5.1. Two triangles, $\triangle ABC$ and $\triangle A'B'C'$, are congruent if the corresponding angles have equal measures, and the corresponding sides have equal lengths. That is, the triangles $\triangle ABC$ and $\triangle A'B'C'$ are congruent iff the following six conditions hold:

$$\begin{aligned} m\angle A &= m\angle A' \qquad |AB| = |A'B'| \\ m\angle B &= m\angle B' \qquad |AC| = |A'C'| \\ m\angle C &= m\angle C' \qquad |BC| = |B'C'| \end{aligned}$$

When this is true, we will write $\triangle ABC \cong \triangle A'B'C'$.

Please note that writing $\triangle ABC \cong \triangle A'B'C'$ not only indicates that the two triangles are congruent, but also says that they are congruent in such a way that vertex A corresponds to vertex A', B to B', and C to C'.

Informally, the notion of congruence has the following intuitive meaning: If you imagine a triangle as a physical object, constructed of sticks joined at their ends, then two triangles are congruent if you can put one on top of another so that they exactly match. (Note that you are allowed to turn a triangle "face down" in the process.) Euclid takes this for granted, but unfortunately never defines what "moving" a triangle is supposed to mean! In fact, many modern approaches to Euclidean geometry *do* rigorously define "rigid motions" of geometric figures, via special transformations of the plane known as "isometries." But it is often the case in mathematics that one can actually accomplish a surprising amount by simply formalizing a few aspects of an intuitive idea, and then pursuing the logical ramifications of the resulting abstract concept. This is the point of view we will adopt herein.

5.3. The SAS congruence Axiom. The following is often called the SAS Axiom:

Side-Angle-Side Congruence Axiom. *If $\triangle ABC$ and $\triangle A'B'C'$ are triangles such that*

$$m\angle ABC = m\angle A'B'C', \ |AB| = |A'B'|, \quad \text{and} \quad |BC| = |B'C'|,$$

then $\triangle ABC \cong \triangle A'B'C'$.

One can also try other ways to specify a triangle in terms of three pieces of information, such as three sides (SSS), three angles (AAA), two angles and a side, or two sides and an angle. For two angles and a side, there are two possibilities, one in which the side connects the two angles (ASA), and one in which it does not (AAS). For two sides and an angle, there are also two possibilities, one in which the two sides are adjacent to the given angle (SAS) and the other in which one is not (SSA).

Exercise 5.1: Convince yourself that SSS and ASA do define a triangle up to congruence, but AAA and SSA do not. (We currently do not have enough tools to prove this rigorously, so here you are merely being asked to draw some convincing diagrams.)

Exercise 5.2: Let A, B, C, D be points such that no three of them lie on a line, the segments $\overline{AC}$ and $\overline{BD}$ intersect, and the intersection point M is the midpoint (see Exercise 3.14) for each of them. Show that

(1) $\triangle AMD \cong \triangle CMB$
(2) $|AD| = |BC|, |AB| = |CD|$
(3) $m\angle ABD = m\angle BDC$
(4) $m\angle ABC = m\angle ADC$.

(In §6.5, we will see that this shows that the quadrilateral $\lozenge ABCD$ is a parallelogram.)

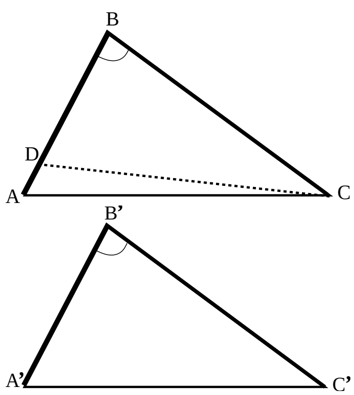
5.4. Congruence via ASA.

Theorem 5.1 (ASA). *If $\triangle ABC$ and $\triangle A'B'C'$ are triangles such that*

$$m\angle ABC = m\angle A'B'C',\ |BC| = |B'C'|, \quad \textit{and} \ \ m\angle ACB = m\angle A'C'B',$$

then $\triangle ABC \cong \triangle A'B'C'$.

Proof. Suppose we are given two triangles $\triangle ABC$ and $\triangle A'B'C'$ which satisfy these hypotheses. If $|AB|$ and $|A'B'|$ were the same, we could just invoke the SAS Axiom.



So let us instead suppose that they are different, and show that this leads to a contradiction. Without loss of generality, assume that $|A'B'| < |AB|$; otherwise, just exchange the names of the two triangles.

By the Ruler Axiom, we can find a point D on $\overrightarrow{BA}$ such that $|BD| = |B'A'|$. Since $|BD| < |BA|$, D is between A and B, and $\overrightarrow{CD}$ is therefore inside $\angle ACB$. Hence $m\angle DCB < m\angle ACB$ by Theorem 4.2. But $\triangle DCB \cong \triangle A'C'B'$ by the SAS Axiom. Hence $m\angle DCB = m\angle A'C'B'$. But $m\angle A'C'B = m\angle ACB$ by hypothesis. Thus

$$m\angle DCB = m\angle A'C'B = m\angle ACB > m\angle DCB.$$

Therefore $m\angle DCB > m\angle DCB$, which is a contradiction. Hence $|AB| = |A'B'|$, and $\triangle ABC \cong \triangle A'B'C'$ by SAS. □

Exercise 5.3: In this proof, some of the references to our previous results are actually less precise than could be desired. In some cases, for example, it might better to refer, not to an axiom or theorem, but rather to an associated exercise; in other places, no justification has been given, but some citation would clearly be appropriate. Carefully check each step in the proof, listing each such imprecision you find, and indicating the manner in which each could be improved.

5.5. Isosceles triangles. A triangle is isosceles if two of its sides have equal length. The two sides of equal length are called legs; the point where the two legs meet is called the apex of the triangle; the other two angles are called the base angles of the triangle; and the third side is called the base.

While an isosceles triangle is defined to be one with two sides of equal length, the next theorem tells us that is equivalent to having two angles of equal measure.

Theorem 5.2 (Base angles equal)**.** *If $\triangle ABC$ is isosceles, with base $\overline{BC}$, then $m\angle B = m\angle C$.* *Conversely, if $\triangle ABC$ has $m\angle B = m\angle C$, then it is isosceles, with base $\overline{BC}$.*

Exercise 5.4: Prove Theorem 5.2 by showing that $\triangle ABC$ is congruent to its reflection $\triangle ACB$. Note that there are two parts to the theorem, and so you need to give essentially two separate arguments.

5.6. Congruence via SSS.

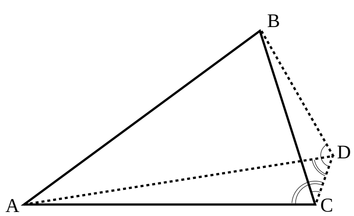
Theorem 5.3 (SSS)**.** *If $\triangle ABC$ and $\triangle A'B'C'$ are such that $|AB| = |A'B'|$, $|AC| = |A'C'|$ and $|BC| = |B'C'|$, then $\triangle ABC \cong \triangle A'B'C'$.*

Proof. If the two triangles were not congruent, then one of the angles of $\triangle ABC$ would have measure different from the measure of the corresponding angle of $\triangle A'B'C'$. If necessary, relabel the triangles so that $\angle A$ and $\angle A'$ are two corresponding angles which differ, with $m\angle A' < m\angle A$.

We find a point D and construct the ray $\overrightarrow{AD}$ so that $m\angle DAB = m\angle A'$, and $|AD| = |A'C'|$. (That this can be done follows from Exercise 4.4) It is unclear where the point D lies: it could lie inside triangle ABC; it could lie on the line $\overleftrightarrow{BC}$ between B and C; or it could lie on the other side of the line $\overleftrightarrow{BC}$. We need to take up these three cases separately.

Exercise 5.5: Suppose the point D lies on the line $\overleftrightarrow{BC}$. Explain why this yields an immediate contradiction.

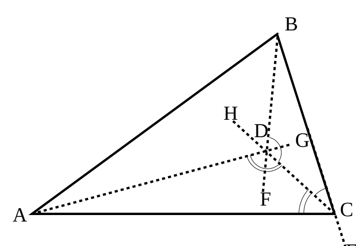
For both of the remaining cases, we draw the segments $\overline{BD}$ and $\overline{CD}$. We observe that, by SAS, $\triangle ABD \cong \triangle A'B'C'$. It follows that $|BD| = |B'C'| = |BC|$ and that $|AD| = |A'C'| = |AC|$. Hence $\triangle BDC$ is isosceles, with base $\overline{DC}$, and $\triangle ADC$ is isosceles with base $\overline{CD}$. Since the base angles of an isosceles triangle have equal measure, $m\angle BDC = m\angle BCD$ and $m\angle ADC = m\angle ACD$.



First, we take up the case that D lies outside $\triangle ABC$; that is, D lies on the other side of $\overleftrightarrow{BC}$ from A.

Exercise 5.6: Finish this case of the proof, first by showing that $m\angle ADC < m\angle BDC$ and $m\angle BCD < m\angle ACD$. Then use the isosceles triangles to arrive at the contradiction that $m\angle ADC < m\angle ADC$.

We now consider the case where D lies inside $\triangle ABC$. Let E be a point on the line $\overleftrightarrow{BC}$ so that C is between B and E to some point E. Observe that $m\angle BCD + m\angle DCA + m\angle ACE = \pi$, from which it follows that $m\angle BCD + m\angle DCA < \pi$. Next, extend the segment $\overline{BD}$ past D to some point F. Also extend the segment $\overline{AD}$ past the point D to some point G, and extend the segment $\overline{CD}$ past the point D to some point H.



Exercise 5.7: Finish this case of the proof by explaining why $\pi < m\angle BDC + m\angle CDA$ and $m\angle BCD + m\angle DCA < \pi$, and then show that this leads to the contradiction $\pi < \pi$.

□

5.7. Congruence via AAS.

Theorem 5.4 (AAS). *Suppose we are given triangles ABC and $A'B'C'$, where $m\angle A = m\angle A'$, $m\angle B = m\angle B'$, and $|BC| = |B'C'|$. Then $\triangle ABC \cong \triangle A'B'C'$.*

This theorem can be proved by methods similar to those used in the proofs above. We will skip this for now, however, and will instead give a much simpler proof later, using a celebrated result about the sum of the angles of any triangle.

This concludes our generalities concerning congruences of triangles. We have now seen four basic congruence results: ASA, SAS, SSS and AAS. We also have seen that the other two possibilities, SSA and AAA, are simply not valid. It follows that, for example, if we are given the lengths of all three sides of a triangle, then the measures of all three angles are determined. However, we do not as yet have any means of computing the measures of these angles in terms of the lengths of the sides.

5.8. Median, altitude, and bisector in an isosceles triangle.

Definition 5.2. Two lines intersecting at a point A are perpendicular or orthogonal if each of the four angles at A has measure $\pi/2$. These angles are called right angles.

It is standard mathematical practice to use the words perpendicular and orthogonal to mean precisely the same thing. Anyone who tries to draw a distinction between them is joking!

In any triangle $\triangle ABC$, there are three special lines passing through the arbitrary vertex we have chosen to call A, namely:

- the altitude from A is perpendicular to $\overleftrightarrow{BC}$;
- the median from A bisects $\overline{BC}$, in the sense that it crosses $\overleftrightarrow{BC}$ at the midpoint D of $\overline{BC}$, which we constructed in Exercise 3.14; and
- the angle bisector bisects $\angle A$, in the sense that if E is the point where the angle bisector meets BC, then $m\angle BAE = m\angle EAC$.

Exercise 5.8: For any triangle $\triangle ABC$, show there exists a unique median thorough A and a unique angle bisector through A.

Later we will show the altitude from A actually exists, and is unique. Note that this isn't completely trivial!

For most triangles, the three lines through a given vertex we've just defined are all different. For an isosceles triangle, however, they all actually coincide:

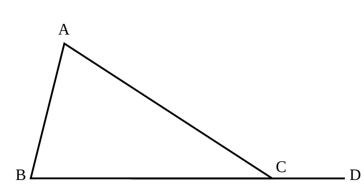
Theorem 5.5. *If B is the apex of the isosceles triangle ABC, and BM is the median, then BM is also the altitude, and is also the angle bisector, from B.*

Proof. Consider triangles $\triangle ABM$ and $\triangle CBM$. Then $|AB| = |CB|$ (by definition of isosceles triangle), $|AM| = |CM|$ (by definition of midpoint), and $m\angle MAB = m\angle MCB$ (by Theorem 5.2). Thus, by the SAS Axiom, $\triangle ABM \cong \triangle CBM$. Therefore, $m\angle ABM = m\angle CBM$, so BM is the angle bisector.

Also, $m\angle AMB = m\angle CMB$. On the other hand, by Protractor Axiom, $m\angle AMB + m\angle CMB = m\angle AMC = \pi$. Thus, $m\angle AMB = m\angle CMB = \pi/2$. □

5.9. Inequalities for general triangles.

Theorem 5.6 (Exterior angle inequality). *Consider the triangle $\triangle ABC$. Let D be some point on the ray $\overrightarrow{BC}$, where C lies between B and D. Then*

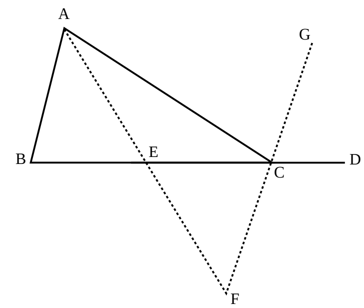


(1) $m\angle ACD > m\angle B$.
(2) $m\angle ACD > m\angle A$.

We will later prove a much stronger result, namely, that $m\angle ACD = m\angle A + m\angle B$. However, to get this stronger statement we will need to also invoke the Parallel Axiom, whereas the result we are about to prove remains true even in "hyperbolic geometry," where all of our axioms *except* the Parallel Axiom hold.

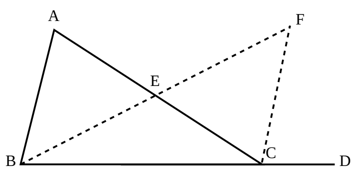
Notice that the following proof depends only on direct use of the SAS Axiom, together with easy consequences of the Incidence, Ruler and Protractor Axioms. This will be an point important point when we finish the proof of Theorem 4.3 in Exercise 6.1.

Proof. We first prove part (1).



Choose E to be the midpoint of the segment $\overline{BC}$, and extend $\overline{AE}$ beyond E to F, so that $|AE| = |EF|$. Now extend $\overline{FC}$ beyond C to some point G.

Exercise 5.9: Finish the proof of part (1) by showing that $m\angle B = m\angle BCF = m\angle DCG < m\angle DCA$. (Hint: use Exercise 5.2.)



Exercise 5.10: Give a proof of part (2) using the figure at left (E is the midpoint of $\overline{AC}$, and $|EF| = |BE|$.)

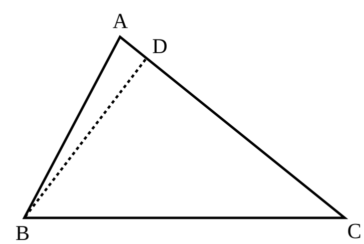
□

We already know that if two sides of a triangle are equal, then the angles opposite to these sides are also equal (Theorem 5.2). The next theorem extends this result: in a triangle, if one angle is bigger than another, the side opposite the bigger angle must be longer than the one opposite the smaller angle.

Theorem 5.7. *In $\triangle ABC$, if $m\angle A > m\angle B$, then we must have $|BC| > |AC|$.*

Proof. Assume not. Then either $|BC| = |AC|$ or $|BC| < |AC|$.

Exercise 5.11: Show that if $|BC| = |AC|$, the assumption $m\angle A > m\angle B$ is contradicted.



Now assume $|BC| < |AC|$, find the point D on $\overline{AC}$ so that $|BC| = |CD|$, and draw the line $\overleftrightarrow{BD}$. Then $\triangle BCD$ is isosceles, with apex at C. Hence $m\angle CBD = m\angle CDB$. Since $\angle CDB$ is an exterior angle for $\triangle ABD$, by Theorem 5.6, $m\angle CDB > m\angle A$. Also, since D lies between A and C, $m\angle DBC < m\angle ABC$. We now have that $m\angle CBD < m\angle CBA < m\angle A < m\angle CDB = m\angle CBD$; so we have reached a contradiction.

□

The converse of the previous theorem is also true: opposite a long side, there must be a big angle.

Theorem 5.8. *In $\triangle ABC$, if $|BC| > |AC|$, then $m\angle A > m\angle B$.*

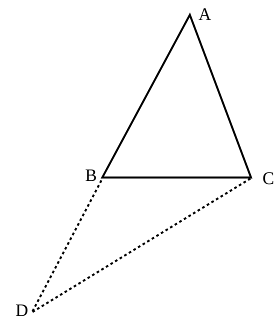
Proof. Assume not. If $m\angle A = m\angle B$, then $\triangle ABC$ is isosceles, with apex at C, so $|BC| = |AC|$, which contradicts our assumption.

If $m\angle A < m\angle B$, then, by the previous theorem, $|BC| < |AC|$, which again contradicts our assumption. □

The following theorem doesn't *quite* say that a straight line provides the shortest route between two points, but what it *does* say is certainly closely related. This result is constantly used throughout much of mathematics, and is known as "the triangle inequality".

Theorem 5.9 (The Triangle Inequality)**.** *In any triangle* $\triangle ABC$*,*

$$|AB| + |BC| > |AC|.$$



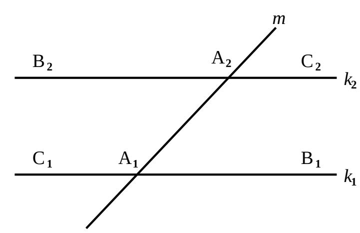
Proof. Extend the segment $\overline{AB}$ past B to the point D so that $|BD| = |BC|$, and join the points C and D with a line to form $\triangle ADC$. Observe that $\triangle BCD$ is isosceles, with apex at B; hence $m\angle BDC = m\angle BCD$. It is immediate that $m\angle DCB < m\angle DCA$. Looking at $\triangle ADC$, it follows that $m\angle D < m\angle C$; by Theorem 5.7, this implies $|AD| > |AC|$. Our result now follows, since $|AD| = |AB| + |BD|$ by Theorem 3.6. $\square$

6. Parallel Lines Revisited

Looking over the proofs in the previous sections, we see that we haven't used the Parallel Axiom since Section 2. For example, our congruence rules for triangles were proved without using this axiom. In this section, we will see what new results can be obtained from the Parallel Axiom.

6.1. Alternate interior angles. We will meet the following situation some number of times. We are given two lines k_1 and k_2, and a third line m, where m crosses k_1 at A_1 and m crosses k_2 at A_2. Choose a point $B_1 \neq A_1$ on k_1, and choose a point $B_2 \neq A_2$ on k_2, where B_1 and B_2 lie on opposite sides of the line m. Then $\angle B_1A_1A_2$ and $\angle B_2A_2A_1$ are referred to as alternate interior angles.

In any given situation, there are two distinct pairs of alternate interior angles. That is, let C_1 be some point on k_1, where B_1 and C_1 lie on opposite sides of m, and let C_2 be some point on k_2, where C_2 and B_2 lie on opposite sides of m. Then one could also regard $\angle C_1A_1A_2$ and $\angle C_2A_2A_1$ as being alternate interior angles. However, observe that $m\angle B_1A_1A_2 + m\angle C_1A_1A_2 = \pi$ and $m\angle B_2A_2A_1 + m\angle C_2A_2A_1 = \pi$. It follows that one pair of alternate interior angles are equal if and only if the other pair of alternate interior angles are equal.



Theorem 6.1. *If the alternate interior angles are equal, then the lines k_1 and k_2 are parallel.*

Proof. Suppose not. Then the lines k_1 and k_2 meet at some point D. If necessary, we interchange the roles of the B_i and the C_i so that $\angle B_1A_1A_2$ is an exterior angle of $\triangle A_1A_2D$. Then D and B_2 lie on the same side of m, so $\angle DA_2A_1 = \angle B_2A_2A_1$. By the exterior angle inequality,

$$m\angle B_1A_1A_2 > m\angle A_1A_2D = m\angle B_2A_2A_1 = m\angle B_1A_1A_2,$$

so we have reached a contradiction. □

6.2. Characterization of parallel lines. Let k_1 be a line, and let A_2 be a point not on k_1. Pick some point A_1 on k_1 and draw the line m through A_1 and A_2. By the Protractor Axiom, we can find a line k_2 through A_2 so that the alternate interior angles are equal. Hence we can find a line through A_2 parallel to k_1.

Theorem 6.2 (Alternate Interior Angles Equal)**.** *Two lines k_1 and k_2 are parallel if and only if the alternate interior angles are equal.*

Proof. To prove the forward direction, construct the line k_3 through A_2, where there is a point B_3 on k_3, with B_3 and B_2 on the same side of m, so that $m\angle B_3A_2A_1 = m\angle B_1A_1A_2$. Then, by Theorem 6.1, k_3 is a line through A_2 parallel to k_1. The Parallel Axiom implies $k_3 = k_1$. Hence $m\angle B_3A_2A_1 = m\angle B_2A_2A_1$, and the desired conclusion follows.

The other direction is just Theorem 6.1, restated as part of this theorem for convenience. □

Exercise 6.1: Let $\angle BAC$ be a non-straight angle, and choose D so that $\overleftrightarrow{AD} \| \overleftrightarrow{BC}$. Use Theorem 6.2 to show that either D and B are on opposite sides of $\overleftrightarrow{AC}$, or else that D and C are on opposite sides of $\overleftrightarrow{AB}$. Conclude that D cannot be in the interior of $\angle BAC$.

Notice that the proof of Theorem 5.6 only depends on Theorem 6.2, along with the Parallel and SAS axioms; most importantly, it does not logically depend on the Crossbar Theorem in any way. For this reason, Exercise 6.1, together with Exercise 4.7 and Exercise 4.8, provides a complete proof of Theorem 4.3.

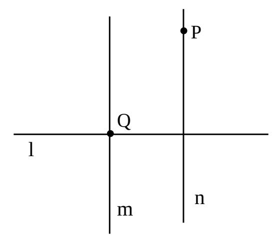
6.3. Perpendicular lines. Recall that a right angle is an angle of measure $\pi/2$, and that two intersecting lines are called perpendicular, or orthogonal, if all four angles formed by these lines are right angles (notation: $l \perp m$). Using Theorem 4.4 (about vertical and complementary angles), it is easy to see that if one of the four angles is a right angle, then so are all of them.

Proposition 6.3. *Let $m \parallel n, l \perp m$. Then $l \perp n$.*

Theorem 6.4. *For any line l and a point P, there exists a unique line n such that $P \in n, n \perp l$. This line is called the perpendicular from P to l.*

Proof. **Existence:** Let Q be an arbitrary point on l. By the Protractor Axiom, there exists a line m going through Q such that $m \perp l$. Now let n be the line going through P and parallel to m (exists by the Parallel Axiom). By Proposition 6.3, $n \perp l$.

Uniqueness: Assume n_1, n_2 are two lines, both containing P and perpendicular to l. Then, by Theorem 6.2, these two lines are parallel: $n_1 \parallel n_2$. But by definition, if two parallel lines have a common point, they must coincide, i.e. $n_1 = n_2$. □



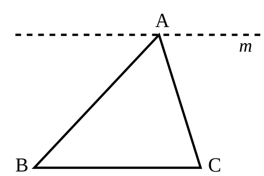
Exercise 6.2: Let A, B be distinct points and let M_1, M_2 be points on different sides of the line $\overleftrightarrow{AB}$ such that $|AM_1| = |AM_2|, |BM_1| = |BM_2|$. Show that $\overleftrightarrow{M_1M_2} \perp \overleftrightarrow{AB}$.

6.4. The sum of the angles of a triangle.

Theorem 6.5. *The sum of the measures of the angles of a triangle is equal to π.*

Proof. Consider $\triangle ABC$, and let m be the line passing through A and parallel to BC.

Exercise 6.3: Use alternate interior angles to complete the proof of this theorem. □



Exercise 6.4: Prove that the external angle of a triangle is equal to the sum of two other angles, i.e., $m\angle ACD = m\angle A + m\angle B$ (notation as in Theorem 5.6).

Exercise 6.5: Prove Theorem 5.4 (congruence via AAS).

6.5. Parallelograms and rectangles. A quadrilateral is a figure consisting of four points A, B, C, D (vertices) and segments AB, BC, CD, DA (sides), such that all points are distinct, no three points lie on the same line, and no two sides intersect (except at vertices). We will denote the resulting figure by $\Diamond ABCD$.

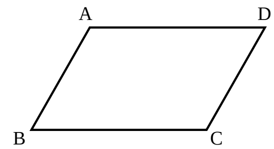
A quadrilateral $\Diamond ABCD$ is said to be convex if A and C are on opposite sides of $\overleftrightarrow{BD}$, and if B and D are on opposite sides of $\overleftrightarrow{AC}$.

Exercise 6.6: Show that the quadrilateral $\Diamond ABCD$ is convex iff its "diagonal" line segments $\overline{AC}$ and $\overline{BD}$ meet in a point.

Exercise 6.7: If $\Diamond ABCD$ is a convex quadrilateral, use the Crossbar Theorem to show that C is in the interior of $\angle BAD$.

Exercise 6.8: Show that the sum of the measures of the angles in a convex quadrilateral is equal to 2π. (Hint: cut the quadrilateral into two triangles.)

Exercise 6.9: In the previous exercise, what goes wrong if $\Diamond ABCD$ is not convex? (Hint: by our conventions, the measure of an angle can never exceed π.)



Definition 6.1. A parallelogram is a quadrilateral $\Diamond ABCD$ in which opposite sides are parallel; that is, $\overleftrightarrow{AB}$ is parallel to $\overleftrightarrow{CD}$, and $\overleftrightarrow{AD}$ is parallel to $\overleftrightarrow{BC}$.

Lemma 6.6. *Any parallelogram is a convex quadrilateral.*

Proof. Since $\overline{CD}$ does not meet $\overleftrightarrow{AB}$ and $\overline{BD}$ does not meet $\overleftrightarrow{AC}$, C is in the interior of $\angle BAD$ by Exercise 4.2. Thus $\overrightarrow{AC}$ meets $\overline{BD}$ by the Crossbar Theorem. Similarly, $\overrightarrow{CA}$ meets $\overline{BD}$. Since $\overleftrightarrow{AC}$ meets $\overleftrightarrow{BD}$ in only one point, and since $\overrightarrow{AC} \cap \overrightarrow{CA} = \overline{AC}$, it follows that $\overline{AC}$ meets $\overline{BD}$. Hence $\Diamond ABCD$ is convex by Exercise 6.6. $\square$

Theorem 6.7. *Let $\Diamond ABCD$ be a parallelogram. Then $m\angle A = m\angle C$; $m\angle B = m\angle D$; $|AB| = |CD|$; and $|BC| = |AD|$.*

Exercise 6.10: Prove this theorem. (Hint: Draw a diagonal.)

Theorem 6.8. *If $\Diamond ABCD$ is a quadrilateral in which $|AB| = |CD|$ and $|AD| = |BC|$, then $\Diamond ABCD$ is a parallelogram.*

Exercise 6.11: Prove this theorem.

Definition 6.2. A rectangle is a quadrilateral in which all four angles are right angles. A rectangle with all four sides of equal length is called a square.

Theorem 6.9. *Any rectangle is a parallelogram.*

Exercise 6.12: Prove this theorem.

Exercise 6.13: Let $\Diamond ABCD$ be a parallelogram with diagonals of equal length (that is, $|AC| = |BD|$). Then $\Diamond ABCD$ is a rectangle.

7. Similarity, and the Pythagorean Theorem

7.1. Similar triangles. We say that triangles $\triangle ABC$ and $\triangle A'B'C'$ are similar, with constant of proportionality k, if $\angle A = \angle A', \angle B = \angle B', \angle C = \angle C'$ and

$$\frac{|A'B'|}{|AB|} = \frac{|B'C'|}{|BC|} = \frac{|A'C'|}{|AC|} = k.$$

If this holds for some positive real number k, we write $\triangle ABC \sim \triangle A'B'C'$.

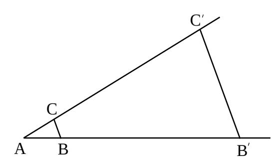
From this definition, it is clear that $\triangle ABC \cong \triangle A'B'C'$ iff they are similar with constant of proportionality $k = 1$.

Exercise 7.1: Show that if $\triangle ABC \sim \triangle A'B'C'$ with constant k_1 and $\triangle A'B'C' \sim \triangle A''B''C''$ with constant k_2, then $\triangle ABC \sim \triangle A''B''C''$ with constant k_1k_2.

7.2. Key theorem. The key tool in the study of similar triangles is the following theorem.

Theorem 7.1. *Consider a triangle $\triangle ABC$ and let $B' \in \overrightarrow{AB}$, $C' \in \overrightarrow{AC}$ be such that lines $\overleftrightarrow{BC}$ and $\overleftrightarrow{B'C'}$ are parallel. Then*

$$\frac{|AB'|}{|AB|} = \frac{|AC'|}{|AC|}$$



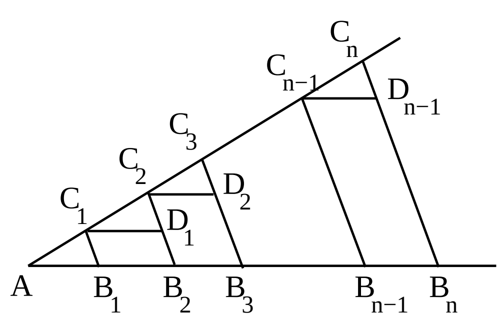
Exercise 7.2: Assuming Theorem 7.1, use the Parallel Axiom to show, conversely, that if $B' \in \overrightarrow{AB}, C' \in \overrightarrow{AC}$ are such that $\frac{|AC'|}{|AC|} = \frac{|AB'|}{|AB|}$, then $\overleftrightarrow{B'C'} \| \overleftrightarrow{BC}$.

The proof of Theorem 7.1 is surprisingly difficult, and will be completed in stages. We begin by proving the following important special case:

Lemma 7.2. *Theorem* 7.1 *is true in the special case in which $\frac{|AB'|}{|AB|} = n$ is a positive integer.*

Proof. Divide the segment AB' into n equal length pieces, i.e. find on it points $B_1 = B, B_2, \ldots, B_n = B'$ such that $|AB_1| = |B_1B_2| = \cdots = |B_{n-1}B_n|$. Through each point B_i, draw a line l_i which is parallel to $\overleftrightarrow{BC}$. Let C_i be the intersection point of l_i with $\overrightarrow{AC}$.

Next, for each C_i, draw a line parallel to $\overleftrightarrow{AB}$ and let D_i be the intersection point of this line with line $B_{i+1}C_{i+1}$.



Exercise 7.3: Show that each of triangles $C_iD_iC_{i+1}$ is congruent to the triangle ABC. (Hint: $\lozenge B_iC_iD_iB_{i+1}$ is a parallelogram.)

Thus, $|C_iC_{i+1}| = |AC|$, so $|AC'| = n|AC|$, and

$$\frac{|AC'|}{|AC|} = n = \frac{|AB'|}{|AB|}$$

□

Exercise 7.4: Use Lemma 7.2 to prove Theorem 7.1 in the case when $\frac{|AB'|}{|AB|} = \frac{1}{m}$ for some positive integer m.

Exercise 7.5: Now combine Lemma 7.2 and Exercise 7.4 to prove Theorem 7.1 in the case when $\frac{|AB'|}{|AB|} = \frac{n}{m}$ is any positive rational number.

Now, one of the fundamental properties of the real numbers $\mathbb{R}$ is that *one can find rational numbers between any two distinct real numbers*:

$$\forall x, y \in \mathbb{R}\ [x < y \Longrightarrow \exists q \in \mathbb{Q}\ (x < q < y)]$$

Using this fact about $\mathbb{R}$, we can now complete the proof of our key theorem.

Proof of Theorem 7.1. Set

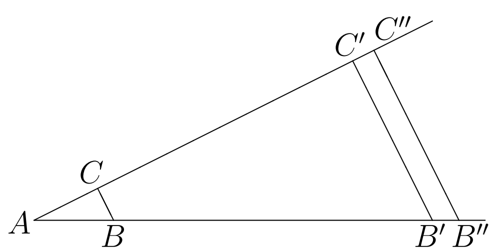
$$k_1 = \frac{|AB'|}{|AB|} \qquad \text{and} \qquad k_2 = \frac{|AC'|}{|AC|}\ .$$

We will show by contradiction that $k_1 = k_2$. Indeed, suppose not. Then the trichotomy axiom for $\mathbb{R}$ tells us that either $k_1 < k_2$, or else $k_2 < k_1$. We will show that either of these possibilities leads to a contradiction.

If $k_1 < k_2$, we can choose a rational number $q = \frac{n}{m}$ such that $k_1 < q < k_2$. Let B'' be the unique point of $\overrightarrow{AB}$ such that

$$\frac{|AB''|}{|AB|} = q$$

and let C'' be the point of $\overrightarrow{AC}$ such that $\overleftrightarrow{B''C''} \parallel \overleftrightarrow{BC}$:



Now $|AB'| < |AB''|$, since $k_1 < q$. Hence $A - B' - B''$, and A is therefore on the opposite side of $\overleftrightarrow{B'C'}$ from B''. But B'' and C'' are on the same side of $\overleftrightarrow{B'C'}$, since $\overline{B''C''}$ is parallel to $\overleftrightarrow{B'C'}$, and so does not meet it. The Plane Separation Axiom therefore tells us that A and C'' are on opposite sides of $\overleftrightarrow{B'C'}$. Hence $A - C' - C''$, so $|AC'| < |AC''|$, and therefore

$$k_2 = \frac{|AC'|}{|AC|} < \frac{|AC''|}{|AC|}\ .$$

But

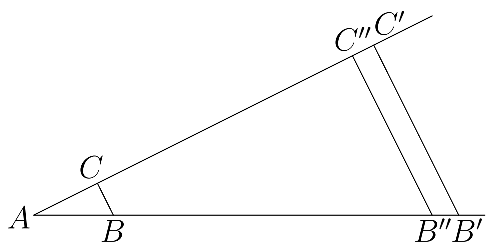
$$\frac{|AC''|}{|AC|} = \frac{|AB''|}{|AB|} = q$$

by Exercise 7.5, so it follows that $k_2 < q$. But since q was chosen at the outset to satisfy $q < k_2$, this is a contradiction. Thus $k_1 < k_2$ is impossible.

In much the same way, we also obtain a contradiction if $k_2 < k_1$. Indeed, if $k_2 < k_1$, we can instead choose a rational number q such that $k_2 < q < k_1$, and once again choose B'' on $\overrightarrow{AB}$ so that

$$\frac{|AB''|}{|AB|} = q$$

and C'' on $\overrightarrow{AC}$ so that $\overleftrightarrow{B''C''} \parallel \overleftrightarrow{BC}$:



This time, $|AB'| > |AB''|$, since $k_1 > q$. Hence $A - B'' - B'$, and A is therefore on the same side of $\overleftrightarrow{B'C'}$ as B''. But C'' is on the same side of $\overleftrightarrow{B'C'}$ as B'', and hence on the same side as A, by the Plane Separation Axiom. Hence $A - C'' - C'$. Thus $|AC'| > |AC''|$, and

$$k_2 = \frac{|AC'|}{|AC|} > \frac{|AC''|}{|AC|}\ .$$

But

$$\frac{|AC''|}{|AC|} = \frac{|AB''|}{|AB|} = q$$

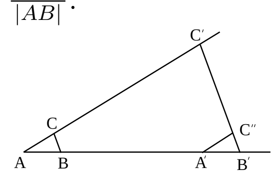
by Exercise 7.5, so we conclude that $k_2 > q$. But since q was chosen to satisfy $q > k_2$, this is another a contradiction, and our proof is therefore complete. □

7.3. Existence of similar triangles.

Theorem 7.3. *In the situation described by Theorem* 7.1, $\triangle ABC \sim \triangle AB'C'$.

Proof. By Theorem 6.2 (alternate interior angles equal), $\angle B = \angle B'$ and $\angle C = \angle C'$. By Theorem 7.1, $\frac{|AC'|}{|AC|} = \frac{|AB'|}{|AB|}$. Thus, it remains to show that $\frac{|BC'|}{|BC|} = \frac{|AB'|}{|AB|}$.

Let A' be a point on $\overrightarrow{BA}$ such that $|A'B'| = |AB|$, and let $C'' \in \overrightarrow{BC}$ be such that $\overleftrightarrow{A'C''} \| \overleftrightarrow{AC'}$.



Exercise 7.6: Show that $\triangle A'B'C'' \cong \triangle ABC$.

Using Theorem 7.1, one easily sees that $\frac{|B'C'|}{|B'C''|} = \frac{|AB'|}{|A'B'|}$. Since $|A'B'| = |AB|$, and $|B'C''| = |BC|$, we get $\frac{|B'C'|}{|BC|} = \frac{|AB'|}{|AB|}$. □

Corollary 7.4. *For any triangle* $\triangle ABC$ *and a real number* $k > 0$, *there exists a triangle* $\triangle A'B'C'$ *similar to* $\triangle ABC$ *with constant* k.

Exercise 7.7: For a triangle $\triangle ABC$, let D be the midpoint of AB and F be the midpoint of AC. Show that

(1) $\overleftrightarrow{DF} \| \overleftrightarrow{BC}$
(2) $|DF| = \frac{1}{2}|BC|$

7.4. Similarity via AAA.

Theorem 7.5 (Similarity via AAA). *Let* $\triangle ABC$, $\triangle A'B'C'$ *be such that* $\angle A = \angle A', \angle B = \angle B', \angle C = \angle C'$. *Then these triangles are similar.*

Proof. Let $k = \frac{|A'B'|}{|AB|}$. Construct a triangle $\triangle A''B''C''$ which is similar to $\triangle ABC$ with constant of proportionality k. Then $|A'B'| = |A''B''|$, and $\angle A = \angle A' = \angle A''$, $\angle B = \angle B' = \angle B''$, $\angle C = \angle C' = \angle C''$. Thus, by ASA, $\triangle A'B'C' \cong \triangle A''B''C''$. □

Theorem 7.6 (Similarity via SAS)**.** *Let $\triangle ABC$, $\triangle A'B'C'$ be such that $\angle A = \angle A'$, $\frac{|A'B'|}{|AB|} = \frac{|A'C'|}{|AC|}$. Then these triangles are similar.*

Exercise 7.8: Prove this theorem.

7.5. Pythagoras' Theorem. A right triangle is a triangle in which one of the angles is a right angle. The hypotenuse of a right triangle is the side opposing the right angle.

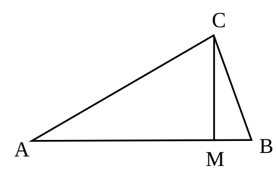
The following theorem, often attributed to Pythagoras, and so called the Pythagorean Theorem, seems to have been known "experimentally" to the Babylonians and Egyptians as early four thousand years ago, and there is considerable historical evidence that this knowledge had spread to India and China by the time of Pythagoras' time, some 2500 years ago. It is quite plausible, however, that the first actual *proof* of the theorem may have been found by Pythagoras' school, and in any case, the earliest general proof to have come down to us is the one in Euclid's *Elements*. The proof given below is not as geometrically intuitive as the one presumably discovered by Pythagoras — but it is far easier to derive from our axioms!

Theorem 7.7 (Pythagorean Theorem)**.** *Let $\triangle ABC$ be a right triangle, with $\angle C$ being the right angle. Then*

$$|AB|^2 = |AC|^2 + |BC|^2.$$

Proof. For brevity, set $a = |BC|$, $b = |AC|$, and $c = |AB|$. Drop a perpendicular from C to AB; let M be the point where this perpendicular intersects $\overleftrightarrow{AB}$.

Exercise 7.9: Show that $\triangle ACM \sim \triangle ABC$, and deduce from this that $|AM| = b^2/c$.



Exercise 7.10: Show that $\triangle CBM \sim \triangle ABC$, and deduce from this that $|BM| = a^2/c$.

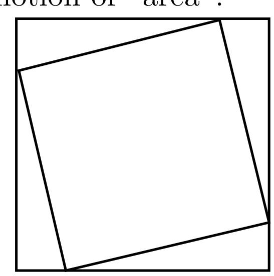
Combining these two exercises, we get

$$c = |AM| + |MB| = \frac{a^2}{c} + \frac{b^2}{c}.$$

Multiplying both sides by c, we obtain the Pythagorean theorem $a^2 + b^2 = c^2$. □

Exercise 7.11: The figure to the right can be used to give a more "geometrically obvious" proof of Pythagoras' theorem — if we allow ourselves to use the notion of "area".

(1) By computing the area of the large square in two ways, prove the Pythagorean theorem.
(2) Carefully analyze the proof of part (1) and list all the properties of area you are using. Can you prove any of them? (This, of course, depends on how one defines area.)



Exercise 7.12: Let $\triangle ABC$ and $\triangle A'B'C'$ be such that $|AB| = |A'B'|$, $|BC| = |B'C'|$, and $m\angle C = m\angle C' = \pi/2$. Prove that $\triangle ABC \cong \triangle A'B'C'$.

8. Circles and lines

8.1. Circles. A circle Σ is the set of points at fixed distance $r > 0$ from a given point, its center. The distance r is called the radius of the circle Σ.

The circle Σ divides the plane into two regions: the inside, which is the set of points at distance less than r from the center O, and the outside, which consists of all points having distance from O greater than r. Note that every line segment from O to a point on Σ has the same length r.

A line segment from O to a point on Σ is also called a radius; this should cause no confusion.

A line segment connecting two points of Σ is called a chord, if the chord passes through the center, then it is called a diameter.

As above, we also use the word diameter to denote the length of a diameter of Σ, that is, the number that is twice the radius.

8.2. Perpendicular bisector. Let A, B be distinct points. The perpendicular bisector of segment AB is the line l which contains midpoint of AB and is perpendicular to $\overleftrightarrow{AB}$.

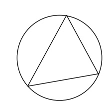
Theorem 8.1. *Let A, B be distinct points. Then $|OA| = |OB|$ iff O lies on the perpendicular bisector of AB.*

Corollary 8.2. *If A, B are two distinct points on a circle Σ, then the center of Σ lies on perpendicular bisector of AB.*

Proposition 8.3. *A line k intersects a circle Σ in at most two points.*

Exercise 8.1: Prove this proposition, using proof by contradiction.

8.3. Circumscribed circles. The circle Σ is circumscribed about $\triangle ABC$ if all three vertices of the triangle lie on the circle. In this case, we also say that the triangle is inscribed in the circle.



Note that another way to describe a circle circumscribed about a triangle is to say that it is the smallest circle for which every point inside the triangle is also inside the circle. In this view, the problem of circumscribing a circle becomes a minimization problem. A given triangle lies inside many circles, but the circumscribed circle is, in some sense, the smallest circle which lies outside the given triangle.

It is not immediately obvious that one can always solve this minimization problem, nor that the solution is unique.

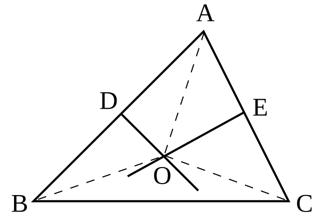
Proposition 8.4 (Uniqueness of Circumscribed Circles)**.** *There is at most one circle circumscribed about any triangle.*

Proof. Suppose there are two circles Σ and Σ' which are circumscribed about $\triangle ABC$. Since points A, B, and C lie on both circles, AB and BC are chords. By Corollary 8.2, the perpendicular bisectors of AB and BC both pass through the centers of Σ and Σ'. Since these two distinct lines can intersect in at most one point, Σ and Σ' share the same center O. Since AO is a radius for both circles, they have the same center and radius, and hence are the same circle. □

Theorem 8.5 (Existence of Circumscribed Circles)**.** *Given $\triangle ABC$, there is always exactly one circle Σ circumscribed about it.*

Proof. We need to show existence of a circumscribed circle; uniqueness was shown in Proposition 8.4.

Let D and E be the midpoints of sides AB and BC respectively. Draw the perpendicular bisectors of AB and BC, and let O be the point where these two lines intersect (note that O need not be inside the triangle). Draw the lines AO, BO and CO. By Theorem 8.1, $|AO| = |BO|$ (since O lies on the perpendicular bisector of AB); similarly, $|BO| = |CO|$. Thus, if we denote $r = |AO| = |BO| = |CO|$, and let Σ be the circle with center at O and radius r, then points A, B, C are on Σ.



□

Corollary 8.6. *In any triangle, the three perpendicular bisectors of the sides meet at a point.*

Exercise 8.2: Explain why Theorem 8.5 implies this corollary.

8.4. Altitudes meet at a point.

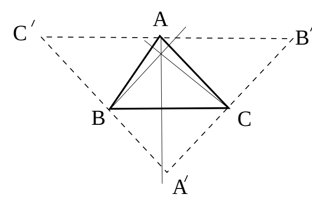
Theorem 8.7. *In any triangle $\triangle ABC$, the three altitudes meet at a point.*

Proof. Draw line l through vertex A, such that $l \parallel \overleftrightarrow{BC}$; similarly, draw lines through vertices B and C parallel to opposite sides of $\triangle ABC$. Let A', B', C' be the intersection points of these lines, as shown in the figure.

Exercise 8.3: (1) Prove that each of triangles $\triangle A'BC, \triangle ABC', \triangle AB'C$ is congruent to $\triangle ABC$.

(2) Prove that A is the midpoint of $B'C'$, B is the midpoint of $A'C'$, and C is the midpoint of $A'B'$.

(3) Prove that altitudes of $\triangle ABC$ are the same as perpendicular bisectors of sides of $\triangle A'B'C'$.



Since, by Corollary 8.6, perpendicular bisectors of $\triangle A'B'C'$ meet at a point, we see that altitudes of $\triangle ABC$ meet at a point. □

8.5. Tangent lines. A line that meets a circle in exactly one point is a tangent line to the circle at the point of intersection. Our first problem is to show that there is one and only one tangent line at each point of a circle.

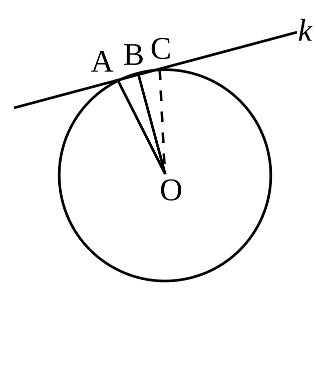
Proposition 8.8. *Let A be a point on the circle Σ, and let k be the line through A perpendicular to the radius at A. Then k is tangent to Σ.*

Proof. There are only three possibilities for k: it either is disjoint from Σ, which cannot be, as A is a common point; or it is tangent to Σ at A; or it meets Σ at another point B. If k meets Σ at B then OAB is a triangle, where $\angle A$ is a right angle. Since OA and OB are both radii, $|OA| = |OB|$. Hence $\triangle OAB$ is isosceles. Hence $m\angle A = m\angle B$. We have constructed a triangle with two right angles, which cannot be; i.e., we have reached a contradiction. □

Proposition 8.9. *If k is a line tangent to the circle Σ at the point A, then k is perpendicular to the radius ending at A.*

Proof. We will prove the contrapositive: if k is a line passing through A, where k is not perpendicular to the radius, then k is not tangent to Σ.

Draw the line segment m from O to k, where m is perpendicular to k. Let B be the point of intersection of k and m. On k, mark off the distance $|AB|$ from B to some point C, on the other side of B from A. Since OB is perpendicular to k, $m\angle OBA = m\angle OBC$. By SAS, $\triangle OBA \cong \triangle OBC$, and so $|OC| = |OA|$. Thus both A and C lie on Σ, and k intersects Σ in two points. Thus, k is not tangent to Σ.



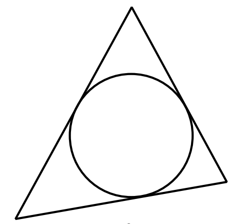
□

Corollary 8.10. *Let A be a point on the circle Σ. Then there is exactly one line through A tangent to Σ.*

Exercise 8.4: Prove this Corollary.

8.6. Inscribed circles.

A circle Σ is inscribed in $\triangle ABC$ if all three sides of the triangle are tangent to Σ. One can view the inscribed circle as being the largest circle whose interior lies entirely inside the triangle. (Note that it is not quite correct to say that the circle lies entirely inside the triangle, because the triangle and the circle share three points.)



We start the search for the inscribed circle with the question of what it means for the circle to have two tangents which are not parallel.

Proposition 8.11. *Let A be a point outside the circle Σ, and let k_1 and k_2 be tangents to Σ passing through A. Then the line segment OA bisects the angle between k_1 and k_2.*

Proof. Let B_i be the point where k_i is tangent to Σ, for $i = 1, 2$. Draw the lines OB_1 and OB_2. Observe that $|OB_1| = |OB_2| = r$, and that, since radii are perpendicular to tangents, $\angle OB_1A = \angle OB_2A = \pi/2$. By Pythagoras theorem, $|AB_1| = \sqrt{|AB_1|^2 + r^2} = |AB_2$.

By SSS, $\triangle OB_1A \cong \triangle OB_2A$. Hence $m\angle OAB_1 = m\angle OAB_2$. □

From the above, we see that if there is an inscribed circle for $\triangle ABC$, then its center lies at the point of intersection of the three angle bisectors, and its radius is the distance from this point to the three sides. Hence we have proven the following.

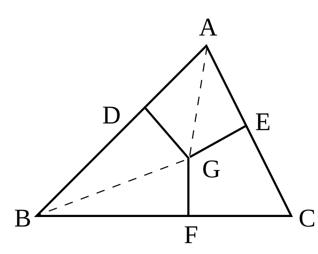
Corollary 8.12 (Inscribed circles are unique)**.** *Every triangle has at most one inscribed circle.*

Theorem 8.13. *Every triangle has an inscribed circle.*

Proof.

Let G be the point of intersection of the angle bisectors from A and B in $\triangle ABC$. Let D be the point where the perpendicular from G meets AB; let E be the point where the perpendicular from G meets BC; and let F be the point where the perpendicular from G meets AC.

Observe that, by AAS, $\triangle ADG \cong \triangle AFG$. Similarly, $\triangle BDG \cong \triangle BEG$ and $\triangle CEG \cong \triangle CFG$.



We have shown that the perpendiculars from G to the three sides all have equal length; call this length r. Then, by Proposition 8.8, the circle centered at G of radius r is tangent to the three sides of $\triangle ABC$ exactly at the points D, E and F. □

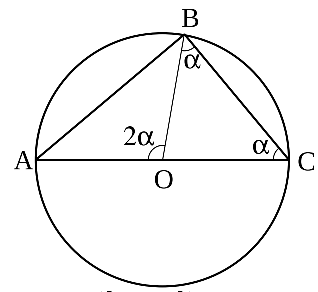
Corollary 8.14. *The three angle bisectors of a triangle meet at a point; this point is the center of the inscribed circle.*

Exercise 8.5: Give a proof of this corollary using the above theorem.

Exercise 8.6: Let A and B be points on the circle Σ. Let k be the line tangent to Σ at A and let m be the line tangent to Σ at B. Prove that if k and m are parallel, then the line segment AB is a diameter of Σ.

8.7. Central angles. Let Σ be a circle with center O, and let A, B be points on Σ. Then the angle $\angle AOB$ is called **central angle**. It turns out that the angles in a triangel ABC inscribed in Σ are closely related with the corresponding central angles.

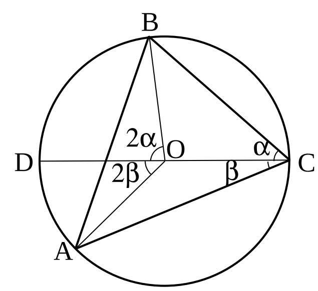
Proposition 8.15. *Let Σ be a circle with center O, and let A, B, C be distinct points on Σ such that AC is a diameter of Σ. Then $m\angle ACB = \frac{1}{2} m\angle AOB$*



Proof. Consider the triangle BOC. Since $|BO| = |OC|$, this triangle is isosceles. Thus, by Theorem 5.2(base angles are equal), $\angle OBC = \angle OCB$. Now consider $\angle AOC$. This is an external angle of $\triangle OBC$, so by Exercise 6.4, it is equal to the sum of two other angles: $\angle AOC = \angle OBC + \angle OCB = 2\angle OCB = 2\angle ACB$. □

The next step is to generalize it to the case when AC is not necessarily a diameter of Σ. however, one must be careful when doing this. The following "theorem" seems a natural generalization — however, it is not correct as stated. We give it here as an example of why it is dangerous to base your proof on things which are "obvious from the figure".

Theorem 8.16 (INCORRECT)**.** *Let Σ be a circle with center O, and let A, B, C be distinct points on Σ. Then $m\angle ACB = \frac{1}{2} m\angle AOB$.*

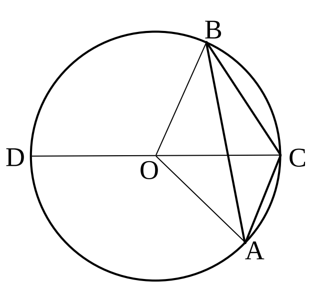


"Proof". Let D be the point on Σ such that CD is a diameter (it is easy to show that such a point exists and is unique). Then $m\angle ACB = m\angle ACD + m\angle DCB$. Since CD is a diameter, we can apply Proposition 8.15 to triangles $\triangle ACD, \triangle DCB$ which gives $\angle ACD = \frac{1}{2}\angle AOD, m\angle DCB = \frac{1}{2} m\angle DOB$, so

$$m\angle ACB = \frac{1}{2}(m\angle AOD + m\angle DOB) = \frac{1}{2} m\angle AOB$$

□

So what is wrong with this theorem and this proof? Here is one problem: if we choose A, B, C so that $\angle ACB > \pi/2$ as shown below, then according to this theorem, $\angle AOB = 2\angle ACB > \pi$. But by Protractor axiom, the measure of any angle is $\leq \pi$. So we get a contradiction which shows that this theorem can not be correct as stated.



Closer look also shows what is the likely origin of this trouble. Namely, looking at this example it seems that the formula $m\angle ACB = \frac{1}{2} m\angle AOB$ would be true if we gave different interpretation of $m\angle AOB$: if instead of measuring the smaller of two angles formed by rays OA and OB (which is the definition we used in Protractor axiom and elsewhere), we measured that of the two angles which contains the point D. This also shows the gap in the proof: the proof assumes that $m\angle AOD + m\angle DOB = m\angle AOB$; however, we didn't explain why it is so. It could be justified by referring to Protractor axiom — but only if the ray $\overrightarrow{OD}$ is inside angle $\angle AOB$. As the two figures above show, this is not always true.

As mentioned above, the statement of the theorem can be corrected. There are several ways of doing so. One possibility is to change the way we measure angles, so instead of saying "for every angle we have its measure", we would say "for every sector there is a measure", with a sector being one of two regions of the plane bounded by the angle. Then replacing in Theorem 8.16 $m\angle AOB$ by "measure of the sector bounded by $\angle AOB$ which does not contain point C" would give a correct theorem.

This can be done (and, in fact, this is the way it is done in most elementary geometry books), but it would require some work — and it is too late to do so now, as we have already extensively used the notion of anlge and Protractor axiom. Therefore, instead we give the following reformulation of Theorem 8.16.

Theorem 8.17. *Let Σ be a circle with center O, and let A, B, C be distinct points on Σ. Then*

$$m\angle AOB = \begin{cases} 2m\angle ACB, & \text{if } m\angle ACB \leq \pi/2 \\ 2\pi - 2m\angle ACB, & \text{if } m\angle ACB > \pi/2 \end{cases}$$

9. Coordinates

In this section, we show how one can relate this axiomatic approach to Euclidean geometry with the familiar coordinate one, in which we use a coordinate system to describe a point by a pair of real numbers — its x and y coordinates. Please note that this is a relatively new approach to geometry: it was introduced Descartes in 17th century — less than 4 centuries ago (for comparison, Euclid's *Elements* were written 23 centuries ago). We will discuss advantages and disadvantages of this approach later.

9.1. Coordinate system. A coordinate system is an identification $f\colon P \to \mathbb{R}^2$, where P is the plane (i.e., the set of all point considered in Euclidean geometry) and $\mathbb{R}^2$ is the set of all pairs (x, y) of real numbers. This naturally extends the notion of coordinate system on a line, discussed in Ruler Axiom.

As with a line, there is more than one coordinate system on the plane. In order to define a coordinate system, we need to specify the origin and coordinate axes. Here are the precise definitions.

Definition 9.1. A coordinate system on the plane is the following collection of data:

- A point O (called the origin).
- Rays $\overrightarrow{OA}$ and $\overrightarrow{OB}$ such that $\overleftrightarrow{OA} \perp \overleftrightarrow{OB}$.

The lines OA and OB are usually called x-axis and y-axis respectively. Please note that the definition of coordinate system asks not just for the lines but for the rays — this is needed to determine the direction on each of the axes.

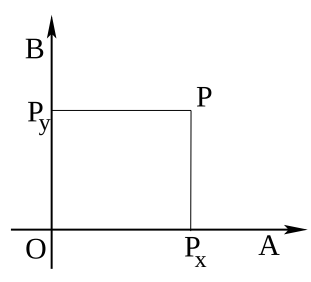
Now comes the promised result about identifying the set of all points with $\mathbb{R}^2$.

Theorem 9.1. *Every coordinate system $O, \overrightarrow{OA}, \overrightarrow{OB}$ defines an identification of the set of all points with $\mathbb{R}^2$.*

Proof. To define an identification, we need:

- Describe a map $f\colon \{points\} \to \mathbb{R}^2$
- Show that conversely, for each $(x, y) \in \mathbb{R}^2$, there is a unique point P corresponding to it (i.e., such that $f(P) = (x, y)$).

To define f, note first that by Ruler Axiom, choice of O and a ray $\overrightarrow{OA}$ defines a coordinate system $f_x\colon \overleftrightarrow{OA} \to \mathbb{R}$ such that $f_x(O) = 0, f_x(A) > 0$. Similarly, ray $\overrightarrow{OB}$ defines a coordinate system $f_y\colon \overleftrightarrow{OB} \to \mathbb{R}$. This allows us to label points on both axes by real numbers.



Now let P a point. Drop perpendiculars PP_x, PP_y from P to $\overleftrightarrow{OA}$ (x-axis) and $\overleftrightarrow{OB}$ (y-axis) (such perpendiculars exist and are unique by Theorem 6.4). So we have two "projections" of P on the axes. Next, define the x and y coordinates $x = f_x(P_x), y = f_y(P_y)$ by using the coordinate systems f_x on the x-axis and f_y on the y-axis. Thus, we have defined a map which for a given point P gives pair of real numbers x and y. We will say that x, y are coordinates of P, or that P has coordinates x, y.

Conversely, let x, y be real numbers. To show that there is a unique point P with coordinates x, y, let P_x be the point on the x-axis such that $f_x(P_x) = x$ (such a point exists and is unique by the Ruler Axiom); similarly, let P_y be the point on y-axis such that $f_y(P_y) = y$. Let l be the perpendicular to x-axis through P_x (exists by Protractor Axiom), and m the perpendicular to y-axis through P_y. Let P be the intersection point of l and m. Then we claim that P has coordinates (x, y) we started with, and moreover, P is the only point that has these coordinates. The proofs of these two statements is left as an easy exercise to the reader. □

As usual, we will write $P = (x, y)$ to say "point P has coordinates (x, y)". We will also commonly use word "horizontal" for a line which is parallel to x-axis and "vertical" for a line which is parallel to y-axis.

Exercise 9.1: Show that any horizontal line is perpendicular to any vertical line.

Exercise 9.2: Show that two distinct points A, B have the same coordinate iff $\overleftrightarrow{AB}$ is a vertical line.

9.2. Equation of a line. In this section we will show that any line l not parallel to y axis can be described by an equation $y = mx + b$. This is not quite easy and requires some preparation. Throughout this section, we assume that we have chosen some coordinate system on the plane.

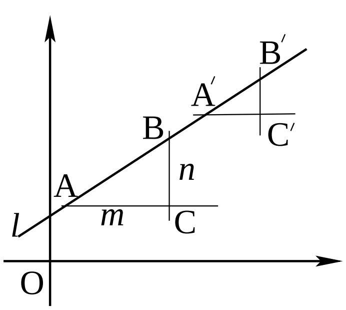
Exercise 9.3: Let $A = (x_1, y_1), B = (x_2, y_2)$ be distinct points. Prove that $\overleftrightarrow{AB}$ is parallel to the y-axis iff $x_1 = x_2$.

Definition 9.2. Let $A = (x_1, y_1), B = (x_2, y_2)$ be points such that $x_1 \neq x_2$. Then we define slope of segment AB by

$$m(AB) = \frac{y_2 - y_1}{x_2 - x_1}$$

Theorem 9.2. *Let l be a line which is not parallel to the y-axis, and let A, B, A', B' be points on l such that $A \neq B, A' \neq B'$. Then the slopes of segments AB and $A'B'$ are equal: $m(AB) = m(A'B')$.*

Proof.



Let m be the line through A parallel to x-axis (exists and is unique by Parallel lines axiom), and n the line through B parallel to y-axis. By Exercise 9.1, $m \perp n$. Let C be the intersection point of m, n. Then $\triangle ABC$ is the right triangle: $m\angle C = \pi/2$, and $|AC| = x_2 - x_1$, $|BC| = y_2 - y_1$ where $A = (x_1, y_1), B = (x_2, y_2)$.
Similarly, let m' be the line through A' parallel to x-axis, and n' the line through B' parallel to y-axis, and let C' be the intersection point of m', n'. Then $\triangle A'B'C'$ is the right triangle: $m\angle C' = \pi/2$, and $|A'C'| = x'_2 - x'_1$, $|B'C'| = y'_2 - y'_1$ where $A' = (x'_1, y'_1), B' = (x'_2, y'_2)$.

Using Theorem 6.2, we see that $m\angle A = m\angle A', m\angle B = m\angle B'$. Thus, $\triangle ABC \sim \triangle A'B'C'$ by AAA. Thus, by definition of similar triangles, $\frac{|A'C'|}{|AC|} = \frac{|B'C'|}{|BC|}$. Denoting this ratio by k, we get $x'_2 - x'_1 = k(x_2 - x_1), y'_2 - y'_1 = k(y_2 - y_1)$, so

$$\frac{y'_2 - y'_1}{x'_2 - x'_1} = \frac{y_2 - y_1}{x_2 - x_1}$$

□

Exercise 9.4: This proof actually has the same deficiencies as our (incorrect) proof of the theorem about central angles: it uses some information about relative positions of points on the line l which is true in the figure shown but was not proved (and, in fact, may be false) in general. Can you identify what information it uses and in which step?

Fortunately, the theorem is still true: even though the proof above has gaps, it can be fixed. Can you do this?

This theorem implies that for a line l not parallel to y-axis, we can define its slope $m(l)$ as the slope of any segment on this line. According to the theorem above, the result doesn't depend on which segment we used.

Now we are ready to prove the main result about equation of a line.

Theorem 9.3. *Let l be a line with slope m which contains point $P = (x_0, y_0)$. Then a point $A = (x, y)$ lies on l iff x, y satisfy the equation*

$$y - y_0 = m(x - x_0)$$

Proof. First, we prove that if $A \in l$ then x, y satisfy this equation. Indeed, by Theorem 9.2 and the definition of the slope of a line, the slope of AP must be equal to the slope of l, so $\frac{y-y_0}{x-x_0} = m$. This is equivalent to the equation above.

Conversely, assume that x, y satisfy $y - y_0 = m(x - x_0)$. We need to prove that $A \in l$.

Consider the line going through A and parallel to y-axis. Let $A' = (x', y')$ be the point of intersection of this line with l. Since $\overleftrightarrow{AA'}$ is parallel to y-axis, points A and A' have the same x-coordinate. Thus, $x = x'$. Next, by previous argument, $y' - y_0 = m(x' - x_0) = m(x - x_0)$. Thus, $y' = m(x - x_0) + y_0 = y$. So $A = A'$. Since by construction '$A' \in l$, this gives $A \in l$. □

Of course, writing the equation of a line is only the beginning. We could continue in this vein and develop equations of a circle, develop trigonometry and so on. However, as we do not have time to cover all this (and most of this you have already seen in other courses), we stop here.

9.3. Advantages and disadvantages of coordinate method. One of the natural questions people ask after seeing the coordinate method is this: why don't we just forget axiomatic approach to Euclidean geometry and start by defining the plane to be the set $\mathbb{R}^2$, let lines be defined by equations like $y = mx+b$, and so on? In fact, some mathematicians (for example, French mathematician J. Dieudonne) have suggested this approach to the study of geometry. However, this has some serious drawbacks. For example, consider Corollary 8.14: three angle bisectors in a triangle intersect at a single point. The proof given in these notes (and going back to Euclid) is rather nice and is based essentially on the fact that there is a unique inscribed circle. However, proving the same theorem using the coordinate approach, by writing equations of the three angle bisectors and then showing that these three equations have a common solution, while not impossible, results in 2 pages of extremely messy computations. So the coordinate approach, while powerful, is not a replacement for a more traditional approach: the best way would to to combine them. By the way, Descartes himself was fully aware of the drawbacks of the coordinate approach and never suggested that it is a is a magical cure-all.

And for the purposes of MAT 200, we certainly want the axiomatic approach: the whole point of this part of the course was to show you logic in action, proving results starting with the axioms and advancing to more and more complicated ones. Axiomatic approach to Euclidean geometry provides a very good example of this.

Homework 2

1. Problem 1, page 53.
2. Problem 3, page 53.
3. Problem 5, page 53.
4. Problem 6, page 54.
5. Problem 9, page 54.
6. Problem 10, page 54.
7. Problem 14, page 55.
8. Show that
$$\sqrt{2+\sqrt{2+\sqrt{2+\cdots+\sqrt{2}}}} = 2\cos\left(\frac{\pi}{2^{n+1}}\right),$$
where there are n 2s in the expression on the left.
9. (Towers of Hanoi) Suppose you have three posts and a stack of n disks, initially placed on one post with the largest disk on the bottom and each disk above it is smaller than the disk below. A legal move involves taking the top disk from on post and moving it so that it becomes the top disk on another post, but every move must place a disk either on and empty post, or on top of a disk larger than itself. Show that for every n there is a sequence of moves that will terminate with all the disks on a post different from the original one. How many moves are required for an initial stack of n disks?

Homework 3

1. Problem 18, page 55.
2. Problem 20, page 56.
3. Problem 21, page 56.
4. Problem 22, page 56.
5. Problem 25, page 57.
6. Problem 26, page 57.
7. Problem 2, page 115.
8. Problem 4, page 115
9. Read Definition 7.7.1 on page 83, and prove followings.
   - $A \times \varnothing = \varnothing$
   - $A \times (B \cup C) = (A \times B) \cup (A \times C)$

Homework 4

1. Problem 5, page 115
2. Problem 7, page 116
3. Problem 8, page 116
4. Problem 9, page 116
5. Problem 18, page 118
6. Let $f : \mathbb{R} \to \mathbb{R}$ be a function and G_f its graph. i.e, $G_f = \{(x, y) \in \mathbb{R}^2 | y = f(x)\}$. We also define $h_{y_0} := \{(x, y) \in \mathbb{R}^2 | y = y_0\}$. Show that if there is $y_0 \in \mathbb{R}$ such that $|G_f \cap h_{y_0}| \geq 2$, then f is not injective (This is also known as "horizontal line test").
7. A set of all functions $f : X \to Y$ is denoted Y^X. For any finite set S, prove that $|\mathcal{P}(S)| = |T^S|$, where $T = \{0, 1\}$.
   Hint : First show that each $f \in T^S$ can be written as

$$\chi_A(x) = \begin{cases} 1 & \text{if } x \in A \\ 0 & \text{if } x \notin A \end{cases}$$

   for some $A \in \mathcal{P}(S)$. Then prove the assignment $A \in \mathcal{P}(S) \mapsto \chi_A \in T^S$ is bijective (the function χ_A is called *characteristic function of* A).

Homework 5

1. Exercise 2.5, Geometry Note Page 4.
2. Exercise 2.6, Geometry Note Page 4.
3. Exercise 3.2, Geometry Note Page 6.
4. Exercise 3.3, Geometry Note Page 6.
5. Exercise 3.4, Geometry Note Page 6.
6. Exercise 3.8, Geometry Note Page 7.
7. Exercise 3.9, Geometry Note Page 7.

Homework 6

1. Exercise 3.11, Geometry Note Page 8.
2. Exercise 3.12, Geometry Note Page 8.
3. Exercise 3.14, Geometry Note Page 8.
4. Exercise 5.1, Geometry Note Page 14.
5. Exercise 5.2, Geometry Note Page 14.
6. Exercise 5.8, Geometry Note Page 16.
7. Exercise 5.10, Geometry Note Page 17.

Homework 7

1. Problem 11.6, page 143
2. Problem 12.3, page 155
3. Problem 12.4, page 155
4. Problem 12.5, page 155
5. 145 points are chosen at random in a one-foot by one-foot square. Prove that there exists two points no more than $\sqrt{2}$ inches apart.
6. Given n integers $a_1, a_2 \cdots, a_n$, not necessarily distinct, there exist integers k and l with $0 \leq k < l \leq n$ such that the sum $a_{k+1} + a_{k+2} + \cdots + a_l$ is a multiple of n.
   Hint: Consider following n integers; a_1, $a_1 + a_2$, $a_1 + a_2 + a_3$, $\cdots$, $a_1 + a_2 + \cdots a_n$. What are their remainders after divided by n?

Homework 8

1. Problem 1, page 182
2. Problem 4, page 182
3. Problem 14, page 184
4. Problem 18, page 185
5. Problem 19.3, page 239

MAT 200: Logic, Language and Proof
Spring 2014

Exams

Practice Exam for Midterm 1

Practice Exam Solution for Midterm 1

Practice Exam for Midterm 2

Practice Exam for Final
Practice Exam Solution for Final

Practice Exam

1. Find negations of following statements.
   - For some real number a, $f(a) = 0$.
   - For all integers m and n, there is an integer p such that $n \geq pm$.
   - $\forall n \in \mathbb{Z}, \exists m \in \mathbb{Z}, m \leq n$.
   - $(\exists q \in \mathbb{Z}, n = 2q+1) \Rightarrow (\exists p \in \mathbb{Z}, n^2 = 2p+1)$.
2. Prove following statements by contradiction.
   - $\sqrt[3]{2}$ is irrational.
   - There exist no integers a and b such that $21a + 30b = 1$.
   - If $a, b \in \mathbb{Z}$, then $a^2 - 4b - 3 \neq 0$.
3. Prove following by induction principle.
   - $n! > 2^n$ for $n \geq 4$.
   - Let f_i be ith Fibonacci number. Show that $\Sigma_{i=1}^{n} f_i^2 = f_n f_{n+1}$.
   - Let a_n be the sequence defined by $a_1 = 1$, $a_2 = 8$, $a_n = a_{n-1} + 2a_{n-2}$, $(n \geq 3)$. Prove that $a_n = 3 \cdot 2_{n-1} + 2(-1)^n$ for all $n \in \mathbb{Z}_+$.
4. By using truth table, for any sets A, B, C and some universal set U, followings hold.
   - $A^c \times B^c \subset (A \times B)^c$
   - $(A - B) - C \subset A - (B - C)$
   - $A \times (B \cup C) = (A \times B) \cup (A \times C)$.
5. Prove or disprove followings.
   - $\exists y \in \mathbb{R}, \forall x \in \mathbb{R}, xy = 1$
   - $\forall x \in \mathbb{R}, \exists y \in \mathbb{R}, xy = 1$
   - $\forall n \in \mathbb{Z}_+, (n$ is even or n is odd).
   - $(\forall x \in \mathbb{Z}_+, n$ is even) or $(\forall x \in \mathbb{Z}_+, n$ is odd)
6. Determine wheter each of following functions is injective, surjective or bijective.
   - $f_1 : \mathbb{R} \to \mathbb{R}$, $f_1(x) = x^3 - x$
   - $f_2 : \mathbb{Z} \to \mathbb{Z}$, $f_2(x) = x^3$
7. Let $f : X \to Y$ is a function and $A_1, A_2 \in \mathcal{P}(X)$.
   - $A_1 \subset A_2 \Rightarrow f(A_1) \subset f(A_2)$
   - $f(A_1 \cap A_2) \subset f(A_1) \cap f(A_2)$
   - $f(A_1 \cup A_2) = f(A_1) \cup f(A_2)$
   - $A_1 \cap A_2 = \varnothing \Rightarrow f^{-1}(A_1) \cap f^{-1}(A_2) = \varnothing$

Practice Exam Solution

1. Find negations of following statements.

   - For some real number a, $f(a) = 0$.
     Solution. For every real number a, $f(a) \neq 0$.
   - For all integers m and n, there is an integer p such that $n \geq pm$.
     Solution. There exist integers m and n, such that $n < pm$ for every integer p.
   - $\forall n \in \mathbb{Z}, \exists m \in \mathbb{Z}, m \leq n$.
     Solution. $\exists n \in \mathbb{Z}, \forall m \in \mathbb{Z}, m > n$.
   - $(\exists q \in \mathbb{Z}, n = 2q + 1) \Rightarrow (\exists p \in \mathbb{Z}, n^2 = 2p + 1)$.
     Solution. $(\exists q \in \mathbb{Z}, n = 2q + 1)$ and $(\forall p \in \mathbb{Z}, n^2 \neq 2p + 1)$

2. Prove following statements by contradiction.

   - $\sqrt[3]{2}$ is irrational.
     Solution. Suppose not. Let $\sqrt[3]{2} = p/q$, where p/q is a reduced fraction. Then $2 = p^3/q^3$, so $p^3 = 2q^3$. It is easy to show that "if n is even $\Leftrightarrow n^3$ is even." p^3 is even thus p is even. Let $p = 2k$. Then $4k^3 = q^3$, so q is even, contradiction.
   - There exist no integers a and b such that $21a + 30b = 1$.
     Solution. Suppose there are such a and b. Then left hand side of the equation is divisible by 3, but right hand side is not.
   - If $a, b \in \mathbb{Z}$, then $a^2 - 4b - 3 \neq 0$.
     Solution. We will consider four cases of a, depending on remainder of a divided by 4. Case 1. If $a = 4k$, then the left hand side of the equation is $4(4k^2 - b) - 3$, which cannot be zero. Case 2. If $a = 4k + 1$, then $4(4k^2 + 2k - b) - 2$ cannot be zero. Case 3. If $a = 4k+2$, then $4(4k^2 + 4k + 1 - b) - 3$ cannot be zero. Case 4. If $a = 4k + 3$, then $4(4k^2 + 6k + 2 - b) - 2$ cannot be zero.

3. Prove following by induction principle.

   - $n! > 2^n$ for $n \geq 4$.
     Solution. Induction on n. If $n = 4$, $24 = 4! > 2^4 = 16$. Assume $n! > 2^n$. Then $(n+1)! = (n+1) \cdot n! > 2^n(n+1) > n2^n + 2^n > n2^n > 2 \cdot 2^n > 2^{n+1}$.
   - Let f_i be ith Fibonacci number. Show that $\Sigma_{i=1}^n f_i^2 = f_n f_{n+1}$.
     Solution. Induction on n. If $n = 1, (f_1)^2 = f_1 \cdot f_2$. Assume $\Sigma_{i=1}^n f_i^2 = f_n f_{n+1}$. Then $\Sigma_{i=1}^n f_i^2 + f_{n+1}^2 = f_n f_{n+1} + f_{n+1}^2 = f_{n+1}(f_n + f_{n+1}) = f_{n+1} f_{n+2}$.
   - Let a_n be the sequence defined by $a_1 = 1$, $a_2 = 8$, $a_n = a_{n-1} + 2a_{n-2}$, $(n \geq 3)$. Prove that $a_n = 3 \cdot 2^{n-1} + 2(-1)^n$ for all $n \in \mathbb{Z}_+$.
     Solution. Induction on n. If $n = 1, a_1 = 3 \cdot 1 - 2 = 1$. If $n = 2, a_2 = 3 \cdot 2 + 2 = 8$. Assume $a_n = 3 \cdot 2^{n-1} + 2(-1)^n$ for all $n \leq k$. Then $a_{k+1} = a_k + 2a_{k-1} = 3 \cdot 2^{k-1} + 2(-1)^k + 6 \cdot 2^{k-2} + 4(-1)^{k-1} = 3 \cdot 2^{k-2}(2+2) + 2(-1)^{k-1}(-1+2) = 3 \cdot 2^k + 2(-1)^{k+1}$.

4. By using truth table, for any sets A, B, C and some universal set U, followings hold.

- $A^c \times B^c \subset (A \times B)^c$
  Solution. Omitted. Will be covered in review.
- $(A - B) - C \subset A - (B - C)$
  Solution. Omitted. Will be covered in review.
- $A \times (B \cup C) = (A \times B) \cup (A \times C)$.
  Solution. Omitted. Will be covered in review.

5. Prove or disprove followings.

- $\exists y \in \mathbb{R}, \forall x \in \mathbb{R}, xy = 1$
  Solution. False.
- $\forall x \in \mathbb{R}, \exists y \in \mathbb{R}, xy = 1$
  Solution. False. Counterexample : $x = 0$.
- $\forall n \in \mathbb{Z}_+, (n$ is even or n is odd).
  Solution. True.
- $(\forall n \in \mathbb{Z}_+, n$ is even) or $(\forall n \in \mathbb{Z}_+, n$ is odd)
  Solution. False.

6. Determine wheter each of following functions is injective, surjective or bijective.

- $f_1 : \mathbb{R} \to \mathbb{R}$, $f_1(x) = x^3 - x$
  Solution. f_1 is not injective, since $f_1(1) = f_1(0) = 0$. However, f_1 is surjective, since for any $k \in \mathbb{R}$, $x^3 - x - k = 0$ for some x.
- $f_2 : \mathbb{Z} \to \mathbb{Z}$, $f_2(x) = x^3$
  Solution. f_2 is injective, since $f_2(n) = f_2(m)$ implies $n^3 - m^3 =$, and $n^3 - m^3 = (n - m)(n^2 + nm + m^2) = 0$, thus $n = m$. However, it is not surjective. (i.e, $f_2(n) \neq 2$ for all n.)

7. Let $f : X \to Y$ is a function and $A_1, A_2 \in \mathcal{P}(X)$.

- $A_1 \subset A_2 \Rightarrow f(A_1) \subset f(A_2)$
  Solution. Suppose $y \in f(A_1)$. Then $\exists x \in A_1, f(x) = y \quad \Rightarrow \quad x \in A_2, f(x) = y$. Thus, $y \in f(A_2)$.
- $f(A_1 \cap A_2) \subset f(A_1) \cap f(A_2)$
  Solution. Let $y \in f(A_1 \cap A_2)$. Then $\exists x \in A_1 \cap A_2, f(x) = y$. This implies $\exists x \in A_1, f(x) = y$ and $\exists x \in A_2, f(x) = y$. Thus $y \in f(A_1 \cap A_2)$.
- $f(A_1 \cup A_2) = f(A_1) \cup f(A_2)$
  Solution $\subset$ inclusion is obvious(same argument as above). To prove other direction, let $y \in f(A_1) \cup f(A_2)$. Then $(\exists x_1 \in A_1, f(x) = y)$ or $(\exists x_2 \in A_2, f(x) = y)$. In either cases, there exists $x \in A_1 \cup A_2$ ($x = x_1$ or $x = x_2$) such that $f(x) = y$.
- $A_1 \cap A_2 = \varnothing \Rightarrow f^{-1}(A_1) \cap f^{-1}(A_2) = \varnothing$
  Solution Omitted, since inverse image was not covered in class.

Midterm 2 questions

The exam will be based on geometry note, from Chapter 1 to Chapter 7. Although you do not need to memorize all definitions, axioms and theorems(most of them will be given in the exam), you need to understand and be able to use to prove questions.

1. We will use a sphere for a model for geometry. A plane is the sphere, and a line contains two points is a great circle contains the two points. Convince yourself (possibly by drawing a picture) that this model satisfies the Incidence Axiom, but fails to satisfy the Parallel Axiom.

2. On page 15, in the proof of Theorem 5.3, discuss why the following statement is true.

   "... If the two triangles were not congruent, then one of the angles of $\triangle ABC$ would have measure different from the measure of the corresponding angle of $\triangle A'B'C'$. "

3. Justify following statement on page 18, from the proof of Theorem 5.9.

   "... Looking at $\triangle ADC$, it follows that $m\angle D < m\angle C$."

4. Theorem 5.6 on page 16 claims $m\angle ACD > m\angle B$. By using the Parallel Axiom, prove that a stronger result; $m\angle ACD = m\angle B + m\angle A$.

5. For any triangle $\triangle ABC$, prove that there is a unique altitude through A, assuming the Parallel Axiom.

6. Let $\triangle ABC$ be a right triangle with $\angle C = \pi/2$. $D \in \overline{BC}$ such that $\overleftrightarrow{CD}$ is the altitude through C. Prove that

$$\frac{1}{|AB|^2} + \frac{1}{|AC|^2} = \frac{1}{|CD|^2}$$

7. A quadrilateral $\diamondsuit ABCD$ is *convex* if A and C are on opposite sides of $\overleftrightarrow{BD}$, and if B and D are on opposite sides of $\overleftrightarrow{AC}$. Show that this definition can be replaced by following statement (Exercise 6.6).

   $\diamondsuit ABCD$ is convex if $\overline{AC}$ and $\overline{BD}$ meet in a point.

   Discuss why following cannot replace the definition of convex quadrilateral.

   $\diamondsuit ABCD$ is convex if $\overleftrightarrow{AC}$ and $\overleftrightarrow{BD}$ meet in a point.

8. Prove that a diagonals segment of a parallelogram bisects the other diagonal segment.

Final Exam Practice

1. For a non-negative integers n define the sequence a_n inductively as follows.

$$\begin{aligned} a_0 &= 1 \\ a_{k+1} &= 3a_k + 1 \end{aligned}$$

Guess the general term of the sequence and prove your answer by mathematical induction.

2. Write following statement using quantifiers: "For every positive real number ϵ, there exists a positive real number δ, such that if $|x - a| \leq \delta$ then $|f(x) - f(a)| \leq \epsilon$." What is the negation of this statement?

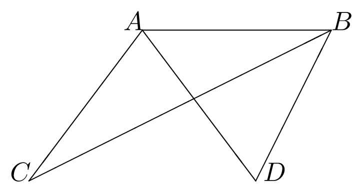
3. Functions $f : \mathbb{R} \to \mathbb{R}$ and $f : \mathbb{R} \to \mathbb{R}$ are defined as follows.

$$f(x) = \begin{cases} x+2 & \text{if } x < -1, \\ -x & \text{if } -1 \leq x \leq 1, \\ x-2 & \text{if } x > 1. \end{cases}$$

$$g(x) = \begin{cases} x-2 & \text{if } x < -1, \\ -x & \text{if } -1 \leq x \leq 1, \\ x+2 & \text{if } x > 1. \end{cases}$$

Find functions $f \circ g$ and $g \circ f$. Is the g inverse of f? Is f injective or bijective? How about g? Sketch and compare the graphs of these functions.

4. Suppose $|AB| = |AC| = |AD|$. Prove that $\angle CAD = 2\angle CBD$.



5. Find the coefficient of x^9 of $(2+x)^7(1-x)^4$.

6. You have 5 identical red balls, 7 identical blue balls, and 4 identical yellow balls, and 8 identical green balls. How many different ways to place them in a row?

7. Let $k \in \mathbb{Z}^+$, $r \in \mathbb{Z}^{\geq 0}$. Find the number of nonnegative solutions of $x_1 + x_2 + \cdots x_k = r$.

8. Show that among any $n+1$ integers, there exists 2 integers so that their difference is divisible by n.

9. A *dearrangement* of $\mathbb{N}_n$ is a bijection $f : \mathbb{N}_n \to \mathbb{N}_n$ with no fixed points. Show that the number of dearrangement is

$$n!\left(\frac{1}{2!} - \frac{1}{3!} + \frac{1}{4!} - \cdots + (-1)^n \frac{1}{n!}\right)$$

(Problem 17, page 185)

10. Prove that $(0, 1) \subset \mathbb{R}$ is not enumerable.

11. For any set X, show that $|X| < |\mathcal{P}(X)|$.

12. Write the greatest common divisor of 662 and 242 as an integral linear combination of 662 and 242, by using Euclidean algorithm.

13. Find all solutions of $242x \equiv 22 \pmod{662}$ in $\mathbb{Z}_{662}$.

14. Fix positive integers a and b. Show that

$$\{am + bn \mid m, n \in \mathbb{Z} \text{ and } am + bn > 0\}$$

has the minimum element c, and c is a common divisor of a and b.

15. Define a relation on $\mathbb{R}$ such that $x \sim y \iff x^2 = y^2$. Show that this relation is an equivalence relation. Describe a class $[4]$ in set builder notation.

16. Show that $3x^2 + 4y^2 = 5z^2$ has no integral solution other than $(0, 0, 0)$.

17. Show that following functions are not well defined.

$$\begin{aligned} f &: \mathbb{Q} \to \mathbb{Q}, \qquad & f\left(\frac{a}{b}\right) &= \frac{a^2}{b^3} \\ g &: \mathbb{Z}_6 \to \mathbb{Z}_4, \qquad & g([a]_6) &= [a+1]_4 \end{aligned}$$

Final Exam Practice

1. For a non-negative integers n define the sequence a_n inductively as follows.

$$\begin{aligned} a_0 &= 1 \\ a_{k+1} &= 3a_k + 1 \end{aligned}$$

Guess the general term of the sequence and prove your answer by mathematical induction.
Solution. We will find p so that the recurrence relation is $a_{k+1} + p = 3(a_k + p)$.

$$a_{k+1} + p = 3a_k + 1 + p = 3\left(a_k + \frac{1+p}{3}\right)$$

Thus $p = (1+p)/3 \Leftrightarrow p = 1/2$. Let $b_k = a_k + \frac{1}{2}$. Then the recurrence relation is simplified to $b_{k+1} = 3b_k$, with $b_0 = \frac{3}{2}$. Then $b_n = \frac{3}{2}3^n$, which results $a_n = \frac{3}{2}3^n - \frac{1}{2}$.

2. Write following statement using quantifiers: "For every positive real number ϵ, there exists a positive real number δ, such that if $|x - a| \leq \delta$ then $|f(x) - f(a)| \leq \epsilon$." What is the negation of this statement?
Solution. There exists $\epsilon > 0$ such that for all $\delta > 0$, $|x - a| \leq \delta$ and $|f(x) - f(a)| > \epsilon$.

3. Functions $f : \mathbb{R} \to \mathbb{R}$ and $f : \mathbb{R} \to \mathbb{R}$ are defined as follows.

$$f(x) = \begin{cases} x+2 & \text{if } x < -1, \\ -x & \text{if } -1 \leq x \leq 1, \\ x-2 & \text{if } x > 1. \end{cases}$$

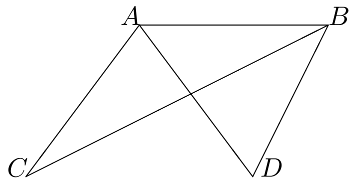
$$g(x) = \begin{cases} x-2 & \text{if } x < -1, \\ -x & \text{if } -1 \leq x \leq 1, \\ x+2 & \text{if } x > 1. \end{cases}$$

Find functions $f \circ g$ and $g \circ f$. Is the g inverse of f? Is f injective or bijective? How about g? Sketch and compare the graphs of these functions.
Solution. $(f \circ g)(x) = x$, but $(g \circ f)(x)$ is,

$$(g \circ f)(x) = \begin{cases} x & \text{if } x < -3, \\ -x-2 & \text{if } -3 \leq x \leq -1, \\ x & \text{if } -1 \leq x \leq 1, \\ -x+2 & \text{if } 1 \leq x \leq 3, \\ x & \text{if } x > 3. \end{cases}$$

Thus f and g are not inverses. In fact, f is surjective but not injective, and g is injective but not surjective.

4. Suppose $|AB| = |AC| = |AD|$. Prove that $\angle CAD = 2\angle CBD$.
Solution. Omitted.



5. Find the coefficient of x^9 of $(2+x)^7(1-x)^4$.
Solution. Coefficient of x^9 is computed by multiplying coefficient of x^7 term from the first binomial and x^2 term from the second binomial, x^6 and x^3, and x^5 and x^4. Coefficients of involving terms are obtained by using binomial theorem.

$$\begin{aligned} & \binom{7}{7} 2^0 \cdot \binom{4}{2} (-1)^2 \cdot x^7 \cdot x^2 \\ + & \binom{7}{6} 2^1 \cdot \binom{4}{3} (-1)^3 \cdot x^6 \cdot x^3 \\ + & \binom{7}{5} 2^2 \cdot \binom{4}{4} (-1)^4 \cdot x^5 \cdot x^4. \end{aligned}$$

The sum of these terms is $34x^9$.

6. You have 5 identical red balls, 7 identical blue balls, and 4 identical yellow balls, and 8 identical green balls. How many different ways to place them in a row?
Solution. $\dfrac{(5+7+4+8)!}{5! \cdot 7! \cdot 4! \cdot 8!}$.

7. Let $k \in \mathbb{Z}^+$, $r \in \mathbb{Z}^{\geq 0}$. Find the number of nonnegative solutions of $x_1 + x_2 + \cdots x_k = r$.
Solution. Consider r identical balls and $k-1$ identical barriers. Placing these $r+k-1$ objects in a row, we will have r ball are split into k different groups. The number of balls in ith group ($i = 1, 2, \cdots, k$) can be regarded as the value of x_i. Then the number of different ways to place $r+k-1$ objects in a row is same as the number of nonnegative integral solutions. Hence, the number of solutions is $(r+k-1)!/(r! \cdot (k-1)!)$.

8. Show that among any $n+1$ integers, there exists 2 integers so that their difference is divisible by n.
Solution. Let $\pi : \mathbb{Z} \to \mathbb{Z}_n$ be the projection map discussed in class. Let X be a set of $n+1$ integers. Then $\pi|_X : X \to \mathbb{Z}_n$ is a map obtained by restriction of domain. Since $|X| = n+1$ and $|\mathbb{Z}_n| = n$, by Pigeonhole Principle $\pi|_X$ cannot be an injection. So there must be $m, n \in X$ such that $[m] = [n] \in \mathbb{Z}_n$.

9. A *dearrangement* of $\mathbb{N}_n$ is a bijection $f : \mathbb{N}_n \to \mathbb{N}_n$ with no fixed points.

Show that the number of dearrangement is

$$n!\left(\frac{1}{2!}-\frac{1}{3!}+\frac{1}{4!}-\cdots+(-1)^n\frac{1}{n!}\right)$$

(Problem 17, page 185)
Solution. Let X be a set of all bijections from $\mathbb{N}_n$ to $\mathbb{N}_n$. Clearly $|X| = n!$. Also we let

$$A_i = \{f \in X \mid f(i) = i\},$$

for $i = 1, \cdots, n$. Then, $\bigcup_i A_i$ is a set of bijections that fix at least one element. This implies $X \backslash \bigcup_i A_i$ is the set of dearrangement. Since $\bigcup_i A_i$ is a subset of X, $|X \backslash \bigcup_i A_i| = |X| - |\bigcup_i A_i|$.
Before we try to compute $|\bigcup_i A_i|$, note that $|A_i| = (n-1)!$. Moreover, letting $A_I := A_{i_1} \cap A_{i_2} \cap \cdots \cap A_{i_r}$ (where $I = \{i_1, i_2, \cdots i_r\} \subset \mathbb{N}_n$), we can easily compute $|A_I| = (n - |I|)!$.

$$\begin{aligned}
\left|\bigcup_{i=1}^n A_i\right| &= \sum_{\varnothing \neq I \subset \mathbb{N}_n} (-1)^{|I|-1}|A_I| \quad \text{(inclusion-exclusion principle)} \\
&= \sum_{i=1}^n \sum_{\substack{I \in \mathbb{N}_n \\ |I|=i}} (-1)^{i-1}\ |A_I| \\
&= \sum_{i=1}^n \sum_{\substack{I \in \mathbb{N}_n \\ |I|=i}} (-1)^{i-1}\ (n-i)! \\
&= \sum_{i=1}^n \left(\begin{array}{c} n \\ i \end{array}\right) (-1)^{i-1}\ (n-i)! \\
&= \sum_{i=1}^n \frac{n!}{i! \cdot (n-i)!}\ (-1)^{i-1}\ (n-i)! \\
&= \sum_{i=1}^n \frac{n!}{i!} \cdot (-1)^{i-1}.
\end{aligned}$$

Thus,

$$\begin{aligned}
|X| - \left|\bigcup_{i=1}^n A_i\right| &= n! - \sum_{i=1}^n \frac{n!}{i!} \cdot (-1)^{i-1} \\
&= n!\left(\frac{1}{2!}-\frac{1}{3!}+\frac{1}{4!}-\cdots+(-1)^n\frac{1}{n!}\right).
\end{aligned}$$

10. Prove that $(0,1) \subset \mathbb{R}$ is not enumerable.
Solution. Omitted.

11. For any set X, show that $|X| < |\mathcal{P}(X)|$.
Solution. Omitted.

12. Write the greatest common divisor of 662 and 242 as an integral linear combination of 662 and 242, by using Euclidean algorithm.
Solution. By Euclidean Algorithm, $2 = 662 \cdot 34 + 242 \cdot (-93)$.

13. Find all solutions of $242x \equiv 22 \pmod{662}$ in $\mathbb{Z}_{662}$.
Solution. Since $\gcd(662, 242) = 2$, There should be two solutions in $\mathbb{Z}_{662}$. Dividing the equation by 2, $121x \equiv 11 \pmod{331}$. By previous question, $2 = 662 \cdot 34 + 242 \cdot (-93) \Leftrightarrow 1 = 331 \cdot 34 + 121 \cdot (-93)$. Mapping onto $\mathbb{Z}_{331}$, we get $1 \equiv 121 \cdot (-93) \pmod{331}$.

$$121x \equiv 11 \Leftrightarrow (-93) \cdot 121x \equiv (-93) \cdot 11 \equiv -1023 \equiv 301 \pmod{331}.$$

Thus $x \equiv 301 \pmod{331}$.
Then, solutions of $242x \equiv 22 \pmod{662}$ are

$$x \equiv 301 \text{ or } 301 + 331 = 632 \pmod{662}.$$

14. Fix positive integers a and b. Show that

$$\{am + bn \mid m, n \in \mathbb{Z} \text{ and } am + bn > 0\}$$

has the minimum element c, and c is a common divisor of a and b.
Solution. Let $am_0 + bn_0 = c$ for some $m_0, n_0 \in \mathbb{Z}$. Note that $a \geq c$ and $b \geq c$. Suppose not. Dividing a and b by c, we will have remainders r_1 and r_2 and at least one of them is nonzero. i.e,

$$a = cq_1 + r_1, \qquad b = cq_2 + r_2$$

$(r_1, r_2 < c)$.
Suppose $r_1 \neq r_2$. Without loss of generality, we can assume $r_2 > r_1$. Then

$$\begin{aligned} am_0q_1 + bn_0q_1 = cq_1 &= a - r_1 \\ am_0q_2 + bn_0q_2 = cq_2 &= b - r_2 \end{aligned}$$

Subtracting these two equations will yield,

$$a(m_0q_1 - m_0q_2 - 1) + b(n_0q_1 - n_0q_2 + 1) = r_2 - r_1 < c,$$

contradiction.
If $r_1 = r_2$, we will multiply 2 on second equation above. That is,

$$\begin{aligned} am_0q_1 + bn_0q_1 = cq_1 &= a - r_1 \\ 2am_0q_2 + 2bn_0q_2 = 2cq_2 &= 2b - 2r_2. \end{aligned}$$

Again, subtraction will yield

$$a(m_0q_1 - 2m_0q_2 - 1) + b(n_0q_1 - 2n_0q_2 + 2) = 2r_2 - r_1 = r_1 < c.$$

Again, contradiction. Therefore, c is a common divisor of a and b.

15. Define a relation on $\mathbb{R}$ such that $x \sim y \iff x^2 = y^2$. Show that this relation is an equivalence relation. Describe a class $[4]$ in set builder notation.
Solution. Reflexive. $x \sim x \Leftrightarrow x^2 = x^2$.
Symmetric. $x \sim y \Leftrightarrow x^2 = y^2$. This implies $y^2 = x^2 \Leftrightarrow y \sim x$.
Transitive. Suppose $x \sim y$ and $y \sim z$. Then $x^2 = y^2 = z^2$. Thus $x \sim z$.
The equivalence class $[4] = \{4, -4\}$.

16. Show that $3x^2 + 4y^2 = 5z^2$ has no integral solution other than $(0, 0, 0)$.
Solution. It suffices to consider solutions (x, y, z) such that the greatest common divisor of a, b, and c is 1. The equation $3x^2 + 4y^2 = 5z^2$ will become $3x^2 + 4y^2 \equiv 0 \pmod 5$ by mapping onto $\mathbb{Z}_5$. In $\mathbb{Z}_5$,

$$\begin{aligned} 0 &\mapsto 0^2 \equiv 0, \\ 1 &\mapsto 1^1 \equiv 1, \\ 2 &\mapsto 2^2 \equiv 4, \\ 3 &\mapsto 3^2 \equiv 4, \\ 4 &\mapsto 4^2 \equiv 1 \pmod 5. \end{aligned}$$

Suppose x and y are not multiple of 5. Then x^2 and y^2 must be one of 1 or 4 (mod 5). In this case, $3x^2 + 4y^2$ cannot be congruent to zero modulo 5. If $x = 5k$ and $y = 5l$, then the equation $3x^2 + 4y^2 = 5z^2$ can be reduced to $15k^2 + 20l^2 = z^2$. Again mapping onto $\mathbb{Z}_5$, the equation is $z^2 \equiv 0$ (mod 5). This forces z must be a multiple of 5, too. Contradiction. Hence, the given equation has no solution in $\mathbb{Z}_5$, so it has no solution in $\mathbb{Z}$.

17. Show that following functions are not well defined.

$$\begin{aligned} f : \mathbb{Q} \to \mathbb{Q}, &\qquad f\left(\frac{a}{b}\right) = \frac{a^2}{b^3} \\ g : \mathbb{Z}_6 \to \mathbb{Z}_4, &\qquad g([a]_6) = [a+1]_4 \end{aligned}$$

Solution. $f(1/2) = 1/8$, but $f(2/4) = 4/64 = 1/16$. Thus f is not well defined.
$g([1]_6) = [1 + 1]_4 = [2]_4$, but $g([1]_6 = [7]_6) = [1 + 7]_4 = [8]_4 = [0]_4$. Thus g is not well defined.

FUNDAMENTALS OF ZERMELO-FRAENKEL SET THEORY

TONY LIAN

ABSTRACT. This paper sets out to explore the basics of Zermelo-Fraenkel (ZF) set theory without choice. We will take the axioms (excluding the axiom of choice) as givens to construct and define fundamental concepts in mathematics such as functions, real numbers, and the addition operation. We will then explore countable and uncountable sets and end with the cardinality of the continuum.

CONTENTS

1. INTRODUCTION

Set theory is a branch of mathematics that studies collections of objects. Each collection is called a set and the objects in the collection are called elements of the set. Modern set theory began in the 1870s with the works of Georg Cantor and Richard Dedekind. Later work over the course of the 19th and 20th centuries revealed many paradoxes in set theory (some of which will be discussed later). This created a need for an axiomatic system that corrects these paradoxes. Ernst Zermelo proposed the first axiomatic set theory in 1908. Later, Abraham Fraenkel and Thoralf Skolem proposed some revisions including the addition of the Axiom Schema of Replacement. The resulting axiomatic set theory became known as Zermelo-Fraenkel (ZF) set theory. As we will show, ZF set theory is a highly versatile tool in defining mathematical foundations as well as exploring deeper topics such as infinity.

2. THE AXIOMS AND BASIC PROPERTIES OF SETS

Definition 2.1. A *set* is a collection of objects satisfying a certain set of axioms. (These axioms are stated below.) Each object in the set is called an *element* of the set.

Remark 2.2. The *membership property* is the most basic set-theoretic property. We denote it by $\in$. Thus we read $X \in Y$ as "X is an element of Y" or "X is a member of Y" or "X belongs to Y".

Since the axioms form our definition of a set, we need an axiom to postulate that sets indeed do exist. More specifically, that at least one set exists.

Axiom of Existence. *There exists a set which has no elements.*

Date: August 23, 2011.

Now that we've established that at least one set exists, we need a way to show uniqueness of sets. Intuitively, there should only be one set that has no elements, but we need the next axiom to prove this.

Axiom of Extensionality. *If every element of X is an element of Y and every element of Y is an element of X, then $X = Y$.*

From the Axiom of Extensionality, we see that $X = Y$ is a property based on the elements contained in X and Y. To generalize, if two sets have the same elements, then they are identical. We can now set out to prove the uniqueness of the set with no elements.

Lemma 2.3. *There exists only one set with no elements.*

Proof. Suppose there exists two sets A and B which both have no elements.
If $x \in A$ then $x \in B$.
If $y \in B$ then $y \in A$.
Therefore by the Axiom of Extensionality, $A = B$.
($x \in A$ is a false antecedent and so "$x \in A$ implies $x \in B$" is automatically true. The same is also true for $y \in B$.) □

Definition 2.4. The unique set with no elements is called the *empty set* and is denoted by $\varnothing$.

Now that we have established that a unique set exists, we are naturally interested in the existence and uniqueness of other sets.

Axiom Schema of Comprehension. *Let $P(x)$ be a property of x. For any A, there exists a B such that $x \in B$ if and only if $x \in A$ and $P(x)$ holds.*

Lemma 2.5. *For every A, there is a unique set B such that $x \in B$ if and only if $x \in A$ and $P(x)$.*

Proof. Suppose B' is another set such that $x \in B'$ if and only if $x \in A$ and $P(x)$.
If $x \in B$ implies $x \in A$ and $P(x)$, then $x \in B'$.
If $x \in B'$ implies $x \in A$ and $P(x)$, then $x \in B$.
Thus we have $x \in B$ if and only if $x \in B'$.
Therefore $B = B'$. □

Axiom of Pair. *For any A and B, there exists C such that $x \in C$ if and only if $x = A$ or $x = B$.*

Definition 2.6. We define the *unordered pair* of A and B as the set having exactly A and B as its elements and use $\{A, B\}$ to denote it.

Axiom of Union. *For any S, there exists U such that $x \in U$ if and only if $x \in A$ for some $A \in S$.*

Definition 2.7. We call the set U the union of S and denote it by $\bigcup S$.

Definition 2.8. We call A a *subset* of B if every element of A belongs to B. We denote this by $A \subseteq B$.

Axiom of Power Set. *For any S, there exists P such that $X \in P$ if and only if $X \subseteq S$.*

Definition 2.9. We call P the *power set* of S and denote it by $\mathscr{P}(S)$.

Axiom of Infinity. *An inductive set exists.*

We will revisit the Axiom of Infinity in more depth. Inductive sets will be defined later in the paper. They are crucial in defining the set of natural numbers.

Axiom Schema of Replacement. *Let $P(x, y)$ be a property such that for every x there is a unique y for which $P(x, y)$ holds. For every A there exists B such that for every $x \in A$ there is $y \in B$ for which $P(x, y)$ holds.*

The Axiom Schema of Replacement aims to correct some of the paradoxes that arise out of the use of the Axiom Schema of Comprehension. The key difference between the two is that the property $P(x, y)$ [in Replacement] depends both on x as well as the unique y for which $P(x, y)$ holds, whereas $P(x)$ [in Comprehension] only depends on x.

Definition 2.10. The *union* of A and B is the set of all x which belong in either A, B, or both. We denote it by $A \cup B$.

Remark 2.11. $A \cup B$ exists by our system of Axioms.
By Axiom of Pair, we have $\{A, B\}$.
Apply Axiom of Union on $\{A, B\}$ to arrive at $A \cup B$.

Definition 2.12. The *intersection* of A and B is the set of all x which belong to both A and B. We denote it by $A \cap B$.

Remark 2.13. $A \cap B$ also exists by our system of Axioms.
We can apply Axiom Schema of Comprehension to the set A and the property $P(x) : x \in B$. It is easy to show that $A \cap B = \{x \in A \,|\, x \in B\}$.

Definition 2.14. The *difference* of A and B is the set of all $x \in A$ such that $x \notin B$. We denote it by $A - B$.

Remark 2.15. It should be apparent that we can apply the Axiom Schema of Comprehension to the set A and the property $P(x) : x \notin B$ to arrive at $A - B = \{x \in A \,|\, x \notin B\}$.

Remark 2.16. As expected, each of the sets described above is unique. We will leave the proofs as exercises to the unconvinced reader.

3. Relations and Functions

Definition 3.1. An ordered pair (a, b) is defined to be $\{\{a\}, \{a, b\}\}$.

Since sets are unordered ($\{a, b\} = \{b, a\}$), this definition allows us to express ordered pairs as a unique set of a singleton $\{a\}$ and an unordered pair $\{a, b\}$. Using this system we can further define *ordered triples*

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

Ordered quadruples ... *ordered n-tuples* etc. follow in a similar fashion.

Definition 3.2. A set R is a *binary relation* if all elements of R are ordered pairs. (i.e. for $z \in R$ there exists x and y such that $z = (x, y)$. We can also denote $(x, y) \in R$ as xRy, and say that x is in relation R with y if xRy holds.)

Definition 3.3. The *membership relation on A* is defined by

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

The *identity relation on A* is defined by

$$Id_A = \{(a, b) \,|\, a \in A, b \in A, \text{ and } a = b\}.$$

Definition 3.4. Let A, B be sets. The *cartesian product of A and B* is defined by

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

Remark 3.5. We can use the axioms to show that the set $A \times B$ does in fact exist. By Axiom of Pair, $A \cup B$ exists as a unique set. Thus $\mathscr{P}(A \cup B)$ exists. Apply Axiom of Power Set again to show that $\mathscr{P}(\mathscr{P}(A \cup B))$ exists (and is unique). It is apparent that $(a, b) = \{\{a\}, \{a, b\}\} \in \mathscr{P}(\mathscr{P}(A \cup B))$. We simply apply the Axiom of Schema Comprehension with the properties $P(a) : a \in A$ and $P(b) : b \in B$ to finish constructing $A \times B$.

Definition 3.6. A binary relation F is called a *function* if aFb_1 and aFb_2 imply $b_1 = b_2$ for any a, b_1, and b_2. This unique b is the value of F at a and is denoted $F(a)$ or F_a. If dom $F = A$ and ran $F \subseteq B$, we can denote F by $F : A \to B$, $\langle F(a) \,|\, a \in A\rangle$, $\langle F_a \,|\, a \in A\rangle$, or $\langle F_a\rangle_{a\in A}$

Definition 3.7. Let $f : A \to B$ be a function.
1) f is *injective* if for $a_1 \in A$ and $a_2 \in A$, $f(a_1) = f(a_2)$ if and only if $a_1 = a_2$. We call f an *injection.*
2) f is *surjective* if for every $b \in B$, there exists some $a \in A$ such that $f(a) = b$. We call f a *surjection.*
3) f is *bijective* if it is both injective and surjective. We call f a *bijection.*

Definition 3.8.
(a) Functions f and g are called *compatible* if $f(x) = g(x)$ for all $x \in \operatorname{dom} f \cap \operatorname{dom} g$.
(b) A set of functions F is called a *compatible system of functions* if any two functions f and g from F are compatible.

Theorem 3.9. *If F is a compatible system of functions, then $\bigcup F$ is a function with* dom $(\bigcup F) = \bigcup\{\text{dom } f \,|\, f \in F\}$*. The function $\bigcup F$ extends all $f \in F$.*

Proof. We need to show (1) $\bigcup F$ is a function and (2) dom $(\bigcup F) = \bigcup\{\text{dom } f | f \in F\}$.

(1) Suppose there exists $(a, b_1) \in \bigcup F$ and $(a, b_2) \in \bigcup F$.
Then there exists functions $f_1, f_2 \in F$ such that $f_1(a) = b_1$ and $f_2(a) = b_2$.
But since f_1 and f_2 are compatible and $a \in \text{dom} f_1 \cap \text{dom} f_2$, therefore $b_1 = f_1(a) = f_2(a) = b_2$.
This shows that $\bigcup F$ is a function.

(2) Suppose $x \in \text{dom} \bigcup F$. Then $x \in \text{dom} f$ for some $f \in F$.
Suppose $y \in \text{dom} f$ for some $f \in F$. Then $x \in \text{dom} \bigcup F$.
Therefore $\text{dom}(\bigcup F) = \bigcup\{\text{dom} f \,|\, f \in F\}$. □

Definition 3.10. Let A and B be sets. The set of all functions on A into B is denoted B^A.

(We will return to this unique set B^A later in the proof of the cardinality of the continuum.)

4. Equivalences and Orderings

In this section, we will finish defining a few important types of relations that will help in defining natural and real numbers in set theory.

Definition 4.1. Let R be a binary relation in A.
(a) R is *reflexive in* A if for all $a \in A$, aRa.
(b) R is *symmetric in* A if for all $a, b \in A$, aRb implies bRa.
(c) R is *antisymmetric in* A if for all $a, b \in A$, aRb and bRa imply $a = b$.
(d) R is *asymmetric in* A if for all $a, b \in A$, aRb implies that bRa does not hold.
(i.e. aRb and bRa cannot both be true.)
(d) R is *transitive in* A if for all $a, b, c \in A$, aRb and bRc imply aRc.

These individual properties serve as the building blocks for the next three relationships, which will allow us to truly make progress.

Definition 4.2.
(a) R is an *equivalence on* A if it is reflexive, symmetric, and transitive in A.
(b) R is a *(partial) ordering of* A if it is reflexive, antisymmetric, and transitive in A. The pair (A, R) is called an *ordered set.*
(c) R is a *strict ordering of* A if it is asymmetric and transitive in A.

Remark 4.3. Now that we have established the definition of orderings and strict orderings, we can use $\leq$ and $\preceq$ to denote orderings and $<$ and $\prec$ to denote strict orderings. Thus $(A, \leq)$ is an ordered pair consisting of a set A and an ordering $\leq$, and $(B, \prec)$ is a strictly ordered pair consisting of a set B and a strict ordering $\prec$.

There is a close relationship between orderings and strict orderings as we will see in the next theorem.

Theorem 4.4.
(a) Let R be an ordering of A. Then the relation S in A defined by

$$aSb \text{ if and only if } aRb \text{ and } a \neq b$$

is a strict ordering of A.
(b) Let S be a strict ordering of A. Then the relation R in A defined by

$$aRb \text{ if and only if } aSb \text{ or } a = b$$

is an ordering of A.

Proof.
a) We need to show that S is asymmetric. Suppose aSb and bSa both hold for some $a, b \in A$. Then aRb and bRa both also hold. It follows that $a = b$ because R is antisymmetric. This is a contradiction since $a \neq b$. Therefore S is asymmetric.

b) We need to show that R is antisymmetric. Suppose aRb and bRa both hold for some $a, b \in A$. Suppose that $a \neq b$. Then aSb and bSa both hold. This is a contradiction since S is asymmetric. Therefore $a = b$, showing that R is antisymmetric. □

Definition 4.5. An ordering $<$ of A is called *linear* or *total* if any two elements of A are comparable in the ordering $<$. (i.e. for any $a, b \in A$, either $a < b$, $a < b$, or $a = b$.) The pair $(A, <)$ is called a *linearly ordered set*

(Intuitively, we see that the $\leq$ and $<$ relations in the set of real numbers satisfy the definition of linear orderings, but we can't view these relations in that light yet because we haven't yet defined numbers.)

5. Natural Numbers

In defining the natural numbers we begin by examining the most fundamental set, the empty set. We can very easily create a pattern that is a prime candidate for the definition of the natural numbers.

$\varnothing$ has zero elements.

$\{\varnothing\}$ has one element. (The set containing the empty set as an element has one element, namely, the empty set.)

$\{\varnothing, \{\varnothing\}\}$ has two elements. (The set containing the empty set and the set containing the empty set.)

And this process would continue infinitely until all the natural numbers have been defined.

But though the empty set is unique, a set containing one element is not. We could very well take any of the sets created above and construct a set with just one set. (e.g. take $\{\varnothing, \{\varnothing\}\}$ and construct $\{\{\varnothing, \{\varnothing\}\}\}$ to be a set with one element.) We see that the number of elements in a set will be essential to defining the natural numbers. Therefore we just need to make this definition rigorous.

Definition 5.1. *Cardinality* is the measure of the number of elements in a set. We denote the cardinality of a set A by $|A|$. Sets A and B have the same cardinality if there is a bijection from A to B. A and B are called *equipotent* if such a bijection exists.

Remark 5.2. This definition tells us that we do not necessarily need to know how many objects each set contains to know if they contain the same number. A bijection ensures that each element in A is paired with a unique element in B, and conversely each element in B is paired with a unique element in A. Therefore the two sets must have the same cardinality. This use of bijection will become increasingly important when we begin examining and comparing infinite sets.

Revisiting our prime candidate for natural numbers, we can revise it as:

$0 = \varnothing$

$1 = \{0\} = 0 \cup \{0\} = \{\varnothing\}$

$2 = \{0, 1\} = 1 \cup \{1\} = \{\varnothing, \{\varnothing\}\}$

$3 = \{0, 1, 2\} = 2 \cup \{2\} = \{\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\}\}$ etc.

We see that each number is defined based on the number that precedes it. This sequence is anchored by 0. As long as 0 is defined, then 1 can be defined. Once 1 is defined, 2 can also be, and so on. This brings us to the concept of induction.

Definition 5.3. The successor of a set x is the set $S(x) = x \cup \{x\}$.

Definition 5.4. A set I is called *inductive* if
(a) $0 \in I$.
(b) If $n \in I$, then $(n + 1) \in I$. (Here $n + 1$ denotes the successor to n).

Clearly, an inductive set contains 0 and with it, each successor. So any inductive set should contain the natural numbers. So to define a set that contains *only* the natural numbers, we arrive at the following definition:

Definition 5.5. *The set of all natural numbers* is defined by

$$N = \{n \,|\, n \in I \text{ for every inductive set } I\}$$

The elements of N are called the *natural numbers*.

Remark 5.6. A possible concern is whether we can even define such a set from ZF axioms. Certainly, the property $P(n) : n \in I$ for every inductive set I is a valid property of n. But unless there exists an inductive set, this property will always create the empty set under the Axiom Schema of Comprehension. The Axiom of Infinity allows us to move past this obstacle.

Now that we have natural numbers at our disposal, we will explore a few properties of natural numbers.

Definition 5.7.
(a) The relation $<$ on N is defined by: For all $m, n \in N$, $m < n$ if and only if $m \in n$.
(b) The relation $\leq$ on N is defined by: For all $m, n \in N$, $m \leq n$ if and only if $m \in n$ or $m = n$.

Theorem 5.8. $(N, <)$ *is a linearly ordered set.*

Proof. We need to show (I) The relation $<$ is an ordering of N and (II) Any two elements in N are comparable. We will do this by induction.

(I) We need to show (A) $<$ is transitive on N and (B) $<$ is asymmetric on N.

(I.A.) Consider the property $P(n)$: for all $k, m \in N$, if $k < m$ and $m < n$, then $k < n$. We need to show this holds for all $n \in N$.
(i) Base case: Consider $P(0)$.
Since there does not exist an $m \in N$ such that $m < 0$, $P(0)$ is trivially true.
(ii) Induction hypothesis: Suppose $P(n)$ holds. Consider $P(n + 1)$.
Suppose $k < m$ and $m < n + 1$ both hold. This implies $m < n$ or $m = n$.
Case 1) $m < n$. Then $k < n$ by induction hypothesis.
Case 2) $m = n$. Then since $k < m$, $k < n$ is trivial.
Thus $P(n)$ holds for all $n \in N$.
Therefore $<$ is transitive on N.

(I.B.) Suppose have $n < m$ and $m < n$. Then by transitivity $n < n$. Consider the property $Q(n)$: $n \not< n$. We need to show this holds for all $n \in N$.

(i) Base case: Consider $Q(0)$.
Suppose $Q(0)$ does not hold. Then we have $0 < 0$, which by definition is $\varnothing \in \varnothing$, which is a contradiction to the defnition of $\varnothing$.
(ii) Induction hypothesis: Suppose $Q(n)$ holds. Consider $Q(n+1)$.
Suppose $Q(n+1)$ does not hold. Then $n+1 < n+1$, by definition, is $n+1 \in n+1$.
We know $n+1 = n \cup \{n\}$, which implies that $n+1 \in n$ or $n+1 = n$.
Case 1) $n+1 \in n$. Thus $n+1 < n$. But since $n < n+1$, by transitivity we have $n < n$, which contradicts the induction hypothesis.
Case 2) $n+1 = n$. This is obviously a contradiction.
Thus $Q(n)$ holds for all $n \in N$.
Therefore $<$ is asymmetric on N.

(II) We need to show any two elements in N are comparable in $<$. Consider the property $R(n) : \forall m \in N$, either $m < n$, $n < m$, or $m = n$. We need to show this holds for all $n \in N$.
(i) Base case: Consider $R(0)$.
$0 \leq m$ for all $m \in N$, so $0 < m$ or $m = m$. Thus $R(0)$ holds.
(ii) Induction hypothesis: Suppose $R(n)$ holds. Consider $R(n+1)$.
Consider an arbitrary $m \in N$. Since $R(n)$ holds, $n < m$, $m < n$, or $m = n$.
Case 1) $m < n$. Then since $n < n+1$, by transitivity $m < n+1$.
Case 2) $m = n$. Then since $n < n+1$, $m < n+1$ is trivial.
Case 3) $n < m$. We need to show $m = n+1$ or $n+1 < m$.
Apply induction on m. Consider the property $S(m)$: for all $n \in N$ if $n < m$, then $n+1 \leq m$. Need to show this holds for all $m \in N$.
a) Base case: Consider $S(0)$. $S(0)$ holds since there is no $n < 0$.
b) Induction hypothesis: Suppose $S(m)$ holds. Consider $S(m+1)$. Assume $n < m+1 \Rightarrow n < m$ or $m = n$.
Case i) $n < m$. Thus $n+1 \leq m$ by induction hypothesis.
$m < m+1$ implies $n+1 < m+1$. Thus $n+1 \leq m+1$.
Case ii) $n = m$. Thus $n+1 = m+1$ implies $n+1 \leq m+1$.
$\therefore$ $S(m)$ holds for all $m \in N$.
Thus $R(n)$ holds for all $n \in N$.
Therefore any two elements in N are comparable in $<$.
Therefore $(N, <)$ is a linearly ordered set. ☐

Definition 5.9. A linear ordering $\prec$ of a set A is a *well-ordering* if every nonempty subset of A has a $\prec$ -least element. The structure $(A, \prec)$ is called a *well-ordered set*.

Theorem 5.10. *$(N, <)$ is a well-ordered set.*

Proof. We will prove by using strong (or complete) induction.
Let X be a nonempty subset of N. Suppose X does not have a $<$ -least element. Then consider the set $N - X$.
Case 1) $N - X = \varnothing$. Then $X = N$ and so 0 is a $<$ -least element. Contradiction.
Case 2) $N - X \neq \varnothing$. There exists an $n \in N - X$ such that for all $k < n,\ k \in N - X$.
(n necessarily exists because $0 \in N - X$, else $0 \in X$ and would be a $<$ -least element of X.)
Since we have supposed that $N - X$ does not have a least element, thus $n \notin X$.
Using strong induction, we see that for all $k < n,\ k \in N - X$ and $n \in N - X$. We can conclude $n \in N - X$ for all $n \in N$. Thus $N - X = N$ implies $X = \varnothing$.
This is a contradiction to X being a nonempty subset of N. ☐

6. Recursion and the Addition Operation

We will now move on to define basic operations on the natural numbers. Though ZF set theory is an adequate tool for rigorously defining all four basic operations of natural numbers (addition, subtraction, multiplication, and division), we will content ourselves to defining addition and leaving the others to a more specialized text of arithmetic of the natural numbers.

Definition 6.1. A *sequence* is a function whose domain is a natural number or N. A sequence whose domain is some natural number $n \in N$ is called a *finite sequence of length* n and is denoted

$$\langle a_i \,|\, i < n \rangle \text{ or } \langle a_i \,|\, i = 0, 1, \ldots, n-1 \rangle \text{ or } \langle a_0, a_1, \ldots, a_{n-1} \rangle.$$

The unique characteristic of a sequence is that we can order the elements. Since the domain is composed of natural numbers, and we've proven in the previous chapter that the set of natural numbers are linearly ordered, we can order the elements in a sequence by the natural number each element corresponds to. This is essential in our next topic of recursion.

Example 6.2. Let us consider two infinite sequences:

(a) The sequence $f : N \to N$ defined by
$$S_0 = 1 \qquad S_{n+1} = 2n$$
(b) The sequence $g : N \to N$ defined by
$$F_0 = 0 \qquad F_{n+1} = F_n \times (n+1).$$

(Here $n+1$ also denotes the successor to the natural number n.)

The key distinction between these functions is their parameters for defining the $n+1$ term. S is formulated by a property $P(x, y)$: $s_x = y$. We can immediately conclude from our axioms that $S = \{(x, y) \in N \times N \,|\, P(x, y)\}$ exists and is unique.

Examining F, we see that each F_{n+1} depends on the previous term F_n. It is not yet apparent how we can formulate a property $P(x, y)$ to prove the existence and uniqueness of F as we can of S. F_{n+1} can be computed provided that F_n is computed, which brings us to the definition of a computation.

Definition 6.3. A function $t : (m+1) \to A$ is called an *m-step computation based on a and g* if $t_0 = a$, and for all k such that $0 \leq k < m$, $t_{k+1} = g(t_k, k)$.

So F can be restated as:

$$F_0 = 0 \qquad F_m = 0 \times 1 \times 2 \times \ldots \times m$$

showing that F is the result of an m-step computation. Our next theorem will show that such a recursive function exists and is unique.

Theorem 6.4. The Recursion Theorem
For any set A, any $a \in A$, and any function $g : A \times N \to A$, there exists a unique sequence $f : N \to A$ such that
(A) $f_0 = a$
(B) $f_{n+1} = g(f_n, n)\ \forall n \in N$.

Proof. (The existence of f)
Let $a \in A$ and $g : N \times A \to A$.
Let $F = \{t \in \mathscr{P}(N \times A) \,|\, \text{t is an m-step computation on } a \text{ and } g \text{ for some } m \in N\}$.
Let $f = \bigcup F$.

Claim 1: f is a function.

(By theorem 3.9, it is enough to show that F is a system of compatible functions.)
Let $t, u \in F$, dom $t = n \in N$, dom $u = m \in N$.
We can assume without loss of generality that $n \leq m$. We will use finite induction to prove $t_k = u_k\ \forall k < n$.

(a) Base case: $k = 0$.
We know t and u are computations based on a and g. Thus $t_0 = a = u_0$ is trivial.
(b) Induction hypothesis: Let k be such that $k + 1 \leq n$. Suppose $t_k = u_k$.
Then $t_{k+1} = g(t_k, k) = g(u_k, k) = u_{k+1}$.

Therefore F is a system of compatible functions.
Therefore f is a function.

Claim 2: dom $f = N$ and ran $f \subseteq A$.

(It is obvious that dom $f \subseteq N$ and that ran $f \subseteq A$. We then need to show that $N \subseteq$ dom f to prove dom $f = N$. We will prove with induction.)
(a) Base case: Clearly $t = \{(O, a)\}$ is a 0-step computation. Thus $0 \in$ dom f.
(b) Induction hypothesis: Suppose t is an n-step computation ($n \in$ dom f).
Define t' on $(n+1)+1$ by

$$t'_k = t_k \text{ if } k \leq n \qquad t'_{n+1} = g(t_n, n).$$

We can see that t' is an n+1 step computation. Thus $(n+1) \in$ dom f.
Therefore dom $f = N$.

Claim 3: f satisfies conditions (A) and (B)

(a) Clearly $f_0 = a$ since $t_0 = a$ for all $t \in F$. Thus satisfying (A).
(b) Let t be an (n+1) step computation. Then $f_k = t_k$ for all $k \in$ dom t.
This implies $f_{n+1} = t_{n+1} = g(t_n, n) = g(f_n, n)$. Thus satisfying (B).

Therefore the existence of a function f satisfying the properties required by the Recursion Theorem follows from Claims 1,2, and 3.

(The uniqueness of f)

Let $h : N \to A$ satisfy (A) and (B). We will show $f_n = h_n$ for all $n \in N$ by induction.
(a) Base case: $f_0 = a = h_0$ is trivial.
(b) Induction hypothesis: Suppose $f_n = h_n$.
Then $f_{n+1} = g(f_n, n) = g(h_n, n) = h_{n+1}$.
Therefore $h = f$. □

Theorem 6.5. The Parametric Recursion Theorem
Let $a : P \to A$ and $g : P \times A \times N \to A$ be functions. There exists a unique function $f : P \times N \to A$ such that
(a) $f(p, 0) = a(p)$ for all $p \in P$
(b) $f(p, n+1) = g(p, f(p, n), n)$ for all $n \in N$ and $p \in P$.

Proof. Define a parametric m-step computation to be a function $t : P \times (m+1) \to A$ such that, for all $p \in P$,

$$t(p, 0) = a(p) \quad \text{and} \quad t(p, k+1) = g(p, t(p, k), k)$$

for all k such that $0 \leq k < m$. The rest of the proof is similar to the proof of the recursive theorem with the additional task of carrying p along and so will be omitted. □

Notice that the parametric version takes into account an additional variable of p. This allows us to define addition of natural numbers because addition is binary operation.

Theorem 6.6. Addition Operation of Natural Numbers
There is a unique binary operation $+ : N \times N \to N$ such that
(a) $+(m, 0) = m$ for all $m \in N$
(b) $+(m, n+1) = +(m, n) + 1$ for all $m, n \in N$.

Proof. This is the exact same proof as the parametric version of the recursive theorem. Let $A = P = N$, $a(p) = p$ for all $p \in P$, and $g(p, x, n) = x + 1$ for all $p, x, n \in N$. □

This definition satisfies all properties of addition such as
i) $a + 0 = a$
ii) $a + b = b + a$

iii) $a + (b + c) = (a + b) + c$
We leave these proofs as an exercise to the ambitious reader.

As mentioned at the beginning of the chapter, ZF set theory is an adequate tool to define all arithmetic operations of the natural (and real) numbers. We will simply take them as givens from here on out.

7. Integers, Rationals, and Reals

Now that we have the natural numbers, defining integers and rational numbers is well within reach.

Definition 7.1. Let $Z' = N \times N$. We can define an equivalence relation $\approx$ on Z' by $(a, b) \approx (c, d)$ if and only if $a + d = b + c$. Then we denote the *set of all integers* by

$$Z = Z'/\approx \qquad \text{(The set of all equivalence classes of } Z' \text{ modulo } \approx\text{).}$$

Definition 7.2. Let $Q' = Z \times (Z - \{0\}) = \{(a, b) \in Z^2 \,|\, b \neq 0\}$. We can define an equivalence relation $\approx$ on Q' by $(a, b) \approx (c, d)$ if and only if $a \cdot d = b \cdot c$. Then we denote the *set of all rational numbers* by

$$Q = Q'/\approx \qquad \text{(The set of all equivalence classes of } Q' \text{ modulo } \approx\text{).}$$

Definition 7.3. A linearly ordered set $(P, <)$ is called dense if for any $a, b \in P$ such that $a < b$, there exists $z \in P$ such that $a < z < b$.

Lemma 7.4. *$(Q, <)$ is dense.*

Proof. Let $x = (a, b)$, $y = (c, d) \in Q$ be such that $x < y$.
Consider $z = (ad + bc, 2bd) \in Q$. It is easily shown that $x < z < y$. □

Before we can define the real numbers, we will need a few more concepts.

Definition 7.5. Let $(P, <)$ be a linearly ordered set.
A pair of sets (A, B) is called a *cut* if
(a) A and B are nonempty disjoint subsets of P and $A \cup B = P$.
(b) If $a \in A$ and $b \in B$, then $a < b$.

(A, B) is called a *Dedekind cut* if additionally
(c) A does not have a greatest element.

(A, B) is called a *gap* if additionally
(d) B does not have a least element.

Remark 7.6. We have two kinds of Dedekind cuts
1) Ones where $B = \{x \in P \,|\, x \geq p \text{ for some } p \in P\}$
2) gaps

This distinction will be needed later in the proof of completion.

We see even though rational numbers are dense, they clearly have gaps. Take for example the two sets
1) $A = \{x \in Q \,|\, x > 0 \text{ and } x^2 > 2\}$
2) $B = \{x \in Q \,|\, x \notin A\}$

Clearly (A, B) is a gap in Q. Intuitively, we know that the real numbers cannot have gaps, and so our next step is to explore how to close gaps. We notice that the existence of gaps is closely related to the existence of suprema of bounded sets.

Definition 7.7. Let $(P, <)$ be a dense linearly ordered set. P is *complete* if every nonempty $S \subseteq P$ bounded above has a supremum. (i.e. $(P, <)$ does not have any gaps.)

There is a close relationship between dense linearly ordered sets and complete linearly ordered sets as we will show. This close relationship is what will allow us to define the real numbers.

Theorem 7.8. *Let $(P, <)$ be a dense linearly ordered set without endpoints. Then there exists a complete linearly ordered set $(C, \prec)$ such that*
(a) $P \subseteq C$.
(b) If $p, q \in P$, then $p < q$ if and only if $p \prec q$.
(c) P is dense in C.
(d) C does not have endpoints.

Furthermore, $(C, \prec)$ is unique up to an isomorphism over P. The linearly ordered set $(C, \prec)$ is called the completion *of $(P, <)$.*

Proof. Part 1: (The existence of completion)

We reference the two kinds of Dedekind cuts from remark 7.6.
We will denote those of the first kind by
$[p] = (A, B)$ where $B = \{x \in P \,|\, x \geq p$ for some $p \in P\}$.
We can then define the set
$P' = \{[p] \,|\, p \in P\}$
$C = \{(A, B) \,|\, (A, B)$ is a Dedekind cut in $(P, <)\}$.
Furthermore, we can order C and P' by $(A, B) \prec (A', B')$ if and only if $A \subset A'$.

Claim 1: $(P', \prec)$ is isomorphic to $(P, <)$.

Let $p, q \in P$ and the corresponding $[p] = (A, B), [q] = (A', B') \in P'$ where $A = \{x \in P \,|\, x < p\}$ and $A' = \{x \in P \,|\, x < q\}$. Suppose $p < q$. Then it follows that $A \subset A'$. So $[p] \prec [q]$, which proves the claim.

Claim 2: $(C, \prec)$ is a linearly ordered set.

a) Let $[r] = (A, B)$, $[s] = (A', B')$, and $[t] = (A'', B'') \in C$ where $A = \{x \in P \,|\, x < r\}$, $A' = \{x \in P \,|\, x < s\}$, and $A'' = \{x \in P \,|\, x < t\}$. Suppose $[r] \prec [s]$ and $[s] \prec [t]$. Then $A \subset A'$ and $A' \subset A'' \Rightarrow A \subset A'' \Rightarrow [r] \prec [t]$. Therefore $(C, \prec)$ is transitive.

b) Suppose $[r] < [s]$ and $[s] < [r]$. Then $A \subset A'$ and $A' \subset A$ which is a contradiction.
Therefore $(C, \prec)$ is asymmetric.

c) Take $[s]$ and $[t]$. Since these sets are defined based on s and $t \in P$, one and only one of three cases can occur: $s < t$, $t < s$, or $s = t$. It follows that $A \prec A'$, $A' \prec A$, or $A = A'$. Thus $[s] \prec [t]$, $[t] \prec [s]$, or $[t] = [s]$. Therefore $(C, \prec)$ is comparable.

Therefore $(C, \prec)$ is a linearly ordered set.

Claim 3: $(C, \prec)$ satisfies (a)-(d) from the theorem.

(a) By definition, P' is a set of Dedekind cuts of P. Therefore $P' \subseteq C$ is trivial.

(b) Let $[p] = (A, B), [q] = (A', B') \in P'$ where $A = \{x \in P \,|\, x < p\}$ and
$A' = \{x \in P \,|\, x < q\}$. Suppose $[p] \prec [q]$ (where $\prec$ denotes the relation in P'). It follows that $A \subset A'$. We know also that $[p], [q] \in C$. $\therefore$ $[p] \prec [q]$ (where $\prec$ denotes the relation in C). The converse is similarly trivial. (This shows that $\prec$ in P' coincides with $\prec$ in C.)

(c) Let $[p] = (A, B), [q] = (A', B') \in P'$ where $A = \{x \in P \,|\, x < p\}$ and
$A' = \{x \in P \,|\, x < q\}$. Suppose $[p] \prec [q]$. Thus $p < q$ and $A \subset A'$. Consider $z \in A - A'$. Then $p < z < q$ and $[p] \prec [z] \prec [q]$. Since $[z] \in P'$, we can conlude that P' is dense in $(C, \prec)$.

(d) Let $[p] = (A, B)$ where $A = \{x \in P \,|\, x < p\}$. Since $(P, <)$ does not have endpoints, there exists $z > p$. It follows that there exists $[z]$ such that $[p] \prec [z]$. Therefore C does not have endpoints.

Claim 4: $(C, \prec)$ is complete.

Let S be a nonempty subset of C that is bounded above.
Let $A_s = \bigcup\{A \,|\, (A, B) \in S\}$ and $B_s = P - A_s = \bigcap\{B \,|\, (A, B) \in S\}$.

We can see that (A_s, B_s) is a dedekind cut and is an upper bound of S.
(We need to show that (A_s, B_s) is the supremum of S.)
Suppose (A_0, B_0) is an upper bound of S. Then $A \subseteq A_0\ \forall (A, B) \in S$. It follows that $A_s \subseteq A_0$. This shows that $(A_s, B_s) \preceq (A_0, B_0)$. Therefore (A_s, B_s) is the supremum of S and $(C, \prec)$ is complete.

Therefore $(C, \prec)$ is the completion of $(P, <)$.

Part 2: (Uniquness of completion up to an isomorphism)

Let $(C, \prec)$ and $(C^* \prec^*)$ be two complete linearly ordered sets satisfying (a)-(d). We need to show there exists an isomorphism between the two.
If $c \in C$, then let $S_c = \{p \in P \,|\, p \leq c\}$.
If $c^* \in C$, then let $S_c^* = \{p \in P \,|\, p \leq^* c^*\}$.
We define the mapping $h : C \to C^*$ as follows: $h(c) = \sup^* S_c$.
We now need to prove that h is onto, preserves orderings, and $h(x) = x \ \ \forall x \in P$.
(1) Let $c^* \in C^*$. Then $c^* = \sup^*\ S_c$, so we can choose $c = \sup\ S_{c^*}$. We see that $S_c = S_{c^*}$ and $h(c) = c^*$, therefore showing that h is onto.
(2) Let $c \prec d$. Then there exists $p \in P$ such that $c \prec p \prec d$ because P is dense. We see that $\sup^*\ S_c \prec^* p \prec^* \sup^*\ S_d$, showing that $h(c) \prec^* h(d)$.
(3) Let $x \in P$. Then $\sup\ S_x = \sup^*\ S_x = x$, so $h(x) = x$. □

Definition 7.9. *The set of all real numbers* is the completion of $(Q, <)$ and is denoted by $(R, <)$.

8. Cardinality of Sets

A very natural question in the study of sets is the number of elements contained in a set. This question is very simple when the set is finite. (i.e. The set is equipotent to some natural number.) We simply say that the set has n elements, whatever the natural number n may be. The question becomes more interesting when examining infinite sets, which is naturally our next task.

Definition 8.1. *The cardinality of A is less than or equal to the cardinality of B* if there exists an injection $f : A \to B$. We denote this by $|A| \leq |B|$.

Definition 8.2. If $|A| = K$, $|B| = L$, and $A \cap B = \varnothing$, then $K + L = |A \cup B|$.

Definition 8.3. If $|A| = K$ and $|B| = L$, then $K \cdot L = |A \times B|$.

Lemma 8.4. *If $A_1 \subseteq B \subseteq A$ and $|A_1| = |A|$, then $|A| = |B|$.*

Proof. We know there exists an injection $f : A \to A_1$. We can define two sequences of sets by

$A_0 = A; \quad A_{n+1} = f[A_n]$ for each $n \in N$
$B_0 = B; \quad B_{n+1} = f[B_n]$ for each $n \in N$.

We will show that $A_n \subseteq B_n \subseteq A_{n+1}$ for all $n \in N$ by induction.
(a) Base case: $n = 0$. $A_0 \subseteq B_0 \subseteq A_1$ is trivial.
(b) Induction hypothesis: Suppose $A_n \subseteq B_n \subseteq A_{n+1}$ holds. Then $f(A_n) \subseteq f(B_n) \subseteq f(A_{n+1})$ holds. And since $f(A_n) = A_{n+1},\ f(B_n) = B_{n+1}$, and $f(A_{n+1}) = A_{n+2}$, then $A_{n+1} \subseteq B_{n+1} \subseteq A_{n+2}$ holds.

Let $C = \bigcup_{n=0}^{\infty}(A_n - B_n)$. We can now define a bijection $g : A \to B$ by

$$g(x) = \begin{cases} f(x) & \text{if } x \in C \\ x & \text{if} x \in (A - C) \end{cases}.$$

$g|_C$ and $g|_{A-C}$ are one to one functions with disjoint ranges. Furthermore
$f[C] \cup (A - C) = B$. Therefore $|A| = |B|$. □

Theorem 8.5. Cantor-Bernstein Theorem
If $|X| \leq |Y|$ and $|Y| \leq |X|$, then $|X| = |Y|$.

Proof. $|X| \leq |Y|$ implies there exists an injection $f : X \to Y$.
$|Y| \leq |X|$ implies there exists an injection $g : Y \to X$.
Clearly $g \circ f : X \to X$ an injection. We can see that $g[f[X]] \subseteq g[Y] \subseteq X$. It follows that $|X| = |g[f[X]]|$ and $|Y| = |g[Y]|$. Therefore By Lemma 8.4, we see that $|X| = |g[Y]| = |Y|$. □

Definition 8.6. A set S is *countable* if $|S| = |N|$. A set S is at most countable if $|S| \leq |N|$. (A set S is countable if there is a bijection between N and S.)

Countability is an essential concept of mathematics when working with infinite values. It distinguishes some infinities from others, giving us a basis for study. We will now show some properties of countability and countable sets.

Theorem 8.7. *An infinite subset of a countable set is countable.*

Proof. Let A be a countable set and $B \subseteq A$ be an infinite set.
Since A is countable, there exists a bijection between N and A denoted by $\langle a_n \rangle_{n=0}^{\infty}$. We can define another function f by

i) $f(0) = b_0 = a_{k_0}$ where k_0 is the least k such that $a_k \in B$.
ii) $f(n+1) = b_{n+1} = a_{k_{n+1}}$ where k_{n+1} is the least k such that $a_k \in B$, $a_k \neq b_i$ for all $i \leq n$.

We can see that $f = \{f(n) \,|\, n \in N\} = \langle b_n \rangle_{n=0}^{\infty}$ exists by the Recursion Theorem and is a bijection between N and B. □

Theorem 8.8. *The union of two countable sets is a countable set.*

Proof. Let $A = \{a_n \,|\, n \in N\}$ and $B = \{b_n \,|\, n \in N\}$ be countable. We can construct a sequence by

$c_{2k} = a_k$ and $c_{2k+1} = b_k \quad \forall k \in N$.

We see that $\langle c_n \rangle)_{n=0}^{\infty}$, showing there exists a bijection between N and $A \cup B$. Therefore $A \cup B$ is countable. □

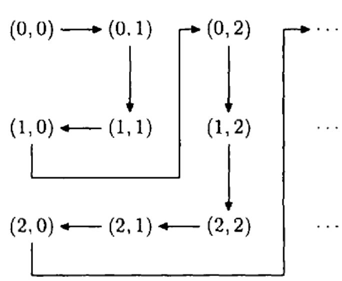
Corollary 8.9. *The union of a finite system of countable sets is countable.*

Proof. This is an immediate result of appling induction to the proof of the previous theorem. □

Theorem 8.10. *If A and B are two countable sets, then $A \times B$ is also countable.*

Proof. It is enough to prove that $N \times N$ is countable. (i.e. $|N \times N| = |N|$.) We will prove this in two ways. First with a simple visual mapping and second with a function.

(1) We can map $N \times N$ by:



(*Graphic taken from *Introduction to Set Theory* by Hrbacek and Jech.)

(2) We can also map this by the function

$$f(k, n) = 2^k \cdot (2n+1) - 1.$$

We can see that f is a bijection from $N \times N$ to N. □

Corollary 8.11. *The cartesian product of a finite number of countable sets is countable. (i.e. N^m is countable for every $m \in N$.)*

Proof. This is an obvious result of induction on theorem 8.10. □

Theorem 8.12. *The set of all integers Z is countable.*

Proof. This a trivial result of our definition of Z and theorem 8.10. □

Theorem 8.13. *An equivalence relation on at most countable sets has at most countably many equivalence classes.*

Proof. Let A be an at most countable set. Let E be an equivalence relation on A. We can define a function $f : A \to [A]_E$ by $f(a) = [a]_E$. We can see that f is a surjection between an at most countable set and its equivalence classes. Thus we have $|[A]_E| = |f[A]| \leq |A|$, proving that $[A]_E$ is at most countable. □

Theorem 8.14. *The set of all rational numbers Q is countable.*

Proof. This is a trivial result of theorem 8.13. □

From the above few properties, we see that any countable set has the same cardinality. We can then form the following definition:

Definition 8.15. $\aleph_0 = |A|$ for all countable sets A.

Remark 8.16. From the above, we can see that $\aleph_0 = |N| = |Z| = |Q|$. We will examine the cardinality of the set of all real numbers R in the following section.

We will end with a few properties of cardinal arithmetic.

Theorem 8.17.
A) For all $n \in N$, $n + \aleph_0 = \aleph_0 + \aleph_0 = \aleph_0$
B) For all $n \in N - \{0\}$, $n \cdot \aleph_0 = \aleph_0 \cdot \aleph_0 = \aleph_0$
C) For all $n \in N - \{0\}$, ${\aleph_0}^n = \aleph_0$

Proof. Omitted. □

9. Uncountable Sets

Intuitively, we know uncountable sets exist because the set of real numbers is uncountable. What is not apparent is the size of the real numbers. To find that, we first begin by proving uncountable sets exist.

Theorem 9.1. Cantor's Theorem
Uncountable sets exist. Namely, the power set of the natural numbers $\mathscr{P}(N)$ is uncountable.

Proof. Suppose $\mathscr{P}(x)$ is countable. Then there exists a bijection $f : N \to \mathscr{P}(N)$. Consider the set $S = \{n \in N \mid n \notin f(n)\}$. We can see that S is a subset of the natural numbers so $S \in \mathscr{P}(N)$. Thus $\exists z \in N$ such that $f(z) = S$.

Case 1) $z \in S$. Thus $z \notin f(z)$ implies $z \notin S$.
Case 2) $z \notin S$. Thus $z \in f(z)$ implies $z \in S$.
This is a paradox, therefore $\mathscr{P}(N)$ is uncountable. □

From this we see that $|\mathscr{P}(N)| > |N|$. Our next theorem will give us a set with the same cardinality as $\mathscr{P}(N)$. This set will also have a crucial connection to the cardinality of the set of real numbers.

Theorem 9.2. $|\mathscr{P}(N)| = |2^N|$. *(Here 2^N denotes the set of all functions on N into 2. See definition 3.10.)*

Proof. We will prove this by constructing a bijection $f : \mathscr{P}(N) \to 2^N$.

Part 1) Let $S \subseteq N$. Thus $S \in \mathscr{P}(N)$.
Define $X_S : N \to \{0,1\}$ by

$$X_s(n) = \begin{cases} 1 & \text{if } n \in S \\ 0 & \text{if } n \notin S \ . \end{cases}$$

Let $f(S) = X_S$. We can see that f is an injection from $\mathscr{P}(N)$ into 2^N. It remains to prove that f is a surjection as well.

Part 2) To show that f is a surjection, it is enough to show that $f(X_n^{-1}(1)) = X_n$.
Let $\phi \in 2^N$. Thus ϕ is a function on N into $\{0,1\}$.

$$\text{Consider } X_{\phi^{-1}(1)}(n) = \begin{cases} 1 & \text{if } n \in \phi^{-1}(1) \\ 0 & \text{if} n \notin \phi^{-1}(1) \end{cases}$$

We can see that $X_{\phi^{-1}(1)} = \phi$. Thus $f(\phi^{-1}(1)) = X_{\phi^{-1}(1)} = \phi$.
Thus f is a surjection from 2^N into $\mathscr{P}(N)$.

Therefore f is a bijection between $\mathscr{P}(N)$ and 2^N, which proves the theorem. □

Corollary 9.3. $|\mathscr{P}(X)| = |2^X|$ *for any set* X.

Proof. Similar to above. Replace N by X. □

Theorem 9.4. *The cardinality of the continuum is* $2^{\aleph_0}$

Proof. We will first prove $|R| \leq 2^{\aleph_0}$, then prove $2^{\aleph_0} \leq |R|$. We can finally use the Cantor-Bernstein Theorem to show that $|R| = 2^{\aleph_0}$.

1) Recall that we constructed real numbers as cuts in the set of rational numbers. Thus $R \subseteq \mathscr{P}(Q) \times \mathscr{P}(Q)$. We can see that $|\mathscr{P}(Q)| = |2^Q|$.
Thus $|R| \leq |\mathscr{P}(Q) \times \mathscr{P}(Q)| = |2^Q \times 2^Q| = 2^{\aleph_0} \cdot 2^{\aleph_0} = 2^{\aleph_0 + \aleph_0} = 2^{\aleph_0}$, which shows that $|R| \leq 2^{\aleph_0}$.

2) Consider $x \in [0,1) \subseteq R$. Each x has a unique (countable) decimal expansion.
Let $S = \{x \in [0,1) \,|$ the decimal expansion of x only contains 0's and 1's.$\}$.
Let $g_a(n) =$ the n^{th} digit in the decimal expansion for a.
We can define a bijection $f : S \to 2^N$ by

$$f(x) =< g_x(n) \,|\, n \in N > .$$

So $|S| = |2^N| = 2^{\aleph_0}$. But since $S \subseteq R$, we have $|S| \leq |R|$. Therefore $2^{\aleph_0} \leq |R|$.

We can apply the Cantor-Bernstein Theorem to conclude $|R| = 2^{\aleph_0}$. □

Acknowledgments.
I thank my mentors William Chan, Eric Astor, and Matthew Wright for their continual guidance and support. I thank Dr. J Peter May for granting me this opportunity to study mathematics in the REU program. I also want to acknowledge that many of the definitions, theorems, and proofs presented are based on those in *Introduction to Set Theory* by Karel Hrbacek and Thomas Jech. It has been my primary guide to writing this paper.

References

[1] Karel Hrbacek and Thomas Jech. Introduction to Set Theory (Second Edition: Revised and Expanded). Marcel Dekker, Inc. 1984.
[2] Thomas Jech. Set Theory (The Third Millenium Edition: Revised and Expanded). Springer Verlag. 2003.